
Stephen Reid

January, 2018

Submitted in partial fulfilment of MSc in Library and Information Science, City, University of London
Abstract

Introduced in parliament in November 2015, the Draft Investigatory Powers Bill was the most recent version of legislation written to provide a statutory basis for a range of powers providing police and security services with various means of capturing or intercepting electronic communications. Previous efforts at legislating for these powers attracted widespread criticism, and provoked political and legal opposition, and this Bill reprised concerns over what some felt to be the excessive scope of the powers included. This research seeks to examine UK national newspaper reporting of the legislation, published around the dates of the publication of the draft version of the bill, and when the legislation passed into law as The Investigatory Powers Act 2016, in order to evaluate the quality of this reporting.

Using the methodology of Critical Discourse Analysis to examine reports from a representative selection of UK national newspapers, the study aims to identify the dominant ways in which the issues are constructed in the news, and the range of sources which are drawn upon to demonstrate the disparate perspectives available. Working from the basis that newspapers represent a significant source of public information on important contemporary social issues, the research seeks to evaluate the effectiveness of newspaper reporting in providing a full and informative depiction of such matters.
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Aims and objectives</td>
<td>10</td>
</tr>
<tr>
<td>Methodology</td>
<td>13</td>
</tr>
<tr>
<td>The search for research data</td>
<td>14</td>
</tr>
<tr>
<td>Conducting the analysis</td>
<td>16</td>
</tr>
<tr>
<td>Selection of excerpts</td>
<td>18</td>
</tr>
<tr>
<td>Research validity</td>
<td>18</td>
</tr>
<tr>
<td>Research ethics</td>
<td>20</td>
</tr>
<tr>
<td>Literature review</td>
<td>21</td>
</tr>
<tr>
<td>Investigatory Powers legislation</td>
<td>21</td>
</tr>
<tr>
<td>Newspaper framing</td>
<td>22</td>
</tr>
<tr>
<td>Sources in the news</td>
<td>24</td>
</tr>
<tr>
<td>Surveillance</td>
<td>27</td>
</tr>
<tr>
<td>Analysis</td>
<td>32</td>
</tr>
<tr>
<td>2015</td>
<td>33</td>
</tr>
<tr>
<td>Discourse of need for the powers</td>
<td>33</td>
</tr>
<tr>
<td>Discourse of harms and risks</td>
<td>38</td>
</tr>
<tr>
<td>Discourse of government concessions</td>
<td>40</td>
</tr>
<tr>
<td>Discourse of oversight and safeguards</td>
<td>45</td>
</tr>
<tr>
<td>Exceptions to discourses</td>
<td>50</td>
</tr>
<tr>
<td>2016</td>
<td>55</td>
</tr>
<tr>
<td>Discourse of insufficient opposition</td>
<td>55</td>
</tr>
<tr>
<td>Discourse of privacy and rights</td>
<td>59</td>
</tr>
<tr>
<td>ECJ ruling: discourse of need</td>
<td>62</td>
</tr>
<tr>
<td>ECJ ruling: discourse of justice</td>
<td>65</td>
</tr>
<tr>
<td>Discussion</td>
<td>68</td>
</tr>
<tr>
<td>Limitations</td>
<td>74</td>
</tr>
<tr>
<td>Implications</td>
<td>76</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Reflective statement</td>
<td>77</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>79</td>
</tr>
<tr>
<td>References</td>
<td>80</td>
</tr>
<tr>
<td><strong>Appendices</strong></td>
<td>86</td>
</tr>
<tr>
<td>1. Articles for 2015</td>
<td>86</td>
</tr>
<tr>
<td>2. Articles for 2016</td>
<td>281</td>
</tr>
<tr>
<td>3. Themes and sources of 2015</td>
<td>436</td>
</tr>
<tr>
<td>4. Themes and sources of 2016</td>
<td>439</td>
</tr>
<tr>
<td>5. Research Proposal</td>
<td>442</td>
</tr>
</tbody>
</table>
Introduction

In the United Kingdom today, there are a significant number and type of sources that may be relied upon, or expected to provide information on subjects or issues of current importance. Social media platforms as a source of information are still in a state of relative immaturity, while radio and television have been a part of our society for decades, and newspapers in one form or another have persisted for centuries. Across these channels of dissemination, whether new or old, there exists a broad range of information which contributes in some way to keeping the population informed, although this differs considerably in its depth, its relevance, and its integrity. There is much talk, and growing concern over the apparent spread of dubious information on the Internet, specifically amongst social media output, and while this is certainly an issue of interest to all with a concern for information and its influence in society, it is important that we not let slip the shortcomings of more longstanding information channels when considering the quality of information available through mass media.

In the same way that information accessed on newer digital platforms can benefit from evaluation or analysis, rather than receiving ready acceptance, the output of what we now think as traditional media channels such as broadcast and print, should also bear due consideration, especially around contentious or divisive issues. While newspapers and their respective online presences are generally absent the most egregious abuses of validity and quality that Facebook, as an example, has been found to enable, it is important to understand the various forces, factors, and decisions which can influence how newspaper reporting is constructed (Curran and Seaton, 2010; Conboy, 2011; Broersma, den Herder and Schohaus, 2013), and what this means for consumers of newspapers, as well as what it might imply for society more broadly.
Though it is difficult to accurately measure the direct influence that a particular news media story or discourse exerts on public beliefs or attitudes (Happer and Philo, 2013), it is evident that when attempting to gauge the reported reach of various types of media, newspapers remain a key source to which people turn for information on contemporary issues. While the media by which people access news reportedly differs according to age, with television claiming a wider influence amongst older groups, newspapers - including their online presences - still feature more prominently as a source than social media (Newman et al., 2017). In light of this, it can be taken that newspapers form some meaningful part of the information landscape of current affairs, and therefore represent a fair indicator of the breadth of viewpoints offered on a particular issue. It is from this perspective that the current research set out to examine the reporting on the Investigatory Powers Act 2016 (IPA) as it appeared in a selection of UK national newspapers. Before further detailing the aims and the scope of the research, however, it will be useful to provide a brief outline of the legislation itself, and its context.

The bill was first published in draft form and presented to Parliament on the fourth of November 2015, and following the usual process of debate and amendment in both the House of Commons and the House of Lords, was enacted into law on the twenty-ninth of November 2016. The Act placed on a statutory footing a series of powers relating to the collection and storage of communications data, including the metadata of the emails, text messages (SMS), and mobile phone calls of UK citizens, as well as obliging Internet Service Providers to store the Internet connection records of their customers for twelve months. In addition, the Act also provided a legal basis for the security agencies to remotely interfere with digital communication devices such as computers, tablets and phones, with the legal requirement for third party companies to assist where necessary (Draft Investigatory Powers Bill, 2015). Some of these powers were covered in some form by previous legislation, such as the Regulation of Investigatory Powers Act of 2000,
while related capabilities had been used despite the absence of laws allowing for their use; this latter misuse being well documented in the information first released by Edward Snowden in June of 2013 (MacCaskill et al., 2013)

A previous attempt to pass similar legislation, The Draft Communications Bill, which was given the moniker of ‘The Snooper’s Charter’, provoked sufficient political opposition to be defeated by the Liberal Democrats in April of 2013, while in coalition government with the Conservatives. The following year saw the passage of the Data Regulation and Investigatory Powers Act 2014 (DRIPA), which provoked a legal challenge by two MPs, ending with a 2015 High Court judgement that two sections of the Act were unlawful and were to be suspended. This lead to the need for renewed legislation, the result of which was the Investigatory Powers Act 2016, and while it passed both Houses of Parliament with relative ease, in this case the European Court of Justice subsequently declared the provision for generalised collection of data to be unlawful. The ramifications of this decision for the powers covered by Act is unclear, especially in light of the UK’s decision to leave the European Union, though recent developments suggest that some changes will have to be made in order for the legislation to comply with the ruling (Travis, 2017).

In an attempt to determine the nature and the breadth of information on the IPA that the British public potentially had ready access to, this research will use reporting from a selection of UK national newspapers as its source material. Through the analysis of this material, it is hoped that several questions of interest might be addressed, and that issues for future consideration and action can be identified.

The first question the research sets out to ask, is to what extent did newspaper reporting of the legislation include a diverse range of voices, or express different
perspectives on the issues at stake? Any attempt to answer this question, inevitably leads to a consideration of how effective newspapers were in informing the public, a role which they have commonly been ascribed (Curran and Seaton, 2010; Matei, 2014; Lischka, 2016). This function of the press has been variously contested and questioned (Curran and Seaton, 2010; Hastedt, 2016), but the idea that news ought to fulfil some informative role in society remains a valid starting point, provided that one takes into consideration the broader context. In an idealised view of newspaper reporting, we would expect coverage to include a healthy diversity of voices and perspectives, particularly in the reporting of divisive or contentious issues, where differing explanations are likely to exist (Philo, 2007; Happer and Philo, 2013). While the availability of diverse information in itself is no guarantee of diverse viewpoints amongst a population, the absence of diverse information seems to be obviously problematic, due to the limiting effect it may have on the ways in which an issue can be understood, represented, or discussed (Fowler, 1991).

The second question which the research will aim to address is the existence of differences in reporting that occur between the different newspaper outlets: i.e. are there any significant differences in how issues are presented, depending upon the newspaper in which they appear; or are there consistent overlaps between particular papers? In a similar way, the existence of similarities and differences in how the issues are reported in the two periods selected will also be examined.

Finally, it is hoped that the research might help to identify some considerations, and possible courses of action that could be taken by those involved in information professions. For those interested in information literacy, and especially for those responsible for teaching and sharing information literacy practices and concepts, there is much of relevance in these questions. This might take the straightforward form of highlighting the need to appraise the quality of
information provided by news outlets, but it could also take the form of more actively addressing gaps or shortcomings of press coverage: while digital technologies have created the means for mass surveillance, they have also significantly eased the dissemination of information alongside of traditional channels.

At a very broad level, the issues under examination here relate to a number of aspects of the contemporary information landscape. This includes examination of the quality of information offered to the population, and the possible influence this may have; discussion of the practices of metadata and data collection, storage and analysis, which in one form or another contribute significantly to the current functioning of the digital world, but whose full implications are as yet unclear; and consideration whether those with professional roles in the world of information ought to be doing more to be involved in starting, and contributing to, debates around issues such as these, which ultimately affect the informational lives of all UK citizens, and are part of a significant change to the ways in which personal data is both understood and used.
Aims and objectives

The primary aim of this research, is to interrogate the newspaper reporting of The Investigatory Powers Act 2016, using Critical Discourse Analysis as its methodology, and this section will further elaborate on this, and the other objectives of the project. The research will draw for its source material upon reports from two periods: first, around the release of the first draft version of the legislation; and second, when the final version of the bill was passed into law. This legislation legitimates the use by police and security services such as GCHQ, of a range of significant powers, including the bulk capture, storage and analysis of communications metadata, and the employment of various capabilities to interfere with electronic devices (Draft Investigatory Powers Bill, 2015). Another key aspect of the Act is the obligation placed upon all telecommunications service providers to store for twelve months, logs of all websites visited by their customers: known in the bill as ‘Internet Connection Records’. Given the broad scope of the powers provided by this Act and the previous failures of the Conservative government to pass similar previous legislation, the relative ease with which this version passed is notable. While this is likely to be the result of a combination of numerous factors, including political events - indeed, a preoccupation with the issues surrounding Brexit is noted in some news coverage of the IPA - the examination of newspaper reporting seems a valuable means for gauging the range of information on the subject available to the public, which serves as a basis for how issues might generally be perceived, and influences further discussion or debate on the matter (Philo, 2008; Broersma, den Herder and Schohaus, 2013).

It is hoped that several objectives can be met in the course of the analysis of this material. The first of these, is to identify the most prominent, and most recurrent ways in which the legislation - be it in draft version, or in the form in which it passed into law - is presented, or framed by newspapers. This is of importance
here, as framing is an active process of choices on inclusion and exclusion, and can forefront certain viewpoints on a matter (Carvalho, 2008), thereby shaping public discourse, opinions and beliefs (Richardson, 2007). Pressures on the production of news, which tend to take the general shape of having to produce more news items, with less time and with fewer resources, has provided opportunities for external sources to more strongly influence how issues are framed by newspapers (Johansson and Odén, 2017), and has also limited the ability of reporters to offer more complex perspectives on issues (Conboy, 2011). Though the role of journalists in choosing the final framing of a story is still considerable, and should not be underestimated (Broersma, den Herder & Schohaus, 2013), Tiffen et al. (2014) highlight the salience of examining the framing of policy debate and political issues, in order to determine how narrowly or broadly these are framed, while Jäger (2001), argues that although varied positions on an issue might be present in newspaper reporting, there is a general homogeneity to the potential range of discourse offered. Specifically, the quality of debate is likely to affected by the range of perspectives and expertise that is drawn upon, beyond that of political actors; ideally, robust discussion should afford the opportunity for concerns from society more generally to be included in a meaningful way.

This relates to the second objective, which is to identify the sources drawn upon in the reporting. Particular emphasis here will be on the range of voices and perspectives that are included, or excluded, from the newspapers by way of being directly or indirectly quoted on the issue; the extent to which any especially dominant sources are present; and the potential implications of any identified dominance. Journalists at all newspapers rely heavily upon sources who can be seen to speak with some authority on an issue (Ekman and Widholm, 2015), in order to maintain credibility and reliability in their reporting. However, in order to serve the function of informing a reading public, it would be hoped that a range of
voices would be included, across the spectrum from dissent to support, and
drawing from sources who are variously impacted upon by the new law.

Thirdly, the research will seek to identify any significant differences in framing that
exist between individual newspapers, and similarly, any consistencies or patterns
that occur across multiple sources. This will take into consideration the two periods
as distinct bodies of reporting, while also highlighting any continuities or changes
in framing that occur across time, and drawing out any examples which offer
notably different views on the legislation. Taking these various dimensions of the
reporting into consideration ought to allow for an analysis which not only identifies
the different discourses at play, but also gives a view of how these evolved, and
how they relate to one another, which in turn offers a fuller picture of how the issue
is constructed (Jäger, 2001; Carvalho, 2008).

There is little doubt that this legislation has potentially serious ramifications for the
informational worlds of each and every UK citizen, from the possible impact of
decisions based upon information gained using the tools legislated for
(Chesterman, 2013; Bernal, 2016), to the potential effects on information seeking
or information behaviour (Lyon, 2015; Rachovitsa, 2016). In light of this, the final
objective of this research will be to consider actions that might be taken by
information professionals, specifically, to ensure that issues such as these are not
swept aside, but instead are exposed to the full debate and consideration that
they deserve. More generally, there may be actions towards the same end that
might be taken by any individual with an interest in the issues at hand, and these
too will be outlined.
Methodology

This research takes as its methodological starting point Critical Discourse Analysis (CDA), a practice defined less by a strict set of methods that must be followed, than by the aim of interrogating texts in order to reveal the often opaque ways in which power is exercised through language. Van Dijk (2001), offers a description of CDA as focused on, ‘social problems, and especially on the role of discourse in the production and reproduction of power abuse or domination.’ It is a methodology which views discourse as ‘socially constitutive’ (Fairclough, Muldering and Wodak, 2011), and which through a critical appraisal of the practice of discourse, aims to identify possible actions for change (Fairclough, 2015). By way of this active aim of contributing towards social change, critical discourse analysis is often overt in its political stance (Van Dijk, 2001; Fairclough, Muldering and Wodak, 2011), which for critics, is a problematic feature (Meyer, 2001; Carvalho, 2008). With regard to the stance of the current research, it is important to note that the subject is approached from the perspective that newspaper reporting lacks sufficient breadth and depth, particularly in its presentation of information on important, and potentially divisive issues.

For Wodak (2001), the language of mass media is deserving of examination, not only as an example of the exercise of power, but also on account of the transparency that it is often claimed to embody. Questioning this notion of the neutral presentation of news (Carvalho, 2008), through an exploration of some of the active processes of its construction, underlies the central aim of the research, and is why CDA seemed a suitable methodology to employ here.

In setting out to explore the context of the passage of the Investigatory Powers Act 2016, initial consideration was given to an analysis of Parliamentary debates and/or official governmental documentation relating to the legislation, in order to get a
sense of the themes and rhetoric used to provide evidence for its necessity. However, amid the current debate over the veracity and trustworthiness of news media, the proposed siting of the analysis was reconsidered. Newspapers, and the individual articles they publish are widely circulated and potentially widely read, allowing them an influence over the way that issues might be understood and discussed in society (Mautner, 2008; Curran and Seaton, 2010; Bednarek and Caple, 2012). This position of influence makes them fruitful and interesting objects of study, in particular for those wishing to explore the forms, uses and power of language in mass media (Mautner, 2008), and through examining the breadth of discussion in newspaper reporting of this subject, it was hoped that a fuller appreciation of the context of the passage of the IPA might be achieved.

The search for research data

Having set out the research question, aims and objectives, and settled on a methodology suitable to address the question, the next step was selecting which newspapers to use as sources. An important consideration at this stage was the desire to capture as representative a range of reporting as possible, but without producing an overwhelming body of research data. The primary inclusion criteria was to use daily newspapers with a national circulation, working from the premise that these have some equality of potential breadth of readership. While I did refer to recent circulation figures to identify the newspapers with the largest circulations (Ofcom, 2017), these figures were not solely influential in the selection process. To limit these national sources to a smaller and more manageable selection, the circulation of a newspaper was considered, along with the aim of including a diversity of newspapers.

This resulted in the following outlets being chosen for final inclusion: The Daily Mail, The Financial Times, The Guardian, The Independent, The Mirror, The Sun,
The Times, and The Telegraph, including daily and weekend titles, and including articles from both print and online versions. All research involving such choices of source is necessarily somewhat selective, but the final selection represents a good variety of available newspapers covering the range from broadsheet to tabloid sources, and includes newspapers with a general sympathy for right wing political parties and perspectives, alongside others more typically aligned with a more left wing view of affairs. Drawing on these sources, it was expected that the research data would offer reporting from across the spectrum, taking in at least all of the most commonly offered representations of this issue.

A scoping search for articles was run in both Factiva and NexisLexis databases, for articles including the terms, “snooper’s charter”, or “investigatory powers act”, or “investigatory powers bill”, in the newspapers previously detailed, and published between the first of November 2015 and the thirty-first of December 2016. These dates were chosen to cover the period preceding the release of the first draft of the bill, through to shortly after the final version was given Royal Assent and passed into law. During this exploratory search, it was discovered that in addition to listing results, Factiva also presents a bar graph view of results that displays the number of relevant items retrieved for each month of the search period. As one of the objectives was to examine reporting from more than one point in time, the ability to view results in this way was helpful in clearly revealing several relative peaks in the reporting, which were tentatively identified for inclusion in the analysis.

However, this initial search returned too many results, marking a clear need to refine the strategy. Taking into account the practical limitations that could be allowed for this, or indeed any project of this type (van Dijk, 2011), the focus of the research was limited to fewer periods. Those finally selected for analysis cover newspaper reporting published between the first of November and the thirty-first
of December 2015, and a second period between the first of November and the thirty-first of December 2016. These two periods were chosen to capture the plentiful newspaper coverage around significant points in the timeline of the bill, as well as the likelihood that they would offer a breadth of perspectives on the legislation.

Having switched to using the NexisLexis database after difficulties refining searches or exporting results from Factiva arose, searches were run for the selected terms and date ranges, though again an unmanageable set of results were returned, many of which were not directly reporting on the topic of interest. Another search was run, but this time adding the restriction to only retrieve results featuring three or more mentions of the terms, and excluding documents of fewer than five hundred words. It was intended that this would bring back fewer, but more relevant results, and also limit the output to lengthier pieces, and potentially those including more depth or detail in the reporting. This new search returned one hundred and four articles in 2015 and one hundred articles in 2016, which appeared much more relevant to the topic, and also provided a set of research data that seemed realistically manageable, and the results were exported as one document for each period, which are included as appendices.

**Conducting the analysis**

The approach to conducting the analysis itself was derived from several principal sources. A book by John Richardson (2007), which deals specifically on the critical discourse analysis of newspapers, in combination with Fairclough’s (2015), more general text on discourse, provided the practical basis for the methodology of this research. In addition to these, a set of guidelines outlined by Willig (2013) were also referred to. Though these guidelines were written with Foucauldian discourse analysis in mind, they were helpful in giving an initial overview of the various ways
in which the bill was constructed in the sampled reporting, and thereby provided a sort of summary of the discourses contained in the texts (van Dijk, 2001). Finally, Potter and Wetherell’s (1987), description of two phases of analysis was invaluable in clearly articulating the progression from identifying patterns in the research data, to the investigation of the possible functions and implications of these patterns, supported by the linguistic evidence found in the text.

An initial read through of results for each period was used to eliminate articles which did not report on the Investigatory Powers Bill as the primary focus of the piece, as well as a small number of duplicated results, bringing the numbers down to forty-five for 2015 and thirty-four for 2016, which formed the data for analysis. A second read through of the material was conducted, with the aim of identifying the various constructions of the legislation that were offered, before embarking on a closer reading and analysis. While reading, it became clear that editorial and opinion pieces showed a tendency towards the polemical in their handling of the issue, and it was decided to remove these from the analysis in order to create a more consistent set of research data to work with. By excluding these, the remaining articles included only what might be viewed as straight reporting on The Investigatory Powers Act, and therefore provided a fairer representation of how the issue was presented as news.

In each of the two periods for which data was gathered, several discourses were identified as being dominant amongst the reporting, by way of the frequency of their usage. This, in combination with a consideration of the most commonly quoted sources, helped to provide a general feel for the reporting, which was used to guide the choices made in how the discourses are approached in the analysis, including the order of their appearance and the discussion of relevant relationships to other discourses. These decisions formed the structure of the analysis, and also helped in the formation of the arguments that are made about
the quality of newspaper reporting on the Draft Investigatory Powers Bill, the
Investigatory Powers Act 2016 as it was passed into law, and the issues that were
offered as relevant to the legislation.

Selection of excerpts

In carrying out the analysis itself, excerpts were chosen which were felt to serve as
illustrative examples of these dominant discourses, and these were interrogated
for a better understanding of their construction, paying specific attention to
functions of vocabulary, grammar and structure (Jäger, 2001; Meyer, 2001;
Carvalho, 2008; Fairclough, 2015).

Within the text of the analysis, each excerpt used will be referenced back to the
number of the article as it appeared in the list retrieved from NexisLexis, and the
year of publication, e.g (1, 2015). The name of the newspaper in which the article
was published will also be noted, and where it is deemed significant to the
discussion, the date of the article will be included in the text. This provides all of
the detail that is potentially relevant to the discussion of the discourses, and also
offers a straightforward means of directing readers to the article quoted in each
case.

Research validity

The position of the research in relation to its subject has been laid out at the
beginning of this section, though the underlying political and social motivation
does not exempt the study from aiming for, and being able to demonstrate validity
in its methods and findings. In relation to this aim, it is vital to note that the initial
‘indexing’ (Seale, 2011), of discourses running through the reporting, carried out
as a manual process, is necessarily prone to variability and rests upon an element of interpretation (Elliott, 2011).

While this limits the precise data that can be provided to validate this early step, other data has been included for reference to by the readers, which does support the validity (Seale, 2011). This includes both the original research data output, in the form of all articles matching the search criteria, within which the narrowed selection initially included for analysis is highlighted, along with some tables used to quantify the occurrence of broad themes within the reporting, and the sources included.

The discourses identified, analysed and discussed in no way represent an exhaustive examination of the issues that were raised in the reporting of the two periods, nor is it intended that they do so. As stated in the aims, it is hoped that the research will highlight some of the more prominent discourses, as a means of evaluating the overall character of the reporting, while acknowledging that alternative readings and evaluations might similarly be made. Nevertheless, it is believed that the identification of prominent discourses, and the discussion of their intended function(s), have been carried out consistently and might be readily inferred from the research texts (Seale, 2011). In addition, it is hoped that the names chosen for the discourses closely match their possible function, but manage to avoid invoking any value judgments.

While it is hoped that adequate steps have been taken to establish the validity of this study, when evaluating the validity of any research, whether quantitative, qualitative, or using mixed-methods, it is helpful to keep in mind the claim that infallibility is not possible (Potter and Wetherell, 1987), alongside the acknowledgement that the very attempt to assess research validity is subject to various differing perspectives (Hammersley, 2008).
Research ethics

All research must of course give proper consideration to ethical issues that might arise from its conduct, and where necessary, should obtain ethical approval from the appropriate ethics body or committee. In this case, no ethical implications were felt to be present. No people were involved at any stage, removing any need to consider issues covering research participants, and the research data used was previously published in UK national newspapers, making it freely available in the public sphere.
**Literature review**

This section will present an overview of the relevant literature, beginning with that which discusses UK legislation for powers similar to those of the Investigatory Powers Act 2016, or the Act itself, before going on to consider literature relating to the framing of newspaper articles, and the sources included or excluded, concluding with an examination of the relevant issues to be found in the literature on surveillance. There is surprisingly little in the way of research on the IPA 2016, but the existence of numerous similar legislative acts in the UK, going back to the Regulation of Investigatory Powers Act 2000 (RIPA), allowed for literature discussing the predecessors of the current Act to be consulted.

**Investigatory Powers legislation**

In the discussion of RIPA 2000, Clarke (2001), highlights the legitimate benefits that surveillance and interception powers provide in tackling serious crime, while pointing out the balancing need for adequate scrutiny to be applied to these powers, something he suggests has been achieved in the legislation. The aim of providing statutory grounding for surveillance powers is welcomed (Reid and Ryder, 2001), and the effectiveness of the provided safeguards are discussed (Hörnle, 2010), with criticism being levelled at the insufficient measures taken to protect privacy and human rights (Fenwick, 2001). It is further suggested that the Act uses exaggerated claims of security need in order to advance the policy (Chatterjee, 2011), and that the legislation is a rushed, short term solution to a much longer term issue, which may ultimately create more problems than it helps to solve (Reid and Ryder, 2001).

The tension between surveillance powers and the need for human rights protections also came up in discussion over the Data Retention and Investigatory
Powers Act 2014 (DRIPA), where particular attention is given to several European Court of Justice rulings on data protection and surveillance legislation, the surprising rush in writing the Act, and the legal challenges being brought against it (Grossman, 2014). In the debate over the Investigatory Powers Act 2016, a continuing theme of the incompatibility of legislation with human rights, especially as they relate to privacy, is to be found (Bieker, 2016; Waranch, 2017), and while there is also a welcoming of debate, policy review, and the attempt to bring more transparency to the known powers of intelligence agencies, there is also acknowledgement of an imbalance in the voices influencing this debate (Hintz and Brown, 2017). Finally, as with previous attempts to legislate for these, or similar powers, the excessive breadth of their reach also comes in for criticism (Waranch, 2017). In searching for additional relevant literature, it was found that there is a good deal of material which considers issues which are connected to the subject of this research, though sometimes in relation to different topics. There are three strands of inquiry, in particular, which are of clear relevance to the attempt to answer the current research question.

**Newspaper framing**

The first of these explores the ways in which subjects are framed within newspaper reporting, and the possible implications of this process of framing. The effort to make this framing explicit is one of the key elements of critical discourse analysis, generally enabled by an examination of the linguistic tools and techniques used to shape the representation of a subject, and given the highly mediated basis of our understanding of the world and the events that take place in it (Potter & Wetherell, 1987; Fairclough, Graham, Lemke and Wodak, 2004), the exposition of the ways in which mass-media messages are constructed might lead at least some readers, viewers and listeners to appreciate the importance of being able to evaluate information.
The framing of issues by newspapers should be understood as one active process amongst the many that together work to create the news. Richardson (2007) argues that we ought to consider every element of a text to be the result of some active choice made by its creator, though with this said, it is important to point out that while the creation of news can be viewed as a process of selections and decisions, this is not to suggest any conspiratorial attempt to deceive or mislead the readership, but rather to dispel any myth of news as a neutral transmission of facts (Fowler, 1991), and to highlight the value of appraising information.

The impact of framing is most pertinent in terms of the initial basis that it forms for the general public's understanding of a subject. Lacking the time, resources, and often the interest to conduct individual research, the public generally rely upon media sources, including newspapers, to acquire and disseminate information on matters of importance or relevance (Matei, 2014). From this position of influence, the emphasis, or foregrounding of certain aspects of a subject, alongside the diminution or exclusion of other aspects (Thorsen, 2017), can work to guide the likely understandings that might be formed by readers.

Although the media construction of a subject might be best understood as part of a dynamic process which informs the reader's perception of an issue or their related opinions and beliefs (Greenberg and Hier, 2009), there is sufficient evidence to argue for the influence that media exerts over 'the construction of public knowledge' (Philo, 2008), and therefore, for an appreciation of newspaper framing to be useful in the evaluation of its quality. Keuhn (2017) offers the further claim that the competing messages or discourses offered by the framing of subjects, contribute towards shaping which aspects of a subject are understood to be important, and that this in turn can determine the debate around future policy decisions. The sort of effects this might involve, include the identification of
particular actors who hold responsibility for causing the issue, or for solving it, or it may work to define the range of potential solutions available (Greenberg and Hier, 2009; Keuhn, 2017).

The ways in which subjects are framed by newspapers then, can serve to limit the breadth of perspectives that might readily be held by those informed only by these sources, as well as determining the starting point for subsequent debates on the subject, as well as any resultant action, and even future policy (van Dijk, 1996; Jäger, 2001; Bednarek and Caple, 2012). For those with any responsibility for information literacy or similar, awareness of the implications of framing could usefully be included as another part of an overall capacity for critical appraisal of information, specifically as it applies to mass-media sources.

**Sources in the news**

A second relevant strand of discussion found in the literature, is focussed upon the examination of sources which are quoted or included in articles, with the general intention of evaluating the extent to which a variety of views on a subject are expressed. Although there is a need for newspapers to draw upon credible sources on which to base their reporting (Bednarek and Caple, 2012), without some breadth of perspectives being made available in the news, there is a clear risk that popular understanding of an issue might be overly narrow, or biased towards one or other of the various ways in which it could be perceived (van Dijk, 1996). This is problematic if we wish to have an informed populace, given that newspapers, through their printed and their online output, represent an appreciable source of general information (Fairclough, 2015).

Newspapers rely upon external sources to produce their reporting (Fowler, 1991), and without the inclusion of sources, reporting would lack the reference to
verifiable information that is helpful in producing reliability. Beyond the considerations of veracity, however, sources also serve the function of providing reporting with essential information on the background and the context of an issue, and in many cases they might have expert knowledge that is central to the understanding of a subject (Ekman and Widholm, 2015). Any exploration of the sources drawn upon by newspapers, should pay attention to a number of factors relating to: the structures, forces, or relationships that determine inclusion or exclusion; which sources are predominantly included or excluded; and the possible, or likely effects of these factors as they direct the influence of newspaper output.

With regards to this first point, Fowler (1991), suggests that the matter of simple convenience can influence the sources used, as journalists go to those who are likely to have newsworthy information to share. Somewhat intertwined with this, is the fact that there are particular sources who have well organised relationships with newspapers or journalists, which again eases the process of obtaining information (Mautner, 2008). In relation to those sources who enjoy such relationships, which include government, Non-Governmental Organisations and corporations (Philo, 2007), there is concern that this has enabled increased media management by the sources, and has led to a closeness which threatens the critical distance which journalism ought to maintain (Conboy, 2011). With these close relationships, there is also mention of a form of dependency, partly driven by the fragile economics of contemporary newspapers (Johansson and Odén, 2017), and which may result in more favourable or positive coverage for fear that these sources will withdraw (Matei, 2014).

When examining the sources most commonly included in newspapers, Fairclough (2015), notes that the sources used do not equally represent all groups of society. While this might be expected to some extent, in part due to the practicalities of
including a variety of voices representing all aspects of an issue, it has been argued that the inclusion of multiple sources might indicate a more active orientation on behalf of journalists attempting to offer differing perspectives (Tiffen et al., 2014), though even with the inclusion of multiple sources, it seems that a hierarchy of sources (van Dijk, 1988) ensures that certain voices enjoy routine and dominant inclusion in newspapers (Herman and Chomsky, 1988).

Exemplifying this, Greenberg and Hier’s (2009) examination of news coverage of CCTV schemes in Canada found that police and government sources dominated in terms of their inclusion as voices, with a similar dominance of sources being reported in other examinations into newspaper coverage of surveillance related issues. Government sources in particular, were found to dominate the coverage of Edward Snowden’s disclosures by the newspapers of both New Zealand (Keuhn, 2017) and the United Kingdom (Wahl-Jorgensen, Bennett and Cable, 2017), while the reporting of encryption, in the context of surveillance and these same disclosures in The Guardian in the UK and The New York Times in the USA, was also found to be heavily skewed towards a legitimation of surveillance powers by political and governmental voices (Thorsen, 2017).

In a project examining the media of eleven countries across Europe, North and South America, Asia and Australasia, with a specific interest in the relationship between news media and engaged citizenship, the measure of this dominance was found to average two to one for government versus opposition sources (Tiffen et al., 2014). The inclusion of government sources at a higher rate than oppositional sources not only tends to lend prominence to the perspective of government, it can also function, by way of repetition, to lend legitimacy to their viewpoint, and to entrench their power to influence the shape of public discussion on an issue (Mautner, 2008). Alongside this prominence of government sources, newspaper coverage of surveillance related issues were found to be lacking in the
inclusion of non-governmental sources as a whole (Lischka, 2016), and non-institutional sources such as academics or researchers, in particular (Keuhn, 2017), though it has also been found that in cases where official consensus on an issue is absent, reporting is more likely to include sources beyond the typical range (Hastedt, 2016). Linked to this discussion of inclusion or exclusion of sources, Bennett (1990) suggests that an indexing of sources and viewpoints can be found in the news, whereby the views of sources tend to align with any already established, or emerging official opinion on a subject.

Though there is much evidence to suggest an imbalance of voices included in the debates of newspaper reporting, it is also important to acknowledge that there is an interplay between the material that sources provide, and the work of journalists and editors, which determines the final shape of the reporting that is produced (Broersma, den Herder and Schohaus, 2013), including the source material and its presentation. For Johansson and Odén (2017), this relationship between source and journalist should be central to research on the news media, given its influence over what information becomes public and in what form, and also over what remains private, while Conboy (2011), would like to see the inclusion of a more active voice for citizens. It is also relevant to note that the diminishing breadth of press ownership might impact on the breadth of reporting (McChesney, 1997; Bagdikian, 2000; Curran and Seaton, 2010), though a detailed consideration of this point is beyond the scope of the current research.

Surveillance

The final relevant aspect of the literature concerns itself with the coverage of surveillance technologies and practices within newspaper reporting; sometimes extending to include more general issues of intelligence and security which also provide context. Surveillance is by no means a new phenomena (Higgs, 2001), nor
an especially new field of study, and there is a sizeable literature on the topic, including plentiful discussion of the potential consequences of surveillance practices and the attendant uses that might be made of the information it provides (Lyon, 2007; Solove, 2011; Marx; 2015; Parsons, 2015; Bernal, 2016).

The development of our society and the means by which it is governed at a local and national level has, over time, lead to increasing amounts of information on individual citizens being held by the state as an entity, leading some to consider surveillance as a condition of modernity (Bennett, 2011), or as an integral part of the functioning of the bureaucratic state (Higgs, 2001; Lyon, 2007). While a certain amount of surveillance of this type might be necessary for the smooth functioning of state infrastructure, the type of surveillance powers provided for by the IPA go considerably beyond such functions, and have been the subject of much debate and disagreement.

Included amongst this, are several recurrent themes which will be discussed here, although a much broader range of debate can be found, covering the need for surveillance as well as the risks; the individual, social and political implications of surveillance; and considerations of future surveillance, amongst other related topics. Though aspects of the recent history of surveillance practices are widely acknowledged, and even spoken about in some of the newspaper reporting analysed during the research, it is argued that the surveillance practices of today are far removed from anything that has gone before, particularly on account of the ways in which they are embedded into the acts of daily digital life that many of us engage in, whether consciously or not (Lyons, 2007; Bernal, 2016; Dencik and Cable, 2017). Indeed, it is suggested by Lyons (2015), that the Internet and its various platforms and methods for communication have made us active participants in surveillance, rather than passive targets.
A persistent theme in the literature on surveillance is the potential for a ‘chilling’ effect on the activities that individuals would normally carry out, and might relate to a variety of contexts and behaviours. In a recent survey (Penney, 2017), respondents reported that knowledge of government surveillance would lead them to change their information behaviour while online, for example, by restricting the information that they searched for or shared with others, a finding that echoes Bernal's (2016), assertion that this function of surveillance to impel individuals towards self-censorship, effects both those receiving and imparting information. For others, the concerns over surveillance touch upon more central aspects of personhood, stemming from our nature as 'informational beings' (Floridi, 2005), and the associated importance of informational privacy (Floridi, 2005; Mathiesen, 2015), and the potential impact that surveillance practices might have upon the capacity for self-definition and self-development (Parsons, 2015).

Lyon (2015), suggests that most people can agree on the benefits derived from the freedom to be oneself, free from observation, though there is recognition that a full account of the possible harms of surveillance can only be gained through consideration of its cumulative and social effects (Hughes, 2015), and that too narrow a focus on individual benefits and rights risks overshadowing these wider aspects of surveillance and power (Huysmans, 2016). A theme commonly used to achieve this end, warns Lyon (2015), is the false balance that is created between the right to privacy and the need for security. The broader discussion of the social impacts of surveillance include the risks posed to freedom of expression and assembly, alongside the potential limiting of relationships (Bernal, 2016; Sloan and Warner, 2015; Stahl, 2016). Solove (2011), highlights the possible use of surveillance to inhibit protest or dissent, while Lyon (2015) draws attention to the profound imbalance of power it creates, and more general condemnation of indiscriminate surveillance practices position them as 'the companion of
repression’ (Marx, 2015), and as endangering ‘the very conditions of democracy itself’ (Parsons, 2015).

Some further risks are also discussed, including concerns over the vulnerability of surveillance data to the same sort of attacks, leaks or accidents inherent to all data storage (Bernal, 2016), and the likely discrimination of surveillance towards certain groups, which may well serve to reinforce existing categories of prejudice (Lyon, 2007; Lyon, 2015). It is also suggested that a desire to believe in technology as the answer can limit the possibility of considering other approaches or solutions, such as increased numbers of police and security service agents (Lyon, 2007; Dencik and Cable, 2017), and that larger scale data based surveillance may be more likely to introduce mistakes into the processes of identification (Lyon, 2015), while failing to adequately account for the possibility of inaccurate data (Clarke, 1994).

There is also felt to be a lack of recognition of the politics of the concepts of privacy and surveillance (Lyon, 2007), as well as those of the categories applied to the data being collected and counted, which tend to be viewed as though naturally occurring, rather than the product of human decisions and processes (Barocas et al., 2014). The same issue of non-neutrality extends to the algorithms on which contemporary surveillance programmes rely, and though the difficulties involved in ‘identifying the influence of human subjectivity in algorithm design and configuration’, along with any potential ethical impact this might have, are acknowledged (Mittelstadt et al., 2016), such issues ought to inform the future debate over surveillance and its workings, which should strive to insist on the provision of better evidence that the powers are both needed, and effective (Bernal, 2016). A fuller debate of these issues might also be expected to enrich the public perception of surveillance. In general, polls have pointed to a public resigned to the inevitability of surveillance, and though older generations view surveillance measures positively while younger generations take a negative view.
(Bakir et al., 2015; Dencik and Cable, 2017), there is both a belief that surveillance improves security, and that it has been taken too far (Dencik and Cable, 2017). Further to this, a lack of discussion of individual agency when it comes to dealing with surveillance (boyd, 2011), has sustained a situation where people have little knowledge of how to limit the surveillance data gathered, and feel that any attempt to do so signals wrongdoing (Dencik and Cable, 2017).

Finally, it is suggested that the ethics of surveillance requires further exploration (Palm, 2014), and that information ethicists might play a role in contributing to the continued debate that is needed (Mathiesen, 2015). Indeed, any evaluation of the above dimensions of surveillance could be beneficially informed by heeding Edward Snowden’s question regarding the ethics of the society we want to live in (Lyon, 2014), which is to say, that the debate over surveillance and the choices arising from that debate, will have lasting consequences, but that these can be influenced by proper consideration.

Having explored the relevant literature, it is now time to turn to the analysis of the research data itself, for a view of how newspapers reported on issues around the Draft Investigatory Powers Bill and The Investigatory Powers Act 2016.
Analysis

For the analysis, articles published in 2015 were examined separately from those of 2016, though the relationship between the two sets of data was present as an aspect of the analysis at all times. The reporting of both periods offered numerous constructions of the Investigatory Powers bill - firstly in its state as a potential piece of legislation, and secondly as enacted law of the UK - and in each case a number of discourses were identified as prominent in terms of the scope of their use: that is, the frequency with which they appeared, and also the range of newspapers making use of them. Some of these were persistent across the two months of news under examination in each year, and several discourses were evident in the reporting of both 2015 and 2016.

In the main, however, discourses enjoyed general inclusion for only part of the time surveyed, giving way to new discourses either as fresh points of discussion were introduced into the news, or with the occurrence of external events that had relevance to the bill. At times, more than one prominent discourse appears at the same time, either providing support for one another, or serving an oppositional role. While the discourses will be analysed in isolation, these sorts of meaningful relationships will also be noted, as they are a key feature of how the reporting functions to provide a cohesive narrative on an issue.

In analysing and discussing the reporting, excerpts will be selected which exemplify specific discourses. These may be chosen to highlight occasions when the same instance of a discourse is used in multiple sources; where features of the chosen text serve especially well to demonstrate the possible function of a discourse; or to illustrate where an exception to the dominant discourses is being offered.
The first articles discussing the bill precede the release of the draft version and its announcement in Parliament, and reporting from the first days of November 2015 frequently outlines the key powers of the IPB, specifically the requirement that Internet Service Providers retain twelve months of ‘internet connection records’ for all customers; the ‘bulk collection’ and storage of all communications metadata; and the provision that technology companies comply with police and security agencies in enabling ‘equipment interference’ (Draft Investigatory Powers Bill, 2015). Having provided this context, articles generally tend to offer some combination of three initial discourses which are broadly taken up. These discourses are, the concessions being made by the government in this new Bill; the need for the key powers which are included within the legislation; and the oversight which will be applied to the powers. There is regular interplay between these discourses, with the ‘need’ being supported by the ‘concessions’ made, or the ‘oversight’ to be offered.

Discourse of need for the powers

Arguably the most central of the three initial discourses, is the case that is made for the need to equip the police and other security agencies with the powers in question in the first place. This discourse sets out the stand taken by the government and its supporters to justify the Investigatory Powers Bill, and position it as necessary. The need for the powers is demonstrated by way of the protection they will offer against the threats facing contemporary society. Typically, these threats take the forms of terrorist attacks, the activities of paedophiles on the Internet, and the somewhat amorphous threat of criminals or serious crime, all of which are said to have taken advantage of new technologies, enabling them to operate beyond the existing capabilities of law enforcement to detect or prevent their activity. While these threats may well be mitigated to some extent by the
capabilities granted by the IPB, and are activities that virtually everyone would be pleased to see curtailed, they also represent potent currents of fear to be tapped into and exploited.

The discourse of need is represented across all of the newspapers, with a particular predominance in the reporting of early November. The following excerpt, which appeared on the first of November in articles in The Sunday Times (8, 2015), The Independent (4, 2015), and the Mail Online (6, 2015), gives a concise account of the need:

‘A government source said ... “We know these powers are needed as technology changes and terrorists and criminals use ever more sophisticated ways to communicate. But we need to give people the reassurance that, not only are they needed, but that they are only ever used in a necessary, proportionate and accountable way. That is what this bill is all about”’

The quoted government source, speaking collectively, says that ‘We know’ the powers are needed. Stated this way, it is to be taken that the government has knowledge on the subject which leads them to be certain of the need, and which eliminates the possibility of any doubt. The need is also linked to changes in technology, which are framed passively with no actor behind them, and also absent any details on what type of technology or any particular instances of it, making for a vague claim. The statement presents these technologies as somewhat uncontrollable, and subject to misuse which can only be prevented by countervailing capabilities. Technology, here, is a space of struggle for balance which these powers will provide, though the argument also opens up the possible
need for the further extension of powers, in order to combat threats which might emerge with future 'changes'.

Explicitly linked with the process of technological change, is the existence of ever more sophisticated means of communication, which are being used by terrorists and criminals. Specifying these two groups amongst the widespread users of encrypted communications services, supports the case that the intent of the legislation is targeted, even while the communications of all UK citizens is set to be collected and stored for possible analysis and use.

The final two sentences of the quote present the entire IPB as a statement of need for the powers, alongside reassurance of the accountable and proportionate use of its powers, though when the source says, ‘... we need to give people ... reassurance ...’, this reads more like an acknowledgement that doubts and concerns are inevitable, and that reassurance will simply be offered as a means to assuage concerns, with the actual aim of enabling the passage of the legislation without any meaningful discussion.

The discourse of need, justified by technological changes that have enabled threats which the powers of the IPB are essential to combatting, is further reinforced by several figures. Theresa May, then Home Secretary and author of the bill, is quoted on the fourth and fifth of November in articles in the Mail Online (42, 2015), the Guardian (30, 2015), The Independent (38, 2015), and the Mail Online (58, 2015), stating that,

‘There should be no area of cyberspace which is a haven for those who seek to harm us to plot, poison minds and peddle hatred under the radar.’
Using a similar theme, Andy Burnham, shadow home secretary, informs us of,

'a 'broad acceptance' that a new law was needed. 'He told
Murnaghan on Sky News: "The online world has created blind
spots the authorities can't see any more."

in a statement reported between the first and the ninth of November by the Mail
Online (6, 2015), the Mail Online (42, 2015), and the Mirror (68, 2015), and which is
repeated again in Parliament, and reported by The Guardian (30, 2015). David
Cameron tells ITV's This Morning that 'we shouldn't allow the internet to be a safe
space for them to communicate and do bad things' (The Guardian, 14, 2015),
'them' being terrorists, criminals and child abductors. This same theme is also
used by the National Police Chiefs' Council, although they warn of 'no-go areas
online where we can't trace criminal activity' (The Guardian, 15, 2015).

These sources, speaking on behalf of the government or some beneficiary of the
IPB, all offer a view of the Internet, though variously named, as an abstract and
unregulated - unlawful even - site of technological struggle between the 'them' of
terrorists, criminals and paedophiles who are seeking to cause harm, and the
police and security agencies whose aim is to protect us against these harms. Their
statements imply the need for the legislation, justifying it either by way of
reference to these unlawful actors, or to new and emergent technology as their
enabler. The quote of Theresa May includes both, implicating both cyberspace
and 'those who seek to harm us'. Entirely absent in all of this, is any suggestion of
agency on the part of ordinary citizens whose daily lives are intertwined with the
same technologies being discussed, instead, they are prospective victims of harm,
to be saved by security agencies provided they are given adequate powers to do
so.
In Burnham’s statement quoted above, when he speaks of the 'broad acceptance' for the new law, he makes another important declaration in support of the discourse of need. No more is offered in terms of clarifying who has accepted the need, though it could readily be inferred that he is speaking on behalf of the political establishment, or at least the two major parties. In a similar vein, a Guardian article of the second of November (12, 2015), tells us,

‘All sides in the highly charged debate acknowledge that a new set [of] laws are required to replace the outdated Regulation of Investigatory Powers Act 2000 and the dozens of other statutes authorising the collection of communications data.’

There is no discussion here of which voices should be included in the categorisation of ‘all sides’, though by drawing attention to the 'highly charged' nature of the debate, it can be taken that even opposing voices are in agreement. Of note, in respect of this, is that the voices most commonly quoted in the reporting of 2015 taken as a whole, are overwhelmingly those of government sources, followed by some prominent politicians as individuals, and then human rights organisations such as Liberty, and their individual spokespersons. Clearly absent from the news are any voices which directly involve or represent citizens of the UK, and when 'all sides' and 'broad acceptance' are spoken of, the power of state actors is reinforced at the expense of the ability of the people to meaningfully influence, or even speak of, such affairs. These attempts by sources that are likely to be considered reliable and authoritative, to discursively claim widespread, or even complete acceptance or agreement, suggest a foregone conclusion where no further meaningful dialogue is required.

This is not to say that the IPB and its powers go entirely unopposed in the newspapers, as the proposed need for the legislation is regularly countered by the
inclusion of critical voices, representing a discourse which challenges the stated need.

**Discourse of harms and risks**

In the following excerpt from The Guardian (15, 2015), the legislation is presented as being part of a prolonged effort by the UK government to obtain the powers, picking up from the Draft Communications Bill.

> ‘Rachel Robinson, policy officer for Liberty, said: “It defies belief that the government continues to seek powers so extraordinarily intrusive that none of our major intelligence allies think them acceptable to use on their people.”’

That this is the case, apparently ‘defies belief’, an allegation which suggests the actions of the government are unthinkable. The powers sought in the IPB, though not detailed in any way, are deemed ‘extraordinarily intrusive’, so much so that they are not thought acceptable for use by the agencies of our allies, and in contrast to attempts to position the powers as required only for combatting the ‘them’ of terrorists, criminals and paedophiles, Robinson implies that they will be more extensively used on the ‘people’ as a whole. The statement attempts to position the UK government as alone in their desire for such excessive powers, a strategy that is made regular use of by those criticising the Bill, and which casts doubt on the claimed need.

Several other sources are quoted in the reporting of November, who offer similar criticisms of the powers and the government, while also introducing the idea that risks might arise from the legislation. In The Guardian (27, 2015), Jim Killock of the Open Rights Group says,
“At first glance, it appears that this bill is an attempt to grab even more intrusive surveillance powers...”

which once again describes the powers as intrusive, relaying the sense of an unwelcome or unauthorised forcing in. When it is said that the bill is an attempt to grab these powers, this suggests that the government are moving suddenly or opportunistically in pursuit of their goal. Killock then continues, saying that the Bill, “also gives the state intrusive hacking powers that can carry risks for everyone’s internet security.” Besides the repetition of the allegedly intrusive nature of the powers, we are also told here of the risks to everyone’s internet security that they represent, although details of these risks are not provided. By not making explicit any of the potential risks that are being claimed, an opportunity to introduce greater depth and complexity to the debate is missed.

Potential risks are alluded to in an Independent article (38, 2015), where Anne Jellema, of the Web Foundation, says of the proposed storage of internet connection records,

“‘It will hurt UK businesses, create new vulnerabilities for criminals to attack, and ride roughshod over the right to privacy.’”

Here, this element of the Bill is declared to be a risk in three distinct ways, though in each case it is left for the reader to infer the specifics of how the risk might manifest. When mentioning new vulnerabilities that will be created by the collection of browsing data, no details of what that might mean for individuals is provided, and similarly when the right to privacy is brought into the discussion, though in this case, Jellema implies an act of disregard when she says that it will ‘ride roughshod over the right to privacy’. A statement by Andy Burnham, quoted
in the Mirror (68, 2015), offers unusual detail on the possible risks of the powers in saying that,

“...There will be fears in some communities, particularly the Muslim community, that these powers will be used against them disproportionately.”

This speaks to the perception that the Bill, particularly when understood from a counter-terrorism perspective, might be employed disproportionately against Muslim individuals and communities, and it offers an almost uniquely specific consideration of the possible impact of this legislation.

The voices criticising the Investigatory Powers Bill seek to position the powers, and the government’s desire to legislate for them, as intrusive, as excessive and indiscriminate, and as creating unnecessary or additional risks, and opening up the possibility of their misuse. However, while these sources are used to provide a counterpoint to the discourse of need, the points raised here are challenged in their turn by the introduction of either the discourse of concession, the discourse of oversight, or sometimes both.

**Discourse of government concessions**

A Sunday Times article of the first of November (8, 2015), headlined ‘Curbs on snooper’s charter’, lays out three concessions that the new legislation is offering.

‘Judges will be given the power to veto surveillance requests by Britain’s intelligence agencies after a dramatic concession by the government.’
‘Police demands to obtain routine access to the internet browsing history of everyone in the UK have also been rejected.’

‘David Cameron’s personal threat to ban encryption online to make it easier for spies to access messages has also been abandoned.’

The headline tells us that this legislation will be more restricted than prior iterations - though it still refers to the bill as the snooper’s charter - and the language used in outlining the concessions suggests strong and significant action has been taken. The introduction of judges into the process of approving surveillance requests is described as a ‘dramatic’ concession; the government is said to have ‘rejected’ ‘demands’ by police for access to internet browsing history; and the ‘threat’ by David Cameron to ban encryption has been ‘abandoned’. The rejection of police demands for access to internet browsing data is covered by a number of articles in other newspapers on the same day, where it is variously said to have been ‘banned’, in The Independent (4, 2015), ‘ditched’, in the Mail Online (6, 2015), and ‘dropped’, in The Guardian (2, 2015). Here we are told of a range of active processes, describing a government that is willing to stand up to the demands made by the authorities for more extensive powers, and to back down on some of its plans if necessary.

Although varied spokespersons for the government present the new Bill as concessionary in nature, there is no discussion of who the concessions are for, or why they are felt necessary, though a Sunday Times article (8, 2015) does tell us that,

‘...ministers have abandoned several of the most controversial elements of the so-called “snooper’s charter” in an effort to
persuade Tory rebels and the Labour leadership to back the plans’,

which offers the view that these moves are designed to win over doubtful political opponents. In referring to the legislation as the ‘so-called’ snooper’s charter, the article recognises the suggestion that the Bill enables snooping, but undermines the suggestion with an implied denial.

The Mail Online (6, 2015) provides a different rationale for the concessions when writing that,

‘[Theresa May] is said to have backtracked on the so-called snooper’s charter amid fears the government would be unable to force new laws through parliament because of concerns over civil liberties.’

We read here again of the government’s need to overcome opposition, though it is suggested that the obstacle to passing the new law is the prospect of concerns over civil liberties. Civil liberties is a rather vague term, and, in some contexts, may convey the sense of a liberal indulgence, though here it has created sufficient concern for May to act. The extract also notes that May fears being unable to ‘force’ laws through parliament, which is an unusual way of discussing the attempt to pass legislation in a democracy. It suggests that the use of force would be permissible, in the first place, but also that the government, or the author of a Bill would wish to have it passed in such a manner. Telling a similar story, though in slightly more measured terms, The Guardian (2, 2015; 14, 2015) writes:
‘The climbdown was prompted by concerns that the government would be unable to get the legislation through parliament because of unease of its implications for civil liberties.’

The discussion of concessions tell us that the government is moving away from previous efforts, and is limiting the extent of the powers in recognition of past criticisms. The language around the concessions also states that the proposed powers or plans that are to be dropped, are ‘controversial’ (Mail Online, 6, 2015), or ‘contentious’ (The Guardian, 2, 2015), suggesting issues certain to provoke argument and fierce debate, and by dropping plans of this nature, the government are positioned as reasonable and willing to compromise.

The language of the ‘climbdown’ implies that the government is ceding ground to opponents or critics, and that civil liberties implications are being taken into account, though there is no attempt in these reports to provide more detail on the nature of these concerns, or for whom these implications might be significant. For those already well-informed on the subject, the possible implications are likely to be clear and obvious, but by mentioning them only implicitly, information on the possible harms of the Investigatory Powers Bill is essentially excluded for many readers.

The discourse of concession does also mention the government’s fears or concerns that the legislation may not pass, explicitly in the articles in the Mail Online (6, 2015) and The Guardian (2, 2015), nevertheless, in the same way that further explanation of civil liberties concerns are absent, there is no move to provide context or details on why the government might have fears that the bill will fail to pass.
Questioning these statements of concession, is a claim that such talk may not be what it seems, however, offered by Shami Chakrabarti in The Independent (4, 2015):

“"It’s a traditional Home Office dance first to ask for the most outrageous, even impractical powers, so that the smallest so-called ‘concessions’ seem more reasonable,” Shami Chakrabarti, the director of campaign group Liberty, told the Guardian. “The frantic spinning distracts from the sleight of hand. Where is the judicial sign-off before our private communications can be collected, hacked and tapped? Where is the move back to targeted surveillance and away from the blanket collection of our private data?”"

The Home Office is portrayed as engaged in a diversionary game in order to make its concessions appear significant, something which is also implied to be typical behaviour for the department when it is spoken of as ‘traditional’. Chakrabarti dismisses the concessions as ‘so-called’, implying their denial as such, and goes on to list changes to the bill that presumably would be considered genuinely concessionary. These are formulated as questions, working to reinforce the denial of what the government has conceded, while explicitly offering changes that we might infer Liberty are requesting the government make, in order to address concerns over the scope of the powers. This statement aims to dismiss the changes publicised by the government, and by including some alternative concessions that might be made, Chakrabarti moves to evade possible criticisms of simply condemning the IPB without offering suggestions on how it might be improved. The Mail Online (6, 2015), quotes her further:
“If the authorities need a judge’s warrant before they search my home, why not before the equal or greater intrusion of accessing my private communications? ... Nothing short of this fundamental safeguard should comfort the public or Parliament that this much-anticipated new Bill is an improvement on the past.”

A comparison is made to the requirement for a warrant before conducting a physical search, stating that this ‘fundamental’ safeguard is the only addition which would satisfactorily reduce what she positions as the intrusive nature of the powers covered by Investigatory Powers Bill. The final part of her statement rejects any claim that the new legislation is better than previous attempts, through reference to the ‘much-anticipated new Bill’, a phrase which aims to undermine the assertion that this is an overhauled and improved Bill. This attempt to challenge the discourse of concession appears only once, however, while the discourse itself is persistent, appearing in coverage throughout both 2015 and 2016, where it is often accompanied by talk of oversight, which we will now explore.

**Discourse of oversight and safeguards**

The general talk of concessions soon narrows to focus only on the addition of judicial oversight to the ministerial approval of warrants, which is quickly positioned as being crucial to the passage of the Bill. David Davis - a Conservative MP who, along with Tom Watson of the Labour party, brought a case against the government over DRIPA 2014 - is quoted in the Sunday Times (8, 2015):

““it is to be welcomed that the government is now recognising some of the spectacular impracticalities of its original approach, notably on encryption, and we should welcome the outbreak of common sense, but the fight will be over judicial oversight.””
Davis twice states that the government has made changes that ought to be welcomed, creating broad inclusion of this welcome by use of the pronoun 'we' in the second instance. He contrasts the 'spectacular impracticalities' of previous legislation with the 'common sense' of the current version, a clear indication of significant change which also positions the new Bill as grounded in sense. Davis here reinforces the idea of controversy, and of a contestable process to get the legislation passed, but restricts the dimension of the fight to the sole issue of judicial oversight. With the necessary improvements over past efforts already made, Davis asserts, this one question is all that must be decided for the law to pass, precluding other challenges.

Reinforcing this line of argument, The Guardian (2, 2015; 14, 2015) reports that,

‘Speaking on BBC1’s Sunday Politics show, Davis said: “Actually I don’t think this bill will get through either Commons or Lords without judicial authorisation ... There’s a new consensus on this right across the board. Across the experts, across the spooks, across the parties, across both houses of parliament.”

Davis once again defines this as the only possible obstruction to the passage of the bill, but also tells us of a consensus around this issue, noting the parties constituting this consensus. We see that all political parties and both the House of Commons and the House of Lords are in agreement, along with the experts - a somewhat vague category - and the spooks. It is to be assumed that this is an exhaustive list of those with the authority to speak on the issue, and that any voice not included is therefore unnecessary to account for, by which Davis restricts the sources able to offer a valid contribution to the debate.
While the matter of a judicial role in approving warrants is briefly reported as a divisive one, the issue soon becomes a cornerstone of the discourse of oversight. It is this discourse which features as the most common of all during the reporting of 2015, with widespread mentions in all newspapers between the first and the ninth of November, a period during which the key arguments, as they appear in newspaper reporting were set out.

In the days leading up to the introduction of the draft bill in parliament, the government’s commitment to ensure suitable oversight of the proposed powers is widely reported. This is begun in a Mail Online (6, 2015) article of the first of November.

‘Mrs May told BBC One’s Andrew Marr Show ... “What I am clear about is that there will be in this Bill strong oversight and authorisation arrangements ... What the Bill will do on Wednesday is, it sets a modern legal framework but, crucially, it has very strong oversight arrangements within it. I think it will be world leading oversight arrangements within the Bill. It will be clear and more comprehensive and comprehensible than the previous legislation has been.”

May repeats the word ‘oversight’ on three occasions, leaving no doubt as to the key message being conveyed here. In the first two instances, the oversight within the Bill is described as ‘strong’, a reassuring suggestion that meaningful and robust measures will be applied to limit the powers. She introduces these by stating that she is ‘clear’ about the arrangements for oversight, which gives a sense of certainty to them, but which also implies a transparency, and then by positioning the inclusion of oversight as crucial to the Bill, highlighting that this is a decisive aspect
of the government’s considerations. In her final mention of oversight, May states that she thinks the Bill will be ‘world leading’ in this regard, a rather overstated claim, but one which implies a very high standard. In a link to the earlier implication of transparency, May also says that the new legislation will be clearer and more comprehensible than previous versions of similar laws.

Following the Bill’s presentation to Parliament on the fourth of November, the following segment of a House of Commons statement by May appeared in the Mail Online (42, 2015). Parts of this also appear in articles in The Guardian (30, 2015), The Telegraph (50, 2015), and The Independent (38, 2015) on the same date.

“"I am clear we need to update our legislation to ensure it is modern, fit for purpose and can respond to emerging threats as technology advances ...
But I am also clear that the exercise and scope of investigatory powers should be clearly set out and subject to stringent safeguards and robust oversight.
She argued that the bill will establish ‘world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world.’”

This first addresses the need for the legislation as a means of protection against threats enabled by new technologies, and then goes on to provide reassurance that the powers covered by the act will be subject to stringent safeguards and robust oversight. The proposed oversight of the bill is again positioned as being world-leading, and part of a regime of transparency and openness, using similar re-wording and hyperbole to support the statement.
In this excerpt, Theresa May tells us that she is clear of the need for the powers, but in the same way, she is also clear that protections are needed, seemingly placing the two considerations in a relationship of equivalence. This is useful in representing the bill as having balanced the two needs that are so commonly set up in opposition to one another in discussions of these issues: security and privacy. By asserting that ‘I am clear’, on these points, May also positions herself as an informed source of authority, and makes it appear that all necessary factors have been considered, thereby minimising the need for further discussion.

As it does in May’s statement to the House of Commons, the discourse of oversight often appears in conjunction with the discourse of need, the latter aiming to dispel concerns over the powers. In a statement which brings together oversight and concession, Andy Burnham offers a view of the IPB which echoes that provided by David Davis in advancing the claim that this legislation is much improved.

‘Andy Burnham, the shadow home secretary, welcomed the proposals laid out in the draft bill, praising Ms May for reconsidering plans set out in the ‘snooper’s charter’ and the two-stage accountability process. “We are pleased to see that the Home Secretary has listened,” Mr Burnham said. “This is neither a snooper’s charter, nor a plan for mass surveillance.”’

This is widely reported, appearing in The Independent (40, 2015), The Guardian (30, 2015), Mail Online (58, 2015), Mirror (68, 2015) between the fourth and the ninth of November, and features a categorical rebuttal of the Bill as a snooper’s charter, alongside a denial of it as a plan for mass surveillance, effectively repeating the same claim for emphasis. As with Davis, who suggested that the new legislation should be welcomed, here Burnham does the same, apparently
praising May for having listened and made the necessary improvements. Though Burnham’s statement does not specify what May has reconsidered, or to whom or what she has listened in the meantime, the implication is an acceptance of past criticisms, and concessions made in light of these. The only detail included is that of judicial oversight, positioning this matter as important enough for specific mention. Finally, in offering his remarks here, Burnham also uses ‘we’, once again suggesting consensus on the issue, though amongst an unspecified plurality.

The discourse of oversight is employed to suggest new and improved legislation, to offer assurances that the legislation will be subjected to safeguards that have been considered as carefully as the rest of the Bill, and which will prevent misuse of the powers. Alongside this, and the other discourses already discussed, there are also some notable exceptions which appear during 2015.

**Exceptions to discourses**

The first of these, is when Andy Burnham questions the strength of the oversight arrangements, which is reported by the Mirror on the ninth of November (68, 2015):

‘In a letter to the home secretary, he wrote: “I have now had the opportunity to study your proposals in detail and have taken advice from the shadow justice secretary.

“This has given rise to concerns that the safeguards you are proposing are not as strong as it appeared when they were presented to the Commons.”

“[You] created the impression that both the home secretary and a senior judge would review the evidence. Indeed, you may recall
that I asked you in the House about what would happen if there were a difference of opinion between the two.

“On closer inspection of the wording of the bill, it would seem that it does not deliver the strong safeguard that you appeared to be accepting.”

This is a significant reversal of his previous endorsement of the Bill, and its provision for oversight in particular, though the appearance of this statement in only one of the newspapers selected for analysis means that a limited readership would have known of this, in comparison with the reporting of his supportive statements in four separate newspapers over several days.

Other pieces that appear amidst the reporting of 2015 which are worthy of consideration for their divergence from the general themes used, include an article in The Independent (72, 2015) on the eleventh of November, where the UN’s special rapporteur on privacy, Joseph Cannataci, is quoted, accusing the government of,

‘... an “orchestrated” propaganda campaign through its allies in the media to get the law passed with public consent.

“We’re now at the stage where for the first time we have an absolute offensive,” he said.

Just do a media analysis of the way the British establishment is trotting out news about the law and the need for the law and ask yourselves the question ‘If this is not orchestrated then what is?’”

Cannataci describes a media ‘offensive‘ by the government in its attempt to get the legislation passed, also asserting that the media have been complicit in conveying the government’s chosen messaging. As if to demonstrate his certainty
of this claim, he invites the readership to analyse the media output for themselves, before invoking the ‘British establishment’ and the way in which they are ‘trotting out news’. This implies the repeated use of the same means to explain or justify something, as part of a concerted effort by those represented by the ‘establishment.’ His statement then ends with a rhetorical question which suggests that the media reporting of the issue is an exemplar of ‘orchestrated’ effort, which creates the sense of a coordinated undertaking.

Near to the end of November, after the creation of the Joint Committee tasked with considering the proposed Bill, The Guardian (83, 2015), reports an accusation that Theresa May intends to ‘fast-track’ the legislation.

‘One member of the committee, Lord Strasburger, tweeted: “Ridiculous. Committee scrutinising massive investigatory powers bill given just 2 weeks to hear witnesses. Govt turning it into rubber stamp.”

This is an interesting indication of how social media has become another means of including voices in news, and also demonstrates that even short texts can achieve much. Strasburger talks of the scrutiny to be applied by the committee to the Bill and the relevant witness evidence, highlighting its scope by describing it as ‘massive’, and also noting the insufficient length of time provided for this significant enterprise. He suggests, by use of ‘rubber stamp’, that the government should be understood to be purposefully setting up a process of approval which denies the necessary consideration. The article provides another voice, which reinforces this same theme:

‘Privacy campaigners also voiced alarm. Eric King, of the Don’t Spy On Us coalition of campaign groups, said: “This timetable is
Inhospitable to informed consideration of extraordinary powers. It is a fraction of the time previous versions of the snooper’s charter received, which had just a fraction of the issues to consider.”

While not going so far as Strasburger did in suggesting the cynical exercise of rubber stamping, King’s statement does allege a timetable that is ‘inhospitable’ to the satisfactory consideration of the issues, and highlights what is felt to be the ‘extraordinary’ nature of the powers in the legislation. King also contrasts this legislation with prior versions, claiming that the current Bill will be considered for only a ‘fraction’ of the time allowed to previous legislation which had a ‘fraction’ of this issues, exaggerating the allegedly small amount of time provided through this repetition. It also introduces the ‘snooper’s charter’ label into the discussion, presumably by way of reinforcing this perception of the Bill.

In the final piece of reporting from 2015 to be considered, The Independent (101, 2015), covering laws newly unveiled by the Chinese government, point out their apparent similarity to the Investigatory Powers Bill.

‘Both the UK and China have claimed that the law doesn’t ban encryption, which ensures that messages can’t be read as they pass over networks. But each appears to undercut the technology that powers such security measures. The international community has condemned the new Chinese powers, and President Obama has raised concerns with Chinese President Xi Jinping. Though the UK’s laws have received scathing reviews from Apple and other companies, they have not been publicly criticised by other governments.’
The report notes shared claims by both governments that their respective laws do not aim to ban encryption, followed by a statement that each of the laws ‘appears’ to ‘undercut’ the technology. Though stopping short of an outright claim that the laws will undermine encryption, the writer positively positions encryption as a security measure, and one which might be weakened by the legislation. There are also a number of interesting juxtapositions here. The first, is the drawing of similarities between laws from nations with such theoretically different systems of government, which would naturally be expected to lead to divergent legislative approaches. That this appears not to be the case, it is implied, should be embarrassing for the government of the UK, a democracy.

The second of these is between the political reaction to the two laws, with the Chinese law said to have been condemned by the international community, naming President Obama, specifically, as raising concerns with his counterpart, President Xi Jinping. Meanwhile, it is noted that the UK laws have been spared such criticism, at least publicly. It is not unexpected, given the nature of political diplomacy between countries considered allies, that such criticism would be withheld, though by way of comparison, Apple and ‘other companies’, are reported to have subjected the IPB to ‘scathing’ review. In the case of the UK, a democracy, who should be understood as included amongst the ‘international community’ along with countries such as the USA, there is the implicit right to determine its own affairs without overt interference from other nations, while in the case of China, an outsider to this category, democracies and their heads of state are entitled to cast judgement. While subtly acknowledging these relationships of power, perhaps, the piece ultimately states that the UK law has drawn less serious criticism, thereby suggesting that it there is probably less to be worried about in the IPB.
2016

Moving on to the reporting of 2016, much of its shape is influenced by two key events relating to the legislation. The first of these is the passage of the Investigatory Powers Act 2016, which leads to a recap of the key powers and the discourse of need, accompanied once again by a discourse of opposition and that of oversight. The second event driving coverage, was the ruling by The European Court of Justice that the sort of indiscriminate collection of data enabled by the Act is illegal, and that therefore, the IPA was at least in part unlawful.

Both of these events provide opportunities to include discourses in support of, and in opposition to, the IPA, and while there is much in common with the reporting of 2015 in terms of the prominent discourses employed, the context in which they are employed differs, and some of the rhetoric used is adapted or heightened accordingly. Nevertheless, due to limitations of space, discourses which are felt to closely resemble counterparts from 2015, will not be further analysed at this stage, though commonalities will be considered in the discussion.

**Discourse of insufficient opposition**

The Act was passed by the House of Lords on the sixteenth of November 2016, and reporting from that point through until early December included criticism of the IPA, along with claims that the legislation was not met with sufficient opposition. A Guardian article of the nineteenth of November (87, 2016), headlined, “Extreme surveillance’ becomes UK law with barely a whimper’, begins:
‘A bill giving the UK intelligence agencies and police the most sweeping surveillance powers in the western world has passed into law with barely a whimper, meeting only token resistance from inside parliament and barely any from outside.’

The description of the powers of the IPA as ‘extreme’, and as unsurpassed in the western world, certainly aims to allow no doubt as to the severity of the issue under discussion. This excerpt frames the Act as something that might inspire shame, both because amongst the ‘western world’ (a proxy for democracy and its associated qualities), the UK alone has seen fit to legitimate such powers; and also on account of it passing so easily. The headline and lead paragraph state that ‘barely a whimper’ was raised in objection, claiming that only token resistance was offered by parliament, and barely anything from anywhere else. As has been noted in the analysis of the 2015 reporting, resistant voices were present, or at least acknowledged in the discussion, though certainly far outweighed by government voices. So while the article seems to lament a lack of resistance, newspaper discussion of the draft IPB can hardly be claimed to have consistently called for, or supported such a thing.

The article continues,

‘The security agencies and police began the year braced for at least some opposition, rehearsing arguments for the debate. In the end, faced with public apathy and an opposition in disarray, the government did not have to make a single substantial concession to the privacy lobby.’
beginning with the suggestion that the arguments to be used in the debate had
been rehearsed by security agencies and police. To prepare for debate is sensible,
but the use of rehearsal here implies a parallel with a public performance of some
type, specifically with acting and the need to learn and practice a prepared script;
while also suggesting arguments planned more for the goal of consistency than a
genuine engagement in dialogue. The report then marks public apathy and a
disorganised political opposition as reasons for the government being able to
pass the legislation without any ‘substantial concession to the privacy lobby’,
though especially with regard to the alleged apathy of the public, this is again an
issue where compelling newspaper reporting might have been able to make an
impact.

Coverage in other newspapers seeks to explain the passage of the Act in a
number of ways. In the Financial Times (81, 2016), of the twentieth of November,
we read the following:

“In 20 years that I’ve been dealing with surveillance policy in this
country I have never seen a more docile parliament,” said Gus
Hosein, executive director of the non-profit organisation Privacy
International, regarding the bill’s passage.

This very directly attributes responsibility for the passage of the Bill to a ‘docile
parliament’. To reinforce the credibility of his suggestion of a submissive, or at
least obedient parliament, Hosein hints at his experience in dealing with
surveillance policy, and by detailing the length of this background, the alleged
docility of this particular parliament is heightened. The implication is, of course,
that a more active, attentive parliament would have prevented the law from
passing, which we presumably ought to understand as being not just a desirable
outcome, but the only possible outcome if parliament had functioned properly.
We read not only of the implicit disappointment that the Bill has passed, then, but also of the malfunctioning of the political system in allowing it to happen.

The reporting around this time offers an alternative reason for the bill having passed, first in the Telegraph of the twenty-eighth of November (76, 2016), where it is said that,

‘Opponents of the Investigatory Powers Bill believe that it has barely been scrutinised due to the fallout from June’s EU referendum.’

The opponents in question are not specified, and while the UK referendum on whether or not to leave the EU, is claimed to be responsible for the inadequate attention given to the Bill, there is no attempt here to attribute responsibility for the scrutiny it seemingly deserved, beyond the allusion to ‘fallout’ from the referendum, which might vaguely suggest a political connection. It is notable, too, that this claimed causality is described as a ‘belief’ of opponents, clearly positioning it as an opinion, and not backed up by proof. A Guardian article of the following day (63, 2016), provides a more explicit view of this possibility, quoting Jim Killock of the Open Rights Group:

‘He said the legislation was debated and passed while the public, media and politicians were preoccupied with Brexit’

This excerpt does not directly attribute responsibility either, but the legislation is said to have been debated and passed during a widespread preoccupation with Brexit, specifically on behalf of the ‘public, media and politicians’, who, presumably, might have otherwise prevented this from happening. It echoes Hosein’s statement considered earlier, in positioning this sequence of events as a
failure of proper function, though here the implied responsibility goes well beyond parliament. The inclusion of the media seems a reasonable one, given their perceived role as the fourth estate of society, though the power of the public to have influenced events is questionable, especially in light of their marginal inclusion as agents of any sort in the media debate.

Overall, during 2016, there is a much more notable left-right political split between newspapers and their coverage, with The Daily Mail, The Times, and The Telegraph reinforcing the discourse of need, and that of oversight - based on the same themes and language of threats and security as during 2015 - while The Independent, The Guardian, the Mirror and the Financial Times, though still including the same discourses in support of the government position, also include more overt criticism of the Investigatory Powers Act. This split will be demonstrated, and discussed, through the analysis of three final discourses.

**Discourse of privacy and rights**

This discourse, which was tentatively voiced to an extent during 2015, is slightly more prominent in 2016, but more importantly, is more specific in some of its criticisms. An example of this can be seen in the Financial Times (81, 2016).

"MPs who voted against the bill during its draft stages, such as SNP MP Joanna Cherry, said they believed that “in order to protect civil liberties, surveillance should be targeted, with warrants from courts that ensure they are focused, specific and based on reasonable suspicion”.

However, the bill allows bulk data collection, dashing the hope that surveillance will have to be targeted and “based on reasonable suspicion”. Mr Hosein said: “No [western] government
anywhere has passed such laws on bulk collection and bulk hacking because it’s mass surveillance. Time and again, courts have ruled this is unlawful and unacceptable in a democratic society.”

The first source included here, MP Joanna Cherry, lays out some requirements that she, along with other MPs opposing the Bill, believed to be necessary in order for the legislation to ‘protect civil liberties’. The statement describes a need for ‘targeted’ surveillance, and the use of warrants to ensure practices that are ‘focused, specific and based on reasonable suspicion’. The adjectives used here demand clear, defined procedures and processes, which suggests the Bill’s use of the opposite. To reinforce this sense, the statement by Hosein, of Privacy International, bluntly defines the laws as ‘mass surveillance’, repeating the use of ‘bulk’ to describe the powers, and noting previous court rulings against these practices. This portrays the opposite of the requirements outlined by MPs. Hosier also situates the laws as undemocratic, using the evidence of the court rulings, and notes once again that the UK government is alone amongst western nations in having passed such laws; not an exceptional state of affairs that we should be proud of, or happy about.

A third critical voice extends upon some of these themes in a statement that variously appears in articles in The Independent between the twenty-ninth and thirtieth of November (67, 2016; 59, 2016), and in the Mirror on the twenty-ninth (70, 2016).

“It’s a sad day for our democracy as this Bill - with its eye-wateringly intrusive powers and flimsy safeguards - becomes law,” said Bella Sankey, the group’s policy director.
“The Home Secretary is right that the Government has a duty to protect us, but these measures won’t do the job. Instead they open every detail of every citizen’s online life up to state eyes, drowning the authorities in data and putting innocent people’s personal information at massive risk. “This new law is world-leading - but only as a beacon for despots everywhere. The campaign for a surveillance law fit for the digital age continues, and must now move to the courts.”

Sankey invokes the same undemocratic state of affairs evidenced by the Bill’s passage, exaggerating both the extent of the powers, and the insubstantial safeguards applied to them. She then uses what is presumably a prior claim by the Home Secretary that the laws help to fulfil the government’s duty to protect the nation, and contrasts this with her own counter claims of what the law will actually accomplish. These include several specific risks of surveillance, notably the risk inherent in storing large amounts of data, and the intrusion into everyone’s privacy enabled by the powers. She then employs the 2015 claim by Theresa May that the law is ‘world-leading’, turning this around with her hyperbolic assertion that they should only be considered such in the example they set for ‘despots’, implying that only despots should be using these powers. The final part of the statement contrasts a desired law, ‘fit’ for the digital age, with the current law that is presumably therefore unfit for purpose, and states the necessity of taking this effort to the courts, demonstrating a willingness to challenge the government, and also a seeming confidence that this step will represent a decisive and favourable outcome.

A final piece, featured in The Times (62, 2016), and mentioned by The Independent (54, 2016) offers Tim Berners-Lee speaking on the newly passed IPA.
‘Wide-ranging surveillance powers that became law yesterday have no place in modern democracy and will ride roughshod over privacy, according to the inventor of the world wide web. Sir Tim Berners-Lee described elements of the new legislation as “disproportionate” and said that the strengthening of snooping powers for police and security services undermined people’s fundamental rights.’

The theme of undemocratic powers is again used in talking about the law, and although Berners-Lee uses more moderate language when describing aspects of the IPA as 'disproportionate', this still offers a view of the powers as being comparatively excessive. The statement concludes with the assertion that the powers undermine fundamental rights, which go unspecified, though the mention of snooping powers quite clearly indicate an intrusion against privacy. A statement by Tim Berners-Lee, noted as the inventor of the world wide web, should presumably also hold some weight in terms of his understanding of the technology, and he could also be assumed to be less politically invested in the debate around the laws.

Following in the aftermath of a ruling by the European Court of Justice, deeming the indiscriminate retention of communication data to be unlawful, two discourses emerge, the first of which is a discourse of need, which makes more explicit use of the threat of terrorism to justify this need, than was present in reporting of 2015.

**ECJ ruling: discourse of need**

This discourse is also more limited in its use, featuring more in what might be perceived as right wing newspapers like The Times, The Telegraph, and The Daily
Mail. As an example, The Times, of the twenty-second of December (23, 2016), states that,

‘Weakening surveillance laws in response to a European court ruling that they are excessive would leave Britain at greater risk of a terrorist attack, former spy chiefs have warned.’

The piece mentions the ‘greater’ risk of terrorist attack that would be posed by altering the IPA to satisfy the ruling, implying both that this new law is a certain preventative, which stands to be weakened, and that there already exists a significant risk of a terrorist attack in the UK. This is served as a warning by ‘former spy chiefs’, who are to be presumed to have good knowledge of such risks, and therefore well positioned to accurately and authoritatively speak on such matters. In a similar way, The Guardian (26, 2016), says that,

‘Lawyers for the UK government maintained that intercepted communications have been at the heart of every terrorist case investigated by police and the security services in recent years.’

As sources, such lawyers might again be presumed be party to accurate and reliable information, and which is available only within suitably selected circles. Therefore, their assertion that communications data have been central to terror investigations of recent years, should be taken seriously. It is implied that this data was intercepted through means comparable to those allowed by the IPA, though no detail is given, nor is any evidence offered for the ultimate accuracy or usefulness of this intercepted data to the resultant investigations; however, there is the sense that the continued availability of such data is essential to security.
In a Telegraph article (22, 2016), the exceptional severity of this continued threat, especially as it is enabled by technology, is used to support an appeal that expectations of privacy be lowered.

‘But while in normal times, any efforts by the agencies of government to pry into our lives should rightly be resisted, these are not normal times. The security threat posed by terrorists who use new mass communication methods to plot their attacks makes some snooping inevitable. The challenge is to strike the right balance between security and privacy; and that is a job for parliament.’

By situating us outside of ‘normal times’, the usual rightful expectation of privacy is invalidated, and we instead ought to accept the inevitable need for ‘some snooping’, though in exchange for our security. In place of any attempt to explain the connection between a power such as the unwarranted and bulk collection of data on every UK citizen’s Internet use, and the prevention of terrorism, the statement relies upon the fear conjured by allowing the plotting and attacks of terrorists. It is also notable that no alternative preventative measures are allowed into the discussion, and that seemingly it is parliament alone who should be allowed the duty of deciding how the balance between security and privacy be achieved, despite arguments that such a balance is a false construction to begin with.

In the same article (22, 2016), this exclusive role for parliament is repositioned slightly as relating to matters of the ‘security of the realm and its people’, with the use of ‘realm’ and later use of ‘sovereignty’ presumably intended to stir nationalistic pride in the monarchal nature of the UK, and a rejection of interference by the outsiders of the ECJ. It begins, however, by noting that,
’Privacy campaigners have hailed the ruling as a landmark in the fight to stop government’s keeping information on their citizens. They have a good argument and many of their points were taken on board in the drafting of the legislation. But in the end the security of the realm and its people is a matter for the Government and parliament, not the European Court. Now that we are leaving the EU here is one area of sovereignty that can be reasserted.’

Privacy campaigners are here acknowledged to have good points to contribute to the debate, though the government is said to have incorporated many of these into the legislation, presumably by way of the ‘concessions’ mentioned in the reporting of 2015. In the final statement, any debate over the legality of the IPA, or consideration of the nature of its powers is put aside, however, giving way to a declaration of satisfaction that, having opted to leave the EU, the UK may once again be free to determine its own affairs. While being a somewhat tangential argument, it could also be intended to function as a way of gaining support for the IPA, by leveraging anti-EU sentiment amongst readers.

The ruling of the ECJ did not provoke an entirely critical response from UK newspapers, however, with claims being offered in support of a countervailing discourse: that of justice, which we will briefly explore in conclusion.

**ECJ ruling: discourse of justice**

Much of this was published in the Financial Times, The Guardian and The Independent, highlighting the more evident political split in the 2016 coverage
that was mentioned earlier. A statement from Tom Watson, one of the MPs who took the government to court over the Draft Communications Bill, offers a concise interpretation of the substance of the ruling, which was reported over the course of two days in The Independent (33, 2016; 20, 2016), the Mail Online (36, 2016), the Mirror (38, 2016) The Guardian (26, 2016), and The Financial Times (24, 2016),

“Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe, but no one would consent to giving the police or the Government the power to arbitrarily seize our phone records or emails to use as they see fit.”

Beginning with the inclusive claim that most of us would accept ‘occasionally’ compromising our privacy in the name of safety, which relies once more on the principle of having to balance the two as opposites, Watson then portrays the IPA as going far beyond that acceptable measure. He strongly suggests that the legislation improperly enables police and government to take hold of our communications, however and whenever they wish, and for whatever end. With the IPA positioned this way, it is clear that the ECJ ruling against the law should be considered appropriate, reasonable and just. This sentiment is supported by a further statement which also appeared in the The Independent (33, 2016; 20, 2016), the Mirror (38, 2016) and The Guardian (26, 2016):

‘Martha Spurrier, director of Liberty, which supported the MPs in bringing the case, said: “Today’s judgement upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant.”’
Spurrier, similarly to Watson, gives a sense of the IPA as excessive and improper, and of the ECJ judgement as a further demonstration of this. The ruling is very much positioned as a victory, and once which is said to support the rights of British citizens against what are presumably the major harms enabled by the Act: the use of surveillance both without warrant, and absent reasonable suspicion.

The final excerpt comes from an article in The Telegraph (21, 2016) of the twenty-second of December, which offers a significantly different take on the judgement:

‘There are solid arguments against mass surveillance, from the risks it poses, to the proper boundary of state actions. A healthy mistrust of governments should be enough to curtail their appetite for expansionist and intrusive policies. A well-founded concern for the types of leader that the democratic process can sometimes favour should be enough to persuade anyone that the democratic state should only go so far.’

Here, the primary risk of mass surveillance and any laws enabling such powers, is said to be the almost inevitable seeming ‘expansionist and intrusive policies’ that governments have an appetite for. The concern over surveillance is much more positioned as part of a general concern that government tends to overreach, rather than specific harms that surveillance might pose to individuals or society, though it nevertheless presents a useful reminder that the democratic state should be limited in its capabilities against its citizens.
Discussion

This section will offer a discussion of the discourses analysed, relating the key issues here, to existing research on the newspaper industry and its practices, and from the field of surveillance studies. It will also reflect on how effectively the research has been in answering the question it posed, the limitations of the research, and finally, the possibilities for future research along with any other implications.

The prominent discourses in the reporting of 2015 are all present from near the beginning of the month, and they quickly coalesce to help establish a general form for the discussion, which, notwithstanding exceptions, is remarkably consistent across the two month period examined. There are three supportive discourses, advanced primarily by sources from within the government (Greenberg and Hier, 2009; Tiffen et al., 2014; Keuhn, 2017), which work together, often in combination, to present the IPB as necessary but also as having taken account of the possible risks of the powers it enables, and the mistakes of previous legislation. These are: ‘need for the powers’, ‘government concessions’ and ‘oversight and safeguards’.

Each of these enjoy widespread inclusion across all of the newspapers examined, and though they predominantly feature during a concentrated period of reporting in the first two weeks of November, 'need' does make appearances through until the end of December, and during 2016 too. These discourses are often countered by 'risks and harms', which also features in newspapers across the range, and mostly during the reports of early November, but tends to be given less prominence in reports - by way of appearing later in the piece - or less space (Thorsen, 2017). It is also mostly placed in opposition to more than one of the supportive discourses mentioned, and though it is clear that organisations such as
Liberty and Privacy International were attempting to raise concerns, the imbalance of reporting functioned to diminish the sense of this (Ekman and Widholm, 2015; Thorsen, 2017).

Articles appeared in a range of different sections of the newspaper, most commonly under news, but also in politics; science; and technology. The reporting as a whole was rather homogenous (Curran and Seaton, 2010; Conboy, 2011), and this was evidenced in the similarities between how these sections reported the issues, with some exceptions to be found amongst 2015 articles featured as ‘politics', where more broadly critical reporting or exceptions to discourses could be found (van Dijk, 1988).

In 2016, significantly more space in the reporting is given to criticism of the legislation, though once again it is generally placed against a fuller discourse of need. It is also noticeable that something of a split occurs in 2016, aligned to the perceived political leanings of the newspapers, with those of the right consistently offering the discourse of need, while the newspapers of the left include more in the way of the discourse of privacy and rights. Nevertheless, what is noticeable at a general level, is the remarkably narrow range of themes running through the reporting of all newspapers, which are fed into by a set of largely shared ways of constructing the legislation for readers (Greenberg and Hier, 2009; Tiffen et al., 2014; Keuhn, 2017).

What is noticeable during both years, is that there is almost no discussion of the possible risks that surveillance practices might hold in a broader, social sense, where more of the serious harms might be found (Hughes, 2015; Lyons, 2015; Bernal, 2016; Stahl, 2016). Instead, the risks of surveillance mentioned are individual harms, which are balanced against issues of collective security or safety (Lyon, 2015). Another issue which might reasonably have received more nuanced
coverage is that of the technologies that are an essential part of surveillance practices (Barocas et al., 2014; Mittelstadt et al., 2016). Though encryption does enter the discussion, it is not provided much in the way of context, and the algorithms and other software enabling contemporary surveillance go unmentioned, despite representing a potentially rich means of questioning the validity and ethics of surveillance (Palm, 2014; Mathiesen, 2015).

The sources who are quoted or referred to within articles play a significant role in defining the breadth of views offered on an issue (Richardson, 2007; Mautner, 2008; Broersma, den Herder and Schohaus, 2013; Tiffen et al, 2014). It is highly relevant to this, that in both 2015 and 2016, government sources, either in the form of individual politicians, unspecified governmental or departmental sources, or entire departments - such as 'The Home Office' - represent the most frequently included 'actors' (Greenberg and Hier, 2009; Tiffen et al, 2014; Keuhn, 2017; Thorsen, 2017; Wahl-Jorgensen, Bennett and Cable, 2017). In 2015, these official sources taken collectively, amount to almost double the total of all other sources included in the reporting. In 2016, the government sources are still far and away the most commonly heard from, though their collective total is slightly below the number of all other sources, offering a more balanced range.

Articles do provide critical voices, and in greater number and prominence during 2016 than 2015, but it is interesting to note that these critical voices are variously introduced as 'campaigners', 'privacy campaigners', 'civil liberties groups', or 'critics' (Potter and Wetherell, 1987; Carvalho, 2008), while those offering support to the law are never similarly labelled as 'supporters' or 'surveillance campaigners'. This identifies those who are criticising or opposing the law as having a clear motive to speak, while on the other side of the discussion, there tend to be government sources or other actors, nominalised only by name and official role (Richardson, 2007; Fairclough, 2015), and without the implied motive. Offering this
neutrality to those speaking for the law, reinforces their existing authority as sources, and orientates the discussion as if the passage of the legislation is the expected and normal course of things. Meanwhile, those speaking for Liberty, or Privacy International, for example, who begin from a less authoritative position, have to attempt to persuade readers, effectively owning the burden of proof in the debate.

During both 2015 and 2016, the range of sources called upon to inform the discussion of issues is limited. It is already noted that government dominate, and that spokespersons from human rights and privacy organisations have a voice, though alongside these two, the only other sources included in the reporting are representatives of police and security agencies, and technology companies and organisations, or individuals with a presumed place to speak on technology, such as Tim Berners-Lee.

Entirely excluded from the discussion, then, are voices from perspectives including academics and researchers in the fields of technology and surveillance, and the citizens of the UK (Conboy, 2011; Lischka, 2016; Keuhn, 2017). Though it is admittedly difficult to credibly include individual public voices in reporting on issues such as this, research and polls have been conducted on people's understanding of privacy issues and their attitude towards surveillance (Bakir et al., 2015; Dencik and Cable, 2017), which speaks directly to the questions around legislation such as the IPA. In addition to being excluded as sources, the reporting also lacks any meaningful attempt to imagine active citizen roles that might be taken in relation to the issues at stake, even though a large part of the population is actively engaged in using the technologies and platforms which enable the planned surveillance powers (Lyon, 2007; Bennett, 2011; Lyon, 2015). This absence of agency leaves the citizen as a passive observer (boyd, 2011), outside of the debate and powerless to act, when arguably, the newspapers ought to be
offering engagement and some sense of inclusion (Conboy, 2011; Fairclough, 2015).

Having discussed the discourses and sources that are present in the reporting, as well as noting those that are absent, it is useful to consider what impact these factors might have on the understanding of the issue that can be gleaned from newspapers. Firstly, it is evident that the reporting of the newspapers, taken as a whole, is quite homogenous in terms of the framing of issues and the sources used, both in terms of the general sense of reporting, and with regard to the fact that it is very common to find the same statements or speeches included across reports in multiple newspapers on the same day, or within a day or two.

Regardless of the newspaper being read, generally speaking, the broad shape of the discussion is presented in a similar way, with even the shifts between discourses taking place in clearly identifiable steps across the range of reporting. While the newspapers do present enough criticism of power to appear oppositional, the overall shape of reporting certainly seems to favour the voice and view of power and authority. This homogeneity of reporting, and its shaping of the discussion especially in 2015, cannot help but have exercised power over the public perception of the IPB, and the level of understanding of the important issues at stake (Fowler, 1991; Mautner, 2008; Philo, 2008; Jäger, 2011; Bednarek and Caple, 2012; Matei, 2014; Fairclough, 2015).

While in 2016 the newspapers do offer more of a critical take on the IPA and its implications, particularly amongst the newspapers with a more left leaning political perspective, it feels like it appears too late in the discussion to be particularly useful. Although subsequent events (Travis, 2017) have demonstrated how crucial it is to continue the debate around these issues (Mathiesen, 2015), it would arguably have been much more constructive to include a more robust critical side
in the discussion during the consideration of the legislation, and before its passage into law. Cynically, it is tempting to view the emergence of more critical reporting after the law had passed, as an effort to appear to be fulfilling the often noted watchdog role (Curran and Seaton, 2010; Matei, 2014; Lischka, 2016), though at a time when less is at stake for reporters. (Matei, 2014)

In the meantime, newspapers with a more right leaning viewpoint tended to offer much more in the way of defence of the need for the IPA, especially when its lawfulness was challenged by the ECJ ruling. It is notable that such division along political lines, which is not uncommon (Fowler, 1991; Curran and Seaton, 2010), is present in the reporting of 2016, but only makes exceptional appearances during 2015. Though the issue does not strictly adhere to any partisan split, it nevertheless seems significant that a division between newspapers was not more in evidence throughout.

In turning to an evaluation of the research, it will be helpful to first reconsider the research question that was to be examined. In this case, the enquiry was the extent to which the reporting of national UK newspapers adequately provided a range of perspectives on the issues surrounding the Investigatory Powers Act 2016 in its various stages, expressed by a diverse range of sources. It also aimed to identify any consistencies in the reporting, both between different newspapers and across the two periods in time, as well as any notable differences.

When evaluating the extent to which the research has been successful, there are a number of factors that are useful to consider. Firstly, in analysing the reporting, an attempt was made to extract and present the discourses which were generally most prominent, but more importantly, functioned to give a coherent sense of the shape of the reporting as a whole, which was the overall aim. In addition to this, in an effort to faithfully portray the quality of the reporting, it was also necessary to
acknowledge and include notable instances of discourse which were unusual or exceptional.

Similarly, the need to examine the data for consistencies and differences, between sources and across time, required that a balance be maintained between presenting sufficient detail to demonstrate such relationships, while also retaining a focus on the objective of viewing the reporting as a complete object of research. It is hoped that the research has somewhat satisfactorily accomplished these balances, presenting a set of discourses in a sequence and in relationship to one another that represents the reporting when considered as a whole, evidenced by excerpts appropriate to the task of demonstrating the meaning and consequences of the discourses.

Limitations

There are, of course, limitations to the research which must be acknowledged, some of which are a result of the practical constraints of the time that can be allowed and the space available, while others are methodological in their nature. With regard to the practical limitations, while the final data for analysis was drawn from only two points in time, around the 2015 introduction of the draft Bill and the 2016 passage of the Act, the original intention was to gather data from a number of additional points in the intervening period. This would have allowed for the examination of reporting set in a broader range of contexts, which may well have offered alternative discourses to those identified and discussed here. The additional data would have also provided the opportunity to construct a fuller view of the reporting across time, as well as the relationship between newspaper coverage and other key events entering the news cycle.
However, analysis of more data would have increased the time required to complete the study, and there was a strict deadline to be met. An increase in data would have also demanded more space for a proper analysis, and the discussion of findings, and here the requirements of the project were also somewhat strict. These limits certainly played a part in guiding the choices behind the data gathering, and the inclusion of particular discourses in the analysis, although such decisions were ultimately driven by factors relating to the data: for example, collecting data from the two periods where reporting was at its peak; and using the most common discourses to form the basis of the analysis, along with some significant exceptions.

It should be noted that another researcher may have selected a different set of articles to use as data for analysis, or identified different discourses as being dominant in the reporting, and in the same way, the excerpts selected to illustrate the analysis here may not necessarily be chosen by another. The analysis in no way represents an exhaustive discussion of the issues discussed in, or absent from, the reporting, but rather provides one possible means of addressing the research question. It is also useful to bear in mind that while the analysis can examine the detail of what is said, and the way in which it is said, it can only theorise when attempting to explain why any particular statement was made, or indeed included in the reporting, using the available evidence as the basis for such theory.

Finally, it would have been helpful to include an examination of the broader information landscape during the time taken for the legislation to move from draft to law, including news from broadcast and digital only sources, in order to better appreciate the possible range of public perception and understanding of the issue. It is acknowledged that newspapers, while representing a significant source of information to the general public, are just one of many contemporary sources.
Implications

In keeping with the use of Critical Discourse Analysis as the methodology for the research, it was hoped that some action might be identified as a result of the research, which could be taken to address the balance of influence held by newspapers over how issues are perceived and discussed. Though echoing existing calls to provide some skills for info lit, in respect of the contemporary information landscape, this is a demand that seems all the more pressing, and in need of application at a younger age, and to the broadest possible audience.

Those with any stake in the quality and integrity of information available, should also be seeking to include their voices in the debates that take place around relevant issues, especially at a time where it is clear that there are critical questions that need to be answered in this arena.

With regard to future research implications, there are ways into a broad range of topics from this starting point, including research on the functioning and influence of other forms of mass media, more specific exploration of the effects of surveillance practices on information behaviour, and a whole array of considerations relating to the ethical implications of algorithms and technology as they apply to the future shape of the information landscape.

It is hoped that the research has helped to further demonstrate that newspaper reporting is very much a shaped and selective product, whose output is not a neutral distribution of facts, and that the evaluation of its language can help to illustrate the ways in which it functions. It is also hoped to have brought something new to the discussion of surveillance, especially as it might be understood and engaged in by the public.
Reflective statement

The origins of this research stem in part from a personal conversation about the nature of government surveillance in the UK today, and more specifically, whether this ought to be considered to pose any potentially meaningful risks to the population in general. This discussion led to a clear recognition that the subject was a divisive one, which in turn provoked an urge for further investigation.

After some consideration of how best to research the subject, the question eventually aligned with ideas of the public sphere, by way of Habermas (1989), and the contemporary discussion over fake news and the problems associated with identifying the veracity of online information, which links in deeply with persistent questions of information evaluation and critical appraisal, whose relevance to all sources of information should be maintained.

In this light, the quality of newspaper reporting as a source of shaping public understanding continues to be highly relevant, and while critics have long pointed out the failings of newspapers to provide adequate breadth on important issues, and the problems associated with an increasingly narrowing range of press ownership, it is of clear and contemporary value to attempt to spread an understanding of the need to evaluate information, as well as making explicit some of the ways in which this can be achieved.

While considering the possible methodology, it was from a wish to produce potentially actionable results that the decision to use Critical Discourse Analysis was reached, and while the research is of course only a partial examination of a wide-ranging subject, it is nevertheless hoped that it contains some fruitful findings that match its aims and objectives.
When embarking upon the analysis of the data, it soon became apparent that there is no clear guide to the process of analysing discourse, which entailed a lengthy period of sometimes frustrating reading and re-reading of the data, in tandem with a few key texts on CDA and discourse analysis more broadly, before I was able to satisfactorily identify a way into the data that made sense. Beginning with all of the broad constructions of the legislation, it was then possible to begin distilling the data, identifying the key discourses and actors, and the examples which highlighted the chosen reading of the data. Throughout the analysis, and even the writing up, I sometimes feared that the selection making process was prone to arbitrariness, though I do feel that a good attempt to answer the research question has been made, based on a coherent selection of discourses, and excerpts which suitably demonstrate these, while also offering a faithful representation of the shape of the reporting as a whole.
Conclusion

This research aimed to examine the newspaper reporting around the Investigatory Powers Act, through its journey as draft legislation to enacted law, with a view to interrogating the quality of the discussion made available to the public, on this important issue. It aimed to do so, through analysing the construction of the language used in the reporting alongside considerations of overarching discourse and the inclusion or exclusion of sources in the debate.

I have demonstrated the way in which select dominant discourses were universally employed in the initial reporting of 2015, to construct an evolving sense of the need for the legislation and the concessions that had been included in the new Bill, with the lesser inclusion of a narrow range of critical voices. I have also shown how the newspaper reporting of 2016 exhibits something more of a division in discourses, and though the need for the legislation is still broadly included, more prominent criticism is evident, and the balance of sources is more even, though still limited in its range.

As such, particularly during the debate over the draft bill, the breadth of perspectives on offer to the public is demonstrably limited, supported by way of a narrow range of voices. Overall, the reporting offers a rather too homogenous depiction of the arguments around such legislation and powers, and does very little by way of encouraging or enabling the public to actively engage with the issues.
References


Appendices

1. Articles for 2015

Results

1. Online surveillance bill 'will fall without judicial oversight'; Former shadow home secretary David Davis says investigatory powers bill will have to let judges' authorise warrants The Guardian, November 1, 2015 Sunday 6:19 PM GMT, POLITICS, (795 words), Frances Perraudin

2. Online surveillance bill 'will fall without judicial oversight'; Former shadow home secretary David Davis says investigatory powers bill will have to let judges' authorise warrants The Guardian, November 1, 2015 Sunday 3:45 PM GMT, POLITICS, (797 words), Frances Perraudin

3. EU referendum: Theresa May could lead 'Out' campaign after Nigel Farage says he'd be 'delighted' if she took the role; Survey suggests she would be the public choice to take charge of the 'Brexit' campaign Independent.co.uk, November 1, 2015 Sunday 11:59 PM GMT, UK POLITICS, (868 words), Nigel Morris

4. UK Government plan to ban WhatsApp dropped, as Theresa May abandons many of proposed new powers for spies; Campaigners say that climbdown is 'spin', to allow Government to sneak in many more intrusive powers Independent.co.uk, November 1, 2015 Sunday 11:19 AM GMT, NEWS, (909 words), Andrew Griffin

5. Theresa May 'backtracks over snoopers' charter' but spies STILL want to be able to access your internet records MailOnline, November 1, 2015 Sunday 8:13 PM GMT, NEWS, (1299 words), SAM TONKIN FOR MAILONLINE

6. Theresa May backtracks over snoopers' charter and drops plans to let police and spies see your internet browsing history MailOnline, November 1, 2015 Sunday 3:21 PM GMT, NEWS, (1132 words), SAM TONKIN FOR MAILONLINE

7. New internet snooping law will NOT ban WhatsApp and Snapchat: Details of the revamped snooper's charter have emerged and the government have backed down on plans to restrict online encryption mirror.co.uk, November 1, 2015 Sunday 8:36 AM GMT, NEWS, UK NEWS, (376 words), By Mikey Smith

8. Curbs on snoopers' charter; Snoopers' charter is needed, police insist The Sunday Times (London), November 1, 2015 Sunday, NEWS; Pg. 1,2, (908 words), Tim Shipman

9. NOW APPS USED DAILY MAIL (London), November 2, 2015 Monday, (649 words)

10. Investigatory powers bill to face strong opposition FT.com, November 2, 2015 Monday 7:23 PM GMT, (873 words), Sam Jones, Defence and Security Editor

11. Nobody is listening to the UK's anti-surveillance campaigners FT.com, November 2, 2015 Monday 5:49 PM GMT, (785 words), Janan Ganesh
12. Theresa May faces fight over web browsing access; Labour and Nick Clegg prepare to contest snooper's charter plan to give intelligence agencies more powers. The Guardian, November 2, 2015 Monday 8:43 PM GMT, WORLD NEWS, (751 words), Patrick Wintour Political editor

13. The Guardian view on the draft investigatory powers bill: snooper's charter 3.0; The debate is getting lost in detail, amid 'concessions' on proposals that were never serious. But at core this week's draft legislation is about legitimising bulk data collection. The consequences are chilling. The Guardian, November 2, 2015 Monday 7:56 PM GMT, COMMENT IS FREE, (981 words), Editorial

14. Lord Carlile criticises proposals for judges to approve spying warrants; Former reviewer of terrorism legislation says it would be glib to require judicial oversight of applications by security services to intercept communications. The Guardian, November 2, 2015 Monday 6:13 PM GMT, UK NEWS, (872 words), Frances Perraudin

15. New law to tell internet service providers to retain browsing data; Lobbying by police ahead of investigatory powers bill suggests ISPs will be required to keep data for 12 months. The Guardian, November 2, 2015 Monday 4:57 PM GMT, LAW, (861 words), Owen Bowcott, Aisha Gani and Alex Hern

16. Lord Carlile criticises proposals for judges to approve spying warrants; Former reviewer of terrorism legislation says it would be glib to require judicial oversight of applications by security services to intercept communications. The Guardian, November 2, 2015 Monday 10:20 AM GMT, UK NEWS, (783 words), Frances Perraudin

17. Grant the spies their powers - but force them to speak up; When a tiny light is shone on MI5 and MI6, as in the Commons' hearing two years ago, there is no threat. Independent.co.uk, November 2, 2015 Monday 6:04 PM GMT, VOICES, (1057 words), Steve Richards

18. Now apps used by jihadi recruiters won't face ban: New bill will not stop encryption as process is vital to all communications such as online banking. MailOnline, November 2, 2015 Monday 12:55 AM GMT, NEWS, (690 words), DANIEL MARTIN CHIEF POLITICAL CORRESPONDENT FOR THE DAILY MAIL

19. Internet firms to be banned from offering unbreakable encryption under new laws; Companies such as Apple, Google and others will no longer be able to offer encryption so advanced that even they cannot decipher it when asked to under the Investigatory Powers Bill. telegraph.co.uk, November 2, 2015 Monday 5:12 PM GMT, NEWS, (705 words), By Tom Whitehead Security Editor

20. Nobody is listening to the anti-surveillance campaigners. Financial Times (London, England), November 3, 2015 Tuesday, COMMENT, Pg. 9, (773 words), Janan Ganesh on Politics

21. May calls for internet companies to store details of website visits; Home secretary tries to sweeten snooper's charter by stating that police will need judicial approval to access internet connection records. The Guardian, November 3, 2015 Tuesday 11:00 PM GMT, WORLD NEWS, (970 words), Alan Travis

22. Investigatory powers bill: snooper's charter to remain firmly in place; Legislation will enshrine security services' licence to hack, bug and burgle their way across the web - with judicial oversight still to be determined. The Guardian, November 3, 2015 Tuesday 12:02 AM GMT, WORLD NEWS, (1112 words), Alan Travis Home affairs editor
23. Give spies power, but make them explain why they need it  
_The Independent (London)_ November 3, 2015 Tuesday, COMMENT; Pg. 27, (975 words), STEVE RICHARDS

24. What is the snooper's charter?; The Investigatory Powers Bill, a revamp of the "snooper's charter" Data Communications Bill, is to be published on Wednesday  
_telegraph.co.uk_, November 3, 2015 Tuesday 11:08 PM GMT, NEWS, (469 words), By Charlotte Krol and agency, video source ITN

25. The politics behind the new Investigatory Powers Bill  
_FT.com_, November 4, 2015 Wednesday 1:08 PM GMT, (628 words), David Allen Green

26. Journalists’ sources must be protected from state intrusion, says society; Society of Editors says provisions in Investigatory powers bill granting access to reporters’ data without judicial approval will breach confidentiality  
_The Guardian_, November 4, 2015 Wednesday 11:42 PM GMT, MEDIA, (490 words), Kevin Rawlinson

27. Theresa May unveils UK surveillance measures in wake of Snowden claims; Spy agencies free to track everyone’s internet use without warrant UK governments have signed secret orders on data collection for years Snowden says bill is most intrusive surveillance regime in the west  
_The Guardian_, November 4, 2015 Wednesday 6:13 PM GMT, WORLD NEWS, (1409 words), Alan Travis Patrick Wintour and Ewen MacAskill

28. Surveillance Q&A: what web data is affected - and how to foil the snoopers; Theresa May’s revived snooper’s charter will give police and spies access to a year’s worth of your web browsing history  
_The Guardian_, November 4, 2015 Wednesday 2:39 PM GMT, WORLD NEWS, (1076 words), Samuel Gibbs

29. Theresa May secures backing of Labour and Lib Dems for surveillance plans - live; Home secretary publishes draft investigatory powers billLabour says legislation is not a ‘snoopers’ charter’Key points of May’s billFull story on new surveillance legislationVerdict on prime minister’s questions  
_The Guardian_, November 4, 2015 Wednesday 2:01 PM GMT, POLITICS, (7081 words), Andrew Sparrow

30. Theresa May unveils surveillance measures in wake of Snowden claims; Home secretary announces new powers for police and security services tracking UK citizens’ internet use without need for judicial check  
_The Guardian_, November 4, 2015 Wednesday 1:22 PM GMT, WORLD NEWS, (998 words), Alan Travis Home affairs editor

31. David Cameron and Jeremy Corbyn at PMQs - Politics live; Rolling coverage of the day’s political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised ‘snoopers’ charter’  
_The Guardian_, November 4, 2015 Wednesday 11:50 AM GMT, POLITICS, (2296 words), Andrew Sparrow

32. Theresa May publishes internet surveillance plans - Politics live; Rolling coverage of the day’s political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised ‘snoopers’ charter’  
_The Guardian_, November 4, 2015 Wednesday 11:26 AM GMT, POLITICS, (2031 words), Andrew Sparrow

33.  

88
34. Theresa May publishes internet surveillance plans - Politics live; Rolling coverage of the day’s political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised ‘snoopers’ charter’ *The Guardian,* November 4, 2015 Wednesday 10:32 AM GMT, POLITICS, (1283 words), Andrew Sparrow

35. Theresa May publishes internet surveillance plans - Politics live; Rolling coverage of the day’s political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised ‘snoopers’ charter’ *The Guardian,* November 4, 2015 Wednesday 9:52 AM GMT, POLITICS, (968 words), Andrew Sparrow

36. Theresa May publishes internet surveillance plans - Politics live; Rolling coverage of the day’s political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised ‘snoopers’ charter’ *The Guardian,* November 4, 2015 Wednesday 9:26 AM GMT, POLITICS, (593 words), Andrew Sparrow

37. ‘Snooper’s Charter’: Forcing internet providers to keep our browsing history leaves us open to security breaches; Let’s not pretend that the Bill does not have the potential to impact on our civil liberties in fundamental ways *Independent.co.uk,* November 4, 2015 Wednesday 8:18 PM GMT, VOICES, (620 words), Editorial

38. Theresa May accused of launching ‘major attack on privacy’ amid plans to give access to citizen’s internet usage without a warrant; Home Secretary under fire over moves to force companies to hold data about internet use for up to 12 months *Independent.co.uk,* November 4, 2015 Wednesday 7:32 PM GMT, UK POLITICS, (821 words), Nigel Morris

39. Theresa May: Sweeping powers for spooks to make internet no-go area for terrorists and paedophiles; Home Secretary sets out the new draft Investigatory Powers Bill, which has been described by the Prime Minister as one of the most important pieces of legislation of the next five years *Independent.co.uk,* November 4, 2015 Wednesday 4:14 PM GMT, UK POLITICS, (564 words), Nigel Morris, Matt Dathan

40. Theresa May: Sweeping powers for spooks to make internet no-go area for terrorists and paedophiles; Home Secretary sets out the new draft Investigatory Powers Bill, which has been described by the Prime Minister as one of the most important pieces of legislation of the next five years *Independent.co.uk,* November 4, 2015 Wednesday 2:26 PM GMT, UK POLITICS, (615 words), Nigel Morris, Matt Dathan

41. PMQs live: Jeremy Corbyn accuses David Cameron of ignoring a looming ‘winter crisis’ in the NHS; Draft Bill will increase ability of intelligence services to obtain access to personal internet use of citizens *Independent.co.uk,* November 4, 2015 Wednesday 12:24 PM GMT, UK POLITICS, (366 words), Adam Whithnall

42. Record of EVERY website you visit to be held for a year with tech firms forced to help spies hack phones and computers *MailOnline,* November 4, 2015 Wednesday 12:59 PM GMT, NEWS, (1447 words), MATT CHORLEY, POLITICAL EDITOR FOR MAILONLINE

43. 89
Could Apple stop selling the iPhone in the UK? Government considers ban of end-to-end encryption method used by devices  
*MailOnline*, November 4, 2015 Wednesday 12:51 PM GMT, SCIENCE, (1013 words), SARAH GRIFFITHS FOR MAILONLINE

44. Record of EVERY website you visit to be held for a year under new spying laws which also give spooks power to hack computers  
*MailOnline*, November 4, 2015 Wednesday 12:32 PM GMT, NEWS, (1085 words), MATT CHORLEY, POLITICAL EDITOR FOR MAILONLINE

45. 7 reasons you should be worried about the Tory snooper’s charter: Theresa May wants to make absolutely sure the police can get to your naked Snapchat pictures if they need to. Here’s why the Investigatory Powers Bill is terrifying  
*mirror.co.uk*, November 4, 2015 Wednesday 5:53 PM GMT, NEWS,UK NEWS, (870 words), By Mikey Smith

46. Snooper's Charter plans revealed: Government wants your to track your porn viewing, Facebook stalking and online shopping; Whether it's a casual text message or a personal image you've shared, it will ALL be stored for the government under new legislation brought in by Theresa May  
*mirror.co.uk*, November 4, 2015 Wednesday 9:20 AM GMT, NEWS,UK NEWS, (317 words), By John Shammas

47. MI5 and GCHQ secretly bulk collecting British public's phone and email records for years, Theresa May reveals; First formal confirmation that there has been mass collection of phone and email records in the UK as Investigatory Powers Bill is published  
*telegraph.co.uk*, November 4, 2015 Wednesday 9:31 PM GMT, NEWS, (937 words), By Tom Whitehead Security Editor

48. Theresa May, the new spy laws... and a warning for the public; POLITICAL SKETCH: As spies are offered access to your internet records, a Tory MP says you shouldn't worry... as long as you've got 'nothing to hide'  
*telegraph.co.uk*, November 4, 2015 Wednesday 7:24 PM GMT, NEWS, (329 words), By Michael Deacon Parliamentary Sketchwriter

49. The politics of surveillance are about politics, not keeping us safe; Is Britain really going to become the first major democracy to log every website its citizens visit?  
*telegraph.co.uk*, November 4, 2015 Wednesday 7:22 PM GMT, (869 words), By Mike Harris

50. Theresa May outlines key measures in Investigatory Powers Bill; The Home Secretary has announced new powers for police and security services in tracking the public’s internet use  
*telegraph.co.uk*, November 4, 2015 Wednesday 3:23 PM GMT, (572 words), By Claire Lomas

51. Surveillance laws revamp has faced a rocky road; The Investigatory Powers Bill, to be published on Wednesday, has been seven years in the making  
*telegraph.co.uk*, November 4, 2015 Wednesday 10:56 AM GMT, NEWS, (388 words), By Tom Whitehead Security Editor

52. RIPA: Protecting children from paedophiles trumps your privacy; Theresa May's new Investigatory Powers bill, condemned by some as a 'Snooper's Charter', is essential to stop vile images being traded online  
*telegraph.co.uk*, November 4, 2015 Wednesday 9:54 AM GMT, (540 words), By Peter Wanless chief executive NSPCC

53. MPs with nothing to hide rally round May's new surveillance plan; Sketch  
The Daily Telegraph (London), November 5, 2015 Thursday, NEWS; OPINION; COLUMNS; Pg. 10, (446 words), Michael Deacon
54. Theresa May's investigatory powers bill is a step in the right direction; The introduction of judicial oversight to surveillance laws should help restore the proper balance of privacy and security - and the trust of all communities.
The Guardian, November 5, 2015 Thursday 12:32 PM GMT, COMMENT IS FREE, (758 words), Keir Starmer

55. May internet plan is an 'attack on privacy': SECURITY
i-Independent Print Ltd, November 5, 2015, NEWS; Pg. 8, (382 words), Nigel Morris DEPUTY POLITICAL EDITOR

56. A hacker's charter; Editorials The requirement that internet providers hang on to our browsing history would leave us open to security breaches
The Independent (London), November 5, 2015 Thursday, NEWS; Pg. 4, (574 words)

57. May is accused of 'breathtaking attack' on privacy in new surveillance measures
The Independent (London), November 5, 2015 Thursday, NEWS; Pg. 8, (745 words), NIGEL MORRIS DEPUTY POLITICAL EDITOR

58. Spooks have been harvesting our phone and email data for 14 years: Now MI5 and police get new power to snoop as terror bill leaves no hiding place online
MailOnline, November 5, 2015 Thursday 9:11 AM GMT, NEWS, (2569 words), JAMES SLACK POLITICAL EDITOR FOR THE DAILY MAIL

59. Government spooks 'secretly spying on UK phone calls for ten years' in anti-terror bid; MI5 is said to have collected vast swathes of data about public communications over the last decade
mirror.co.uk, November 5, 2015 Thursday 7:26 AM GMT, NEWS, UK NEWS, (471 words), By John Shammas

60. What spooks know about you; MAY UNVEILS SPY POWERS
The Sun (England), November 5, 2015 Thursday, EDITORIAL; Pg. 10, (797 words), TOM NEWTON DUNN

61. What spooks know about you; MAY UNVEILS SPY POWERS
The Sun (England), November 5, 2015 Thursday, NEWS; Pg. 8, (721 words), TOM NEWTON DUNN

62. Spy Bill is threat to our freedom
Daily Mirror, November 6, 2015 Friday, FEATURES; OPINION COLUMN; Pg. 52, (566 words), FIONA PARKER

63. Investigatory Powers Bill: Labour accused of acting like a 'nodding dog' over support for Theresa May's plans; Exclusive: LibDem leader Tim Farron promises to lead fight against draft bill as he seeks to carve out a niche for his party
Independent.co.uk, November 6, 2015 Friday 7:05 PM GMT, UK POLITICS, (733 words), Andrew Grice

64. Sacrifice a little privacy to support our spies, says anti-terror tsar: LORD CARLILE warns how without UK intelligence MORE planes might have blown up over Egypt
MailOnline, November 8, 2015 Sunday 1:59 AM GMT, RIGHTMINDS, (1178 words), DAILY MAIL COMMENT

65. SUPPORT OUR SPIES
MAIL ON SUNDAY (London), November 8, 2015 Sunday, (1213 words)
66. Andy Burnham calls for more judicial safeguards in UK surveillance bill; Shadow home secretary, who had welcomed draft investigatory powers bill, shifts position in letter to Theresa May after consulting Lord Falconer

The Guardian, November 9, 2015 Monday 12:07 PM GMT, POLITICS, (588 words), Patrick Wintour Political editor

67. Apple boss warns Tories' snooper's charter could HELP criminals by weakening data security; Fears WhatsApp and Apple's iMessage could be hit by the Investigatory Powers Bill making data less secure

mirror.co.uk, November 9, 2015 Monday 11:39 PM GMT, NEWS, UK NEWS, (513 words), By David Hughes

68. Theresa May's spying Bill stops short of allowing access to your full web browsing history; THE Home Secretary says providers WON'T pass on all the pages visited, but will give "the modern equivalent of an itemised phone bill" to security services.

mirror.co.uk, November 9, 2015 Monday 12:20 PM GMT, NEWS, POLITICS, (1218 words), By Arj Singh

69. Why spies want Apple and Google's help; The Snoopers' Charter isn't an attack on encryption; there is another plan to intercept WhatsApp

telegraph.co.uk, November 9, 2015 Monday 7:32 PM GMT, FINANCE, (900 words), By Christopher Williams Technology, Media and Telecoms Editor

70. The battle over your secrets is only just beginning

The Daily Telegraph (London), November 10, 2015 Tuesday, BUSINESS; BUSINESS; OPINION COLUMNS, Pg. 2, (883 words), CHRISTOPHER WILLIAMS

71. Why tech companies are really worried about the snooper's charter; Slipped into the new investigatory powers bill is a law that could spell the end of encrypted services such as WhatsApp and iMessage.

The Guardian, November 10, 2015 Tuesday 10:07 AM GMT, TECHNOLOGY, (978 words), Alex Hern

72. Theresa May's proposed spying law is 'worse than scary' United Nations says; The draft Investigatory Powers Bill would give the Government sweeping new spying powers

Independent.co.uk, November 11, 2015 Wednesday 10:06 AM GMT, UK POLITICS, (458 words), Jon Stone

73. Theresa May's Snooper Tax could make broadband bills skyrocket; The cost of storing everyone's browsing history for a year will be way more than the Government has prepared for

mirror.co.uk, November 12, 2015 Thursday 3:28 PM GMT, NEWS, UK NEWS, (369 words), By Mikey Smith

74. Paris terror attacks: Calls for snooper's charter to be rushed through to prevent UK atrocities; Lord Carlile says the Investigatory Powers Bill should be passed within a month, warning "it could have been London"

mirror.co.uk, November 15, 2015 Sunday 1:12 PM GMT, NEWS, UK NEWS, (445 words), By Mikey Smith

75. Don't fast-track the new surveillance bill; it needs considered scrutiny; Lord Carlile's call for the investigatory powers bill to be rushed through parliament in the wake of the Paris attacks is a misjudged knee-jerk reaction

The Guardian, November 16, 2015 Monday 11:21 AM GMT, COMMENT IS FREE, (742 words), Paul Bernal

76. Terror attack on British soil 'prevented in the last month'; Security services are understood to have stopped a planned attack in the UK in the last 30 days

mirror.co.uk, November 16, 2015 Monday 1:19 PM GMT, NEWS, UK NEWS, (469 words), By Jack Blanchard
77. Cameron considering speedy passage for spy laws; Terror in Paris; Investigatory Powers Bill; Pressure on PM to expedite legislation that gives agencies more power to track terrorism suspects. 
*The Daily Telegraph (London)*, November 17, 2015 Tuesday, NEWS; Pg. 12,13, (614 words), Steven Swinford

78. Cameron considering speeding up passage of spying laws; Investigatory Powers Bill Pressure on PM to expedite legislation that gives agencies more power to track terrorism suspects.
*The Daily Telegraph (London)*, November 17, 2015 Tuesday, NEWS, Pg. 12,13, (704 words), Steven Swinford

79. The Paris attackers' savage affront to the Western way of life cries out for vengeance; This act of butchery in our cafes and nightclubs proves that Europe is facing an enemy from within - Cameron must act drastically like the British people want him to. 
*telegraph.co.uk*, November 17, 2015 Tuesday 9:57 PM GMT, (1037 words), By Allison Pearson

80. IoS letters, emails and online postings (22 November 2015) 
*Independent.co.uk*, November 22, 2015 Sunday 12:15 AM GMT, LETTERS, (634 words), Independent Voices

81. The snooper's charter is a danger to us all. A man in the pub told me
*The Sunday Times (London)*, November 22, 2015 Sunday, NEWS REVIEW;FEATURES; Pg. 14, (994 words), Jeremy Clarkson

82. Crossword roundup: the all-seeing eye; A spot more cricket and an old new word for state intrusion in the best of the cryptic crop

83. Theresa May accused of rushing surveillance bill through back door; Home secretary gives committee three weeks to study 'snooper's charter', despite having ruled out fast-tracking it after Paris attacks
*The Guardian*, November 26, 2015 Thursday 6:33 PM GMT, POLITICS, (508 words), Alan Travis Home affairs editor

84. Theresa May accused of rushing surveillance bill through back door; Home secretary gives committee three weeks to study 'snooper's charter', despite ruling out fast-tracking it after Paris attacks
*The Guardian*, November 26, 2015 Thursday 4:55 PM GMT, WORLD NEWS, (463 words), Alan Travis Home affairs editor

85. NEWS that one of the Paris gunmen
*The Sun (England)*, December 7, 2015 Monday, NEWS; Pg. 10, (155 words), Kavanagh

86. Wi-Fi Barbie doll 'could be used as spy weapon by the government'; Internet-connected toys would be permitted targets under the proposed 'Snooper's Charter', experts told a House of Commons committee
*mirror.co.uk*, December 9, 2015 Wednesday 7:42 PM GMT, NEWS,WEIRD NEWS, (497 words), By Jack Blanchard

87. Cameron warns SNP on snooping vote
*The Daily Telegraph (London)*, December 14, 2015 Monday, NEWS; Pg. 2, (501 words), Simon Johnson

88. SNP 'risks lives on snoopers' law'. David Cameron to tell First Minister that opposition to new interception powers will put the UK in danger
*The Daily Telegraph (London)*, December 14, 2015 Monday, NEWS; FRONT PAGE; Pg. 1, (598 words), Simon Johnson
89. Beaming First Minister Nicola Sturgeon looks thrilled to be outside Number 10 as Cameron pushes SNP to support new powers for spies. MailOnline, December 14, 2015 Monday 6:21 PM GMT, NEWS, (739 words), GERRI PEEV, ALAN RODEN FOR THE DAILY MAIL and MARTIN ROBINSON FOR MAILONLINE

90. David Cameron tells Nicola Sturgeon: Back snoopers' charter. Speaking ahead of their Downing Street talks, the Prime Minister says he wants SNP support for his plans to give the security services more powers to monitor terrorists online. telegraph.co.uk, December 14, 2015 Monday 6:31 AM GMT, NEWS, (608 words), By Simon Johnson Scottish Political Editor

91. Cameron urges Sturgeon to back 'snoopers' charter'. The Times (London), December 14, 2015 Monday, NEWS; Pg. 5, (519 words), Hamish Macdonell

92. Telecoms companies raise questions over cost and feasibility of 'snooper's charter'. BT, Vodafone, 02 Telefonica, EE and 3 tell peers it is not yet possible to determine whether proposals are technically possible. The Guardian, December 15, 2015 Tuesday 6:47 PM GMT, LAW, (762 words), Alan Travis and Owen Bowcott

93. Apple calls on UK government to scale back snooper's charter. Tech company makes rare foray into British politics in a submission to the committee on the investigatory powers bill. The Guardian, December 21, 2015 Monday 10:36 PM GMT, TECHNOLOGY, (818 words), Alex Hern

94. Apple criticises Investigatory Powers Bill: Theresa May's spying law could endanger privacy and security, company says; Apple says the powers would make the 'personal data of millions of law abiding citizens [...] less secure'. Independent.co.uk, December 21, 2015 Monday 10:00 PM GMT, NEWS, (713 words), Andrew Griffin

95. Nearly a quarter of nosy Britons just can't resist looking for their Christmas presents. Express Online, December 22, 2015 Tuesday 9:24 PM GMT, (499 words), Geoff Maynard

96. UK snooping law won't ban WhatsApp, but could leave your data open to HACKERS. Express Online, December 22, 2015 Tuesday 11:39 AM GMT, (693 words), Aaron Brown

97. Apple claims more snooping powers will let 'bad guys' in. The Independent (London), December 22, 2015 Tuesday, NEWS; Pg. 11, (441 words), ANDREW GRIFFIN

98. Apple attacks snooping laws: Technology giants say plans to allow access could cause 'paralysis for business and cause 'serious international conflicts'. MailOnline, December 22, 2015 Tuesday 2:16 PM GMT, NEWS, (388 words), JOSH WHITE FOR THE DAILY MAIL

99. Apple boss Tim Cook calls on British government to scale back snoopers' charter; Cook has already warned against giving spies a "back door" to reading people's e-mails because weakening data security could help criminals. mirror.co.uk, December 22, 2015 Tuesday 9:39 AM GMT, NEWS, TECHNOLOGY & SCIENCE, TECHNOLOGY, (618 words), By Catherine Wylie
Theresa May says new spying powers will be used to bring cyberbullies and online trolls to justice. 

MailOnline, December 25, 2015 Friday 11:44 AM GMT, NEWS, (665 words), SOPHIE JANE EVANS FOR MAILONLINE

101. New Chinese spying laws draw international criticism, despite similarity with UK's Investigatory Powers Bill; China has said that it took inspiration in drafting the powers from the US and elsewhere for a law that bears marked similarities to the UK's 'Snoopers' Charter'.

Independent.co.uk, December 28, 2015 Monday 9:30 AM GMT, NEWS, (574 words), Andrew Griffin

102. Social media bosses face two years in jail if they warn users MI5 is watching them after ministers lose patience with tech giants. 

MailOnline, December 28, 2015 Monday 10:35 PM GMT, NEWS, (598 words), JAMES SLACK POLITICAL EDITOR FOR THE DAILY MAIL

103. Social media bosses face jail if they warn users MI5 is watching them after ministers lose patience with tech giants. 

DAILY MAIL (London), December 29, 2015 Tuesday, (549 words), BY JAMES SLACK POLITICAL EDITOR

104. Facebook and Twitter staff could face jail if they warn users about police surveillance; Snooper's Charter will punish staff at social media companies for warning customers that they are under surveillance.

mirror.co.uk, December 30, 2015 Wednesday 11:32 AM GMT, NEWS, TECHNOLOGY & SCIENCE, TECHNOLOGY, (457 words), By Gavin Cordon

The Guardian

November 1, 2015 Sunday 6:19 PM GMT

Online surveillance bill 'will fall without judicial oversight'; 
Former shadow home secretary David Davis says investigatory powers bill will have to let judges' authorise warrants

BYLINE: Frances Perraudin

SECTION: POLITICS

LENGTH: 795 words

Plans to grant police and intelligence officers new powers to monitor suspects online will not get through parliament without a requirement for judges to sign off on spying warrants, the former Conservative shadow home secretary David Davis has said.

The backbench MP was speaking before the publication of a draft of the investigatory powers bill, due on Wednesday, with the Home Office so far refusing to indicate whether the proposed legislation will include judicial approval of applications made by the security services to intercept communications.

Speaking on BBC1's Sunday Politics show, Davis said: "Actually I don't think this bill will get through either Commons or Lords without judicial authorisation ... There's a new consensus on this right across the board - across the experts, across the spooks, across the parties, across both houses of parliament."

Related: Theresa May forced to backtrack over plan to 'snoop' on internet use
Davis, who has campaigned with Labour's deputy leader, Tom Watson, against what they see as draconian surveillance legislation, denied that a system requiring judicial approval would be less accountable. "Every time I've asked a question of any minister on a security matter ... they say 'we don't comment on security matters.' There is no accountability."

The Home Office has already said that it has dropped several contentious proposals from the bill, including plans to allow the police and security services full access to everyone's internet browsing history. The climbdown was prompted by concerns that the government would be unable to get the legislation through parliament because of unease of its implications for civil liberties.

A report published in June by David Anderson QC recommended that judicial rather than ministerial authorisation of individual, targeted intercept warrants should be required. His position runs counter to parliament's intelligence and security committee, which said in March that responsibility should remain with ministers. The Royal United Services Institute favours an approach under which government authorises some warrants and judges others.

Related: Don't be fooled by spook propaganda: the state still wants more licence to pry | Henry Porter

Speaking on BBC1's Andrew Marr Show, the home secretary, Theresa May, said she sets time aside every day to consider such warrants. "I will be explaining the government's position to parliament this week," she said.

Davis said: "At the moment, the home secretary does about 10 of these warrants in a working day. It's impossible for any one person to do this. It's bad practice, it's bad managerially, it's bad legally and it's bad in terms of counter-terrorism."

Speaking to on the Murnaghan programme on Sky News, the former Liberal Democrat leader Lord Ashdown said the upper house would ensure that judicial oversight of warrants was added to the bill if it was not included in the draft. "This is precisely constitutionally the kind of bill within which we should be intervening if indeed the legislation is deficient,"he said.

The shadow home secretary, Andy Burnham, said on Thursday that Labour would not support the investigatory powers bill unless it included judicial oversight of national security warrants. A spokesperson for Burnham said the shadow cabinet had agreed the party's position, including the opposition leader, Jeremy Corbyn, and his deputy, Tom Watson, who both voted against the current emergency legislation.

Speaking on BBC1's Sunday Politics programme, the shadow home office minister, Keir Starmer, a former director of public prosecutions, said judicial authorisation of new intercept powers was a red line for Labour.

Related: Peers could block police powers to access internet browsing histories

"We've got the chance to have a modern comprehensive law that sets out the powers for law enforcement and the security services and, at the same time, we've got the chance - a historic chance - to get the safeguards right. And one of the safeguards that's really important is judicial authorisation of intercept warrants," he said.

"There's a big difference between data and content, and by content we mean what are people actually saying to each other. That should be signed off by a judge. That's what happens in other countries."

The Sun reported on Thursday that the attorney general, Jeremy Wright, had advised May against giving judges oversight. A minister told the paper: "The attorney general's advice was very clear. It would be totally irresponsible of government to allow the legal system to dictate to us on matters as important as terrorism. Not only would they tie things in knots very quickly, but they are not elected and answerable to nobody."

LOAD-DATE: November 1, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc.
Online surveillance bill 'will fall without judicial oversight';
Former shadow home secretary David Davis says investigatory powers bill will have to let judges' authorise warrants

BYLINE: Frances Perraudin

SECTION: POLITICS

LENGTH: 797 words

Plans to grant police and intelligence officers new powers to monitor suspects online will not get through parliament without a requirement for judges to sign off on spying warrants, the former Conservative shadow home secretary David Davis has said.

Theresa May has said the investigatory powers bill, a draft of which will be published on Wednesday, will include "strong oversight and authorisation arrangements", but has refused to say whether it will include judicial approval of applications made by the security services to intercept communications.

The Home Office said on Saturday that it had dropped several contentious proposals from the bill, including plans to allow the police and security services full access to everyone's internet browsing history. The climbdown was prompted by concerns that the government would be unable to get the legislation through parliament because of unease of its implications for civil liberties.

Related: Theresa May forced to backtrack over plan to 'snoop' on internet use

Speaking on BBC1's Sunday Politics show, Davis said: "Actually I don't think this bill will get through either Commons or Lords without judicial authorisation ... There's a new consensus on this right across the board. Across the experts, across the spooks, across the parties, across both houses of parliament."

Davis, who has campaigned with Labour's deputy leader, Tom Watson, against what they see as draconian surveillance legislation, denied that a system that required judicial approval would be less accountable. "Every time I've asked a question of any minister on a security matter ... they say 'we don't comment on security matters.' There is no accountability."

A report published in June by David Anderson QC recommended that judicial rather than ministerial authorisation of individual, targeted intercept warrants should be required. His position runs counter to parliament's intelligence and security committee, which said in March that responsibility should remain with ministers. The Royal United Services Institute favours an approach under which government authorises some warrants and judges others.

Related: Don't be fooled by spook propaganda: the state still wants more licence to pry | Henry Porter

Speaking on the BBC1's Andrew Marr Show, the home secretary said she sets time aside every day to consider such warrants. "I will be explaining the government's position to parliament this week," she said.

Davis said: "At the moment the home secretary does about ten of these warrants in a working day. It's impossible for any one person to do this. It's bad practice, it's bad managerially, it's bad legally and it's bad in terms of counter-terrorism."
Speaking to on the Murnaghan programme on Sky News, the former Liberal Democrat leader Lord Ashdown, said the upper house would ensure that judicial oversight of warrants was added to the bill if it was not included in the draft.

"This is precisely constitutionally the kind of bill within which we should be intervening if indeed the legislation is deficient," he said.

The shadow home secretary, Andy Burnham, said on Thursday that Labour would not support the investigatory powers bill unless it included judicial oversight of national security warrants. A spokesperson for Burnham said the shadow cabinet had agreed the party's position, including the opposition leader, Jeremy Corbyn, and his deputy, Tom Watson, who both voted against the current emergency legislation.

Speaking on BBC1's Sunday Politics programme, the shadow home office minister, Keir Starmer, a former director of public prosecutions, and said judicial authorisation of new intercept powers was a red line for Labour.

Related: Peers could block police powers to access internet browsing histories

"What we've got here is we've got the chance to have a modern comprehensive law that sets out the powers for law enforcement and the security services, and at the same time we've got the chance - a historic chance - to get the safeguards right.

"And one of the safeguards that's really important is judicial authorisation of intercept warrants," he said.

"There's a big difference between data and content, and by content we mean what are people actually saying to each other. That should be signed off by a judge. That's what happens in other countries."

The Sun reported on Thursday that the attorney general, Jeremy Wright, had advised May against giving judges oversight. A minister told the paper: "The attorney general's advice was very clear. It would be totally irresponsible of government to allow the legal system to dictate to us on matters as important as terrorism. Not only would they tie things in knots very quickly, but they are not elected and answerable to nobody."

LOAD-DATE: November 1, 2015

EU referendum: Theresa May could lead 'Out' campaign after Nigel Farage says he'd be 'delighted' if she took the role;
Survey suggests she would be the public choice to take charge of the 'Brexit' campaign

BYLINE: Nigel Morris

SECTION: UK POLITICS
Theresa May left open the option of leading the drive for Britain to quit the European Union after the Ukip leader Nigel Farage said he would be "absolutely delighted" if she accepted the role.

Following a survey suggesting she would be the public choice to take charge of the "Brexit" campaign, the Home Secretary insisted she was only focused on renegotiating Britain's relationship with the EU.

Her comments were in contrast to David Cameron's warning last week of the dangers to Britain of leaving the EU and attempting to strike a Norwegian-style deal with the bloc.

Ms May is regarded as more Eurosceptic than either the Prime Minister or Chancellor George Osborne, who flies to Berlin on 2 November to hold talks with German minister to discuss Britain's demands.

Mr Cameron is expected next week to make public his demands, which will be discussed at a summit of EU leaders next month.

Ms May would be the most popular choice to head the Out campaign in the referendum promised by Mr Cameron, according to the Survation poll for the pressure group Leave.EU. She attracted the backing of 22.2 per cent of respondents ahead of Mr Farage with 18.6 per cent.

Asked on BBC1's Andrew Marr Show whether there was any prospect of her leading the campaign, she replied: "There are some people who say you should be in at all costs, there are people who say you should be out at all costs.

"Actually I say let's do this renegotiation. Let's see what reform we can bring about as a result of that renegotiation and then put it to the British people."

Ms May would not say whether she instinctively backed leaving or remaining in the EU.

She said: "The decision isn't going to be my decision individually or the prime minister's decision individually. It will be for the British public and that's the important thing."

The Home Secretary has struck a Eurosceptic note in recent months, calling for limits to freedom of movement within the EU. She has also raised the prospect in the past of withdrawing from the European Convention on Human Rights if it is necessary to end the abuse of human rights laws.

Mr Farage told the programme that voters would support Ms May if she admitted her experience of presiding over increasing net migration had led her to support Britain's withdrawal.

The Ukip leader said: "If [she] was to say 'look I've been here, I've been at the sharp end, we cannot do this as EU members, we need a better way', of course the public would come behind it. And you know what, so would I too."

Asked if he would support her as leader of the Out campaign, he replied: "I would be absolutely delighted of course."

Read more

'Out' campaigners warned 'Brexit' would damage trade with US

Nick Clegg: Keeping the EU at arm's length would be a disaster for UK

European Union trade deals 'will bring in £20bn for Britain'

'Out' backers in EU referendum set to make billions from Brexit

In his meetings in Berlin, Mr Osborne will be seeking German backing for Britain's demands, including an "emergency brake" to protect states outside the single currency from decisions taken by eurozone members.

He will hold talks with the Finance Minister Wolfgang Schäuble and address an audience of German business leaders at the annual conference of the BDI, the Federation of German Industries.

Ahead of the visit Mr Osborne said: "The UK and German economies are the beating heart of Europe, the engine for growth and jobs. Together we make the world's third-largest economy, behind only America and China and since the crisis ended, we have generated two-thirds of EU growth."
"But the future holds challenges for our economies. We must cut debt and boost productivity. To do this, we need a strong EU, fit for today's challenges and working for the benefit of all 28 member states. The UK's reform and renegotiation plans aim to achieve this, which is why these talks with key partners in Europe are so important."

'Snooper's charter': Judges to be in charge

MPs and peers would veto giving the police and security services the power to monitor suspects online unless judges are put in charge of issuing surveillance warrants, the Tory MP David Davis said last night. He issued the warning ahead of this week's publication of a draft Investigatory Power Bill which will overhaul the legislation governing the interception of communications.

In the face of cross-party hostility, Theresa May, the Home Secretary, has dropped plans to give the intelligence agencies full access to computer users' internet browsing history. They will have to obtain a warrant to carry out surveillance.

According to reports on 1 November, ministers would initially issue the warrants and their decisions would be checked by security-cleared judges.

Andy Burnham, the shadow Home Secretary, said there was "broad acceptance" that new legislation was required, but called for the Government to "ensure that judges have the final say". Lord Ashdown, the former Lib Dem leader, said it appeared that the Conservatives had abandoned the worst elements of the "snooper's charter" proposals.

Nigel Morris

UK Government plan to ban WhatsApp dropped, as Theresa May abandons many of proposed new powers for spies; Campaigners say that climbdown is 'spin', to allow Government to sneak in many more intrusive powers

BYLINE: Andrew Griffin

SECTION: NEWS

LENGTH: 909 words

Controversial plans to allow spies and the police to look in on anyone's internet browsing history have been dropped.

The Government has announced that it will no longer proceed with widely-criticised plans to ban or dramatically weaken encryption so that it could read the messages of everyone in the country. While
ministers described the change of policy as a climbdown, campaigning groups said that the move was spin and that many of the worst parts of Theresa May's planned surveillance powers will remain.

The Government has long been looking to give sweeping new powers to spies, which would include the ability to look in on the communications of people in the UK. Senior politicians have repeatedly stressed that they would look to strengthen powers of the country's spying agencies, and ban the technology that keeps them from snooping on communications.

Read more

WhatsApp could be banned under new surveillance plans

The investigatory powers bill is the latest attempt to push through such powers, and will be published on Wednesday in draft form. But it will be without one of the major intrusive parts that had long been suggested, reports the Guardian.

The bill will in fact ban the police and intelligence services from looking in on people's internet browsing histories, according to a statement. That power has been demanded by the security services, but their access to internet connections will instead "be strictly limited and targeted", according to the statement.

Plans to weaken encryption so that spies can read messages will no longer go ahead. The requirement on UK internet service providers that they store data on their users' internet traffic will also be dropped, according to the report.

"We know these powers are needed as technology changes and terrorists and criminals use ever more sophisticated ways to communicate," a Government source told the Guardian. "But we need to give people the reassurance that not only are they needed, but that they are only ever used in a necessary, proportionate and accountable way. That is what this bill is all about."

USA Freedom Act passed by Senate and signed by President Obama, limiting NSA surveillance

But campaigners have said that authorities had intentionally set up the debate so that they could drop the most outrageous parts and still passed strengthened powers. Key controversial parts of the bill will remain, such as leaving out a safeguard that requires judges to sanction any reading of messages.

"It's a traditional Home Office dance first to ask for the most outrageous, even impractical, powers, so that the smallest so-called 'concessions' seem more reasonable," Shami Chakrabarti, the director of campaign group Liberty, told the Guardian. "The frantic spinning distracts from the sleight of hand.

"Where is the judicial sign-off before our private communications can be collected, hacked and tapped? Where is the move back to targeted surveillance and away from the blanket collection of our private data?"

Some of the invasive powers that are expected to be passed into law were first introduced in the Snoopers' Charter - a piece of legislation pursued by Theresa May but defeated in the House of Commons by the Liberal Democrats. After the election earlier this year, Ms May suggested that such powers would return.

But the Government has abandoned those plans in part because of an embarrassing defeat over tax credits earlier this week, reports the Guardian. Senior Government figures were reportedly concerned that the House of Lords would reject the surveillance powers as they did that bill, and the change comes in the wake of discussions between Ms May and David Cameron.

Read more

Theresa May is 'villain of the year' for Snoopers' Charter

May to push huge new spying powers through Parliament

Snoopers' charter set to return to law as Theresa May suggests

The climbdown comes almost exactly a year after David Cameron and the Conservative Government began a campaign apparently to end or severely weaken encryption.

"The question we must ask is: are we prepared to have a means of communication - the internet and a number of modern methods- that we are not able to intercept?" he asked following the publication of the report into the killing of Lee Rigby. "My answer is clear: we should not accept that. We should legislate to ensure that that is the case."

He echoed the comments at the beginning of 2015, after the attacks on Charlie Hebdo.
The Government long characterised the plan to weaken encryption as a way of ensuring that intelligence agencies could get into the communications of criminals. But internet experts pointed out that the same technology is used for a variety of legitimate functions, like keeping internet banking data safe and ensuring that messages aren’t read by people other than their intended recipients.

Computer scientists have also pointed out that it is impossible to weaken encryption in such a way that only the Government can access it, since the same weaknesses can be exploited by malicious hackers. That is a view understood to be held by many of the major technology companies.

The move could partly be a response to changes in the US, where activists have encouraged the authorities to limit the powers of spies. Many have suggested that the US change of policy could spread to many of its allies, including the UK.
Mrs May told BBC One’s Andrew Marr Show: ‘If there are more intrusive requirements, then of course, warrants are required for those.’

‘What I am clear about is that there will be in this Bill strong oversight and authorisation arrangements.

‘What the Bill will do on Wednesday is, it sets a modern legal framework but, crucially, it has very strong oversight arrangements within it.

‘I think it will be world leading oversight arrangements within the Bill. It will be clear and more comprehensive and comprehensible than the previous legislation has been.’

She said the Bill would not include powers to restrict encryption.

Mrs May added: ‘Encryption is important for people to be able to keep themselves safe when they are dealing with these modern communications in the digital age but what we will be doing is setting out the current position, which does enable the authorities with proper authorisation to issue warrants.’

More than 1,400 warrants authorising more intrusive measures cross the Home Secretary’s desk a year, she said.

**WHAT IS AN INTERNET CONNECTION RECORD?**

Under the new plans police and security services will be able to access internet connection records.

The records show what websites users have visited and what device they used to do so.

They do not show the specific web pages or any further information. If officers want to access these, they will be required to get a warrant.

For example, under the new plans police will be able to see that a user has accessed www.dailymail.co.uk but will not be able to see any pages further than that.

It could also say that a person’s mobile phone connected to Whatsapp at 13.09pm and Facebook at 14.02pm but does not include details of what was said or to whom.

The user’s full browsing history will not be available.

Mrs May said she spent ‘as long as is necessary’ considering each one and time was set aside in her diary every day to allow that to happen.

Ministers have looked at all the arguments about handing over that responsibility to independent judges and the decision will be announced on Wednesday, she added.

Meanwhile, a government source told the Guardian: ‘We’re absolutely clear that key parts of the original plans from 2012 will be dropped from the new bill. We have consulted widely ... we are coming forward with a new approach.

‘We know these powers are needed as technology changes and terrorists and criminals use ever more sophisticated ways to communicate. But we need to give people the reassurance that not only are they needed, but that they are only ever used in a necessary, proportionate and accountable way. That is what this bill is all about.’

However, Shami Chakrabarti, director of Liberty, claimed the reported climbdown was mere spin, suggesting the government had ignored the most important safeguard - for any interception to take place only after judicial authorisation had been given.

She said: ‘If the authorities need a judge’s warrant before they search my home, why not before the equal or greater intrusion of accessing my private communications?

‘This happens all over the free world including in the US. Nothing short of this fundamental safeguard should comfort the public or Parliament that this much-anticipated new Bill is an improvement on the past.’

Shadow home secretary Andy Burnham said there was a ‘broad acceptance’ that a new law was needed.

He told Murnaghan on Sky News: ‘The online world has created blind spots the authorities can’t see any more.

‘I’m not going to play politics with this issue,’ he added.

Mr Burnham said he had ‘outlined’ his approach to party leader Jeremy Corbyn.
He called for the Government to 'ensure that judges have the final say' on the most intrusive warrants. Former director of public prosecutions Keir Starmer said there was a 'strong case' for a new law but demanded judicial oversight.

[The Government] will not be giving powers to go through people's browsing history Home Secretary Theresa May

The Labour MP told BBC One's Sunday Politics: 'It is really a chance now for all of us to agree a framework for the future that is on the one hand giving the authorities powers they need but on the other hand entrenching in law the right safeguards, and judicial oversight is really important in that.'

Plans for a two tier system that divides responsibility for warrants between the Home Secretary and judges have been mooted.

But Mr Starmer said: 'I'm not in favour of a two tier system. I think if you are going to go for contents we should go to a judge straight off.'

Former Liberal Democrat leader Lord Ashdown said Mrs May's comments indicated that the worst aspects of the previous 'snooper's charter' had been diminished.

But he warned that if the Bill imposes blanket surveillance and does not have judicial oversight built in, the Lib Dems will seek to amend it in the Lords.

He told Sky News's Murnaghan programme: 'Some of the worst aspects of that have now been diminished, this is a power exercised not against a class of people but on single individuals, based on an evidence base, and subject to judicial oversight.

'Those are the key three principles, they are the principles we used in the era of the steaming kettle.

'If those principles have been preserved in this Bill, I think the Bill looks to me as though it will be far, far better than many imagined it would be.

'But if it isn't then we will use the House of Lords to ensure that it is, let me assure you of that.'

Lord Ashdown said it was right for the Lords to try and improve the Bill as the Commons would always win out in a battle of parliamentary 'ping pong' between the two chambers.

He said: 'In the first stage we (the Lords) are a reforming chamber and this is precisely, constitutionally, the kind of Bill within which we should be intervening if indeed the legislation is deficient.

'So there isn't a constitutional issue about this, there may be about the other (tax credits), but there isn't about this and you may be sure we will exercise those powers within the House of Lords as a whole - Lib Dems are part of it, crossbenchers and others, to ensure that we fulfil our proper constitutional function.'

Conservative David Davis said oversight must not be left in the hands of the Home Secretary.

The former shadow home secretary told the Sunday Politics programme: 'It's got to be independent and it's got to be, ideally, judicially overseen.

'It can't be the policeman in the office next door or a spook in the office next door and it can't be the Home Secretary. It's got to be independent.'
Theresa May backtracks over snoopers' charter and drops plans to let police and spies see your internet browsing history

BYLINE: SAM TONKIN FOR MAILONLINE

SECTION: NEWS

LENGTH: 1132 words

Plans to allow the police full access to internet browsing history scrapped
Theresa May has today backtracked on the so-called snoopers' charter amid fears government would be unable to force new laws through parliament
Concerns over civil liberties believed to be a stumbling block for new Bill
Despite backtrack, opponents say there's still no judicial oversight of spies

Home Secretary Theresa May has ditched controversial plans to allow the police and security services full access to everyone's internet browsing history.

She is said to have backtracked on the so-called snoopers' charter amid fears the government would be unable to force new laws through parliament because of concerns over civil liberties.

In an unexpected climbdown the Home Office said it had dropped several contentious proposals from the original 2012 Investigatory Powers Bill, due to be set out in draft form on Wednesday.

The Home Secretary insisted the Government 'will not be giving powers to go through people's browsing history'.

Mrs May told BBC One's Andrew Marr Show: 'If there are more intrusive requirements, then of course, warrants are required for those.'

'What I am clear about is that there will be in this Bill strong oversight and authorisation arrangements,' she added.

'What the Bill will do on Wednesday is, it sets a modern legal framework but, crucially, it has very strong oversight arrangements within it.

'I think it will be world leading oversight arrangements within the Bill. It will be clear and more comprehensive and comprehensible than the previous legislation has been.'

She said the Bill would not include powers to restrict encryption.

Mrs May added: 'Encryption is important for people to be able to keep themselves safe when they are dealing with these modern communications in the digital age but what we will be doing is setting out the current position, which does enable the authorities with proper authorisation to issue warrants.'

More than 1,400 warrants authorising more intrusive measures cross the Home Secretary's desk a year, she said.

Mrs May said she spent 'as long as is necessary' considering each one and time was set aside in her diary every day to allow that to happen.

Ministers have looked at all the arguments about handing over that responsibility to independent judges and the decision will be announced on Wednesday, she added.

Meanwhile, a government source told the Guardian: 'We're absolutely clear that key parts of the original plans from 2012 will be dropped from the new bill. We have consulted widely ... we are coming forward with a new approach.

'We know these powers are needed as technology changes and terrorists and criminals use ever more sophisticated ways to communicate. But we need to give people the reassurance that not only are they needed, but that they are only ever used in a necessary, proportionate and accountable way. That is what this bill is all about.'
However, Shami Chakrabarti, director of Liberty, claimed the reported climbdown was mere spin, suggesting the government had ignored the most important safeguard - for any interception to take place only after judicial authorisation had been given.

She said: 'If the authorities need a judge’s warrant before they search my home, why not before the equal or greater intrusion of accessing my private communications?

'This happens all over the free world including in the US. Nothing short of this fundamental safeguard should comfort the public or Parliament that this much-anticipated new Bill is an improvement on the past.'

Shadow home secretary Andy Burnham said there was a 'broad acceptance' that a new law was needed.

He told Murnaghan on Sky News: 'The online world has created blind spots the authorities can't see any more.

'I'm not going to play politics with this issue,' he added.

Mr Burnham said he had 'outlined' his approach to party leader Jeremy Corbyn.

He called for the Government to 'ensure that judges have the final say' on the most intrusive warrants.

Former director of public prosecutions Keir Starmer said there was a 'strong case' for a new law but demanded judicial oversight.

Former Liberal Democrat leader Lord Ashdown said Mrs May's comments indicated that the worst aspects of the previous 'snooper's charter' had been diminished.

But he warned that if the Bill imposes blanket surveillance and does not have judicial oversight built in, the Lib Dems will seek to amend it in the Lords.

He told Sky News's Murnaghan programme: 'Some of the worst aspects of that have now been diminished, this is a power exercised not against a class of people but on single individuals, based on an evidence base, and subject to judicial oversight.

'Those are the key three principles, they are the principles we used in the era of the steaming kettle.

'If those principles have been preserved in this Bill, I think the Bill looks to me as though it will be far, far better than many imagined it would be.

'But if it isn't then we will use the House of Lords to ensure that it is, let me assure you of that.'

Lord Ashdown said it was right for the Lords to try and improve the Bill as the Commons would always win out in a battle of parliamentary 'ping pong' between the two chambers.

He said: 'In the first stage we (the Lords) are a reforming chamber and this is precisely, constitutionally, the kind of Bill within which we should be intervening if indeed the legislation is deficient.

'So there isn't a constitutional issue about this, there may be about the other (tax credits), but there isn't about this and you may be sure we will exercise those powers within the House of Lords as a whole - Lib Dems are part of it, crossbenchers and others, to ensure that we fulfil our proper constitutional function.'

Conservative David Davis said oversight must not be left in the hands of the Home Secretary.

The former shadow home secretary told the Sunday Politics programme: 'It's got to be independent and it's got to be, ideally, judicially overseen.
'It can't be the policeman in the office next door or a spook in the office next door and it can't be the Home Secretary. It's got to be independent.'

LOAD-DATE: November 1, 2015
LANGUAGE: ENGLISH
PUBLICATION-TYPE: Web Publication
JOURNAL-CODE: WEBDM

New internet snooping law will NOT ban WhatsApp and Snapchat; Details of the revamped snooper's charter have emerged and the government have backed down on plans to restrict online encryption

BYLINE: By Mikey Smith
SECTION: NEWS, UK NEWS
LENGTH: 376 words

Theresa May has backed down over plans to ban online messaging services that use encryption, it has been revealed.
The new internet snooping laws will not restrict encrypted services like WhatsApp, Snapchat and iMessage.
Details of the revamped snooper's charter emerged last night, with ministers ruling out any proposal to curb the use of encryption online.
But British spies will still be able to intercept the content of internet communications without a warrant.
The government is pushing the Investigatory Powers Bill, due to be unveiled on Wednesday, which it says will give police and security services the powers they need to fight serious crime and terrorism in the digital age.
The emergence of encryption is a major headache for law enforcement bodies, with suggestions that it risks leaving them locked out of some areas of cyber space.
Earlier this week, MI5 chief Andrew Parker said the "conversations of our adversaries" are happening on a bewildering array of devices and digital platforms, adding: "An increasing proportion of such communications are now beyond our reach - in particular with the growing prevalence of sophisticated encryption."
Internet companies will still be required to store the so-called 'internet connection records' of users.
But sources say access to these records - which show which websites a person has visited, but not the specific content viewed - will be "controlled".
They insist the powers would not allow authorities to access records of every person's full internet activity.

Anything more detailed than the main address of the website will require spooks to obtain a warrant from a judge or a cabinet minister.

The snooper's charter was originally floated in 2012, but faced heavy opposition from Lib Dem ministers in the Coalition.

A Government source said: "We're absolutely clear that key parts of the original plans from 2012 will be dropped from the new Bill.

"We know these powers are needed as technology changes and terrorists and criminals use ever more sophisticated ways to communicate.

"But we need to give people the reassurance that not only are they needed, but that they are only ever used in a necessary, proportionate and accountable way. That is what this Bill is all about."

Whatsapp Mirror Politics

LOAD-DATE: November 1, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

Curbs on snooper's charter;
Snooper's charter is needed, police insist

BYLINE: Tim Shipman

SECTION: NEWS; Pg. 1,2

LENGTH: 908 words

JUDGES will be given the power to veto surveillance requests by Britain's intelligence agencies after a dramatic concession by the government.

A new bill will allow spies to search the internet and social media activity of everyone in the UK if they obtain a warrant.

Technology firms will be required to keep records for 12 months, detailing when emails were sent or when people connected to social media sites, such as Twitter, Facebook and WhatsApp.

If officials wanted to read the content of messages, they would need a second warrant.

However, ministers have abandoned several of the most controversial elements of the so-called "snooper's charter" in an effort to persuade Tory rebels and the Labour leadership to back the plans.
The Investigatory Powers Bill, to be unveiled on Wednesday by Theresa May, the home secretary, will make ministers responsible for the initial decision about whether surveillance can go ahead.

But senior sources said there would be a "two-stage" approvals process to ensure that those decisions were supported by a senior judge with security clearance - a key concession demanded by civil liberties groups.

A new investigatory powers commissioner, another senior judge, will be appointed to oversee the entire process.

A Whitehall official said: "The judge will have the support, powers, resources and technical expertise effectively, and visibly, to hold the agencies and law enforcement to account."

Police demands to obtain routine access to the internet browsing history of everyone in the UK have also been rejected. Instead, access to details of web searches and which sites have been visited will be restricted to the most serious cases - such as terrorist suspects.

"Law enforcement will not be able to, or seek to, access everyone's full browsing history," the official said.

"Any access to internet connection records will be strictly limited and targeted."

In another U-turn, plans put forward in 2012 to force British technology companies to store internet traffic from foreign companies that use their networks to reach customers in Britain have been ditched.

David Cameron's personal threat to ban encryption online to make it easier for spies to access messages has also been abandoned.

In an attempt to stop town hall chiefs abusing the rules to spy on local householders, the bill will also create an offence Continued on page 2 uu Continued from page 1 of "wilful or reckless misuse of communications data" by a public authority "punishable by imprisonment".

Measures to enshrine protections in law for journalists' sources will be included. Cameron will also announce plans to put into law the Wilson doctrine, which says MPs cannot be placed under direct surveillance by the intelligence services.

Foreign technology firms will not be forced to meet British data retention obligations. Instead, the government will seek a deal with the US government to govern when and how data can be handed over.

In a letter to The Sunday Times today, leading police chiefs warn that failure to back the plans would have "significant implications for public safety in the UK".

Bernard Hogan-Howe, the Metropolitan police commissioner, argues that the powers are needed to combat terrorism and catch paedophiles.

The letter, also signed by Keith Bristow, director of the National Crime Agency; Sara Thornton, who chairs the national police chief's council; and Mark Rowley, the council's counterterrorism spokesman, says: "The explosion in communications technology has changed the ways in which law enforcement must operate if it is to continue to find missing children, build a case against sexual predators or murderers, catch armed robbers or track down cyberfraudsters who have emptied bank accounts. Currently we are being left behind."

Nonetheless, the bill is likely to lead to public outcry and bitter battles in parliament.

David Davis, the former shadow home secretary, said: "It is to be welcomed that the government is now recognising some of the spectacular impracticalities of its original approach, notably on encryption, and we should welcome the outbreak of common sense, but the fight will be over judicial oversight.

"You need a minister to rule on foreign surveillance requests - it's a political decision whether you bug Angela Merkel's phone - but for domestic authorisations, this could be just another limp oversight arrangement.

"Ministers are currently approving 2,500 warrants a year which means they rely heavily on their support staff. I see no logical argument for this arrangement."

Ministers hope that enough Labour MPs will back the plans to see off a rebellion from the Conservative back benches. Andy Burnham, the shadow home secretary, has struck a deal with Jeremy Corbyn, the Labour leader, that the party's front bench will not oppose the bill if judges are given more powers.
As well as the new powers, the bill will draw together the surveillance rules in six separate acts of parliament. A government source said: "We're clear that key parts of the original plans from 2012 will be dropped from the new bill. We have consulted widely ... and we are coming forward with a new approach.

"We know these powers are needed as technology changes and terrorists and criminals use ever more sophisticated ways to communicate.

"But we need to give people the reassurance that, not only are they needed, but that they are only ever used in a necessary, proportionate and accountable way."

Letters, page 24

LOAD-DATE: November 1, 2015

LANGUAGE: ENGLISH

GRAPHIC: May: new powers sought

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: STS

Copyright 2015 Times Newspapers Limited
All Rights Reserved

Return to List

9 of 104 DOCUMENTS

DAILY MAIL (London)

November 2, 2015 Monday

NOW APPS USED

LENGTH: 649 words

JIHADI RECRUITERS WON'T FACE BAN

BY DANIEL MARTIN CHIEF POLITICAL CORRESPONDENT

MINISTERS have dropped a pledge to crack down on secret messaging apps used by jihadi recruiters to groom British children.

In January, David Cameron indicated he wanted to ban encryption' or weaken it, to allow security services to read what terrorists are saying.

But yesterday, the Home Secretary revealed that the draft Investigatory Powers Bill, to be published this week, will not ban encryption. Theresa May said this was because the process was vital to all modern communications.

Online banking, as well as social media sites such as Facebook and WhatsApp, rely on encryption.

In May, a Daily Mail investigation revealed encrypted mobile phone apps are at the heart of attempts by Islamic State recruiters to target teenagers in Britain and prime them for jihad. Among those using such apps were former Cardiff students Nasser Muthana, 20, and Reyaad Khan, 21, who joined IS and featured in a recruitment video for the terror group. Khan was later killed in an RAF drone strike.

The apps were developed by extremists to send messages that cannot be read by the authorities.

Security experts have warned it would not be possible to ban messaging apps that use encryption.

The Prime Minister spoke of his desire to see an end to encryption after the Charlie Hebdo massacre in January. He said: In extremis, it has been possible to read someone's letter, to listen to someone's
call?...?The question remains: are we going to allow a means of communications where it simply is not possible to do that? My answer to that question is: no, we must not.'

A year before, he had said: Are we prepared to have a means of communication, the internet and a number of modern methods, that we are not able to intercept? My answer is clear: we should not accept that. We should legislate to ensure that that is the case.'

But computer security expert Graham Cluley said at the time: Cameron is living in cloud cuckoo land if he thinks that this is a sensible idea?...?it wouldn't be possible to implement properly.'

Yesterday, Mrs May told BBC1's Andrew Marr Show: We're not banning encryption. Encryption is important for people to be able to keep themselves safe when they're dealing with these modern communications in the digital age.

But what we'll be doing is setting out the current position, which does enable the authorities with proper authorisation to issue warrants.'

Pressed on Mr Cameron's comments, she said: The first duty of any government is to keep our country and our people safe, which is precisely why we are bringing forward the Investigatory Powers Bill?...?[and] setting out a very clear legal framework, clearer than previously.'

Internet experts say encryption technology used by terrorists is also used for legitimate functions such as keeping online banking data safe and ensuring messages are read only by the intended recipients. Robin Simcox, of think-tank the Henry Jackson Society, said an increase in encryption, enabling terrorists to communicate in a more secure way, was a huge challenge for our security services'.

He added: I don't believe the Conservatives ever really were considering banning it. It's not practical?...?A hole in encryption for our security services' benefit is also one that could be exploited by our adversaries.'

A Home Office spokesman said encryption was ensuring safe online commerce and protecting people's personal data'. But she added that companies must be able to access the content of communications on their networks when presented with a warrant, as many of them already do for their own business purposes'.

'THE Investigatory Powers Bill will give protection to journalists' sources. Theresa May has vowed to stop police using anti-terror powers to access reporters' email or phone records unless they have broken the law or serious crime is being investigated.
Theresa May claims the UK's revived Investigatory Powers Bill -- dubbed by critics a snoopers' charter -- is a very different beast from its predecessor, but senior Whitehall officials have conceded that it is still likely to stir staunch opposition when it is published on Wednesday.

According to officials familiar with the drafting, and bodies that have been consulted, the powers laid out by the home secretary will cluster around four main areas.

The first grouping will concern so-called communications data. Such information is often likened to the "envelope" of a letter. It is data that concerns the how, what, where, who and when of communications, but not the content itself. For law enforcement agencies and intelligence authorities it can be of immense value.

The second grouping concerns the content of communications and their interception. The legislation is likely to make it clear that, with a specific warrant in place, the government has the right to demand to see the content of any communication from an organisation with a presence in the UK. It will also outline the time period for which communication service providers will have to hold on to data themselves.

The third grouping will outline powers, with a warrant, for the government to be able to hack into specific computers, electronic systems or mobile devices to obtain intelligence information, known as computer network exploitation. In an age of increasing encryption of communications between devices, this power is particularly crucial for UK spymasters to secure. This will be a new set of powers, that were not present in the previous, aborted legislation.

The fourth grouping will set out the rules allowing the UK's intelligence agencies, led by GCHQ, to continue programmes for the bulk collection and analysis of data.

Across all of these, the question of issuing warrants will loom large. In some areas -- such as the monitoring of communications data and the bulk collection of information by GCHQ for mass analysis -- it is unlikely that additional safeguards will be put in place. Existing practices are likely to be safeguarded by the bill. The proposed legislation is likely, however, to far more specifically delineate the ability to monitor communications of government departments not involved in national security activities. Processes for obtaining communications data -- the first cluster of powers -- will be more carefully defined.

The issuing of warrants for the interception of communications is likely to be the biggest controversy of the bill. So much so that officials at the Home Office were still waiting for a final decision by Ms May as to their exact form at the weekend. The three options for them mirror proposals laid down in the three independent reviews of UK surveillance activities conducted in recent months by parliament's intelligence and security committee, the independent terrorism watchdog David Anderson, and the think-tank RUSI.

Respectively, they favour secretaries of state continuing to issue warrants; an independent judicial authority to grant warrants and a hybrid of the two. Ms May is known to favour the continuance of the current orthodoxy, with secretaries of state approving all warrants. The intelligence agencies -- desperate for minimal disruption to their activities -- staunchly back her. But political pressure from Tory backbenchers and the opposition means it would be a high risk option to go for politically. Some, therefore, see a hybrid model, with retrospective judicial oversight, as the best compromise.

The parallel controversy to the authorisation warrants debate, however -- one likely to receive far less airtime -- is actually the most important, as far as the UK's spooks are concerned. Under the current arrangements, when the government wishes to obtain information on the content of communications from CSPs such as Facebook or Google, there are two avenues. About 70 per cent of the time, CSPs voluntarily provide it. On other occasions, the government must pursue it through the multilateral assistance treaty with the US government. US authorities obtain the communication through their own powers and then share it with the UK. The process, say senior intelligence officials, can take months.

The new bill will aim to force CSPs to comply directly with UK government requests. CSPs in the US say this will be impossible, since it will force them to break US law. The impasse will only be resolvable if the government has been able to secure progress in a diplomatic initiative being spearheaded by Sir Nigel Sheinwald. Sir Nigel is hoping for a new bilateral treaty or agreement with Washington that will give the UK the right to compel information disclosure from US companies for intelligence purposes. It is far from clear whether Sir Nigel is anywhere near getting such a carte blanche agreed.
One top UK security mandarin dismissed the disagreements with CSPs as a "matter of theology". Tech companies too have noted a far more constructive working relationship with Whitehall of late. Without a fairly dramatic display of unity, however, it is hard to see how the Investigatory Powers bill will avoid a schism between British securocrats and the giants of Silicon Valley.

**LOAD-DATE:** July 22, 2016

**LANGUAGE:** ENGLISH

**PUBLICATION-TYPE:** Web Publication

Copyright 2015 The Financial Times Ltd.
All Rights Reserved
Please do not cut and paste FT articles and redistribute by email or post to the web.

Return to List

11 of 104 DOCUMENTS

FT.com

**November 2, 2015 Monday 5:49 PM GMT**

**Nobody is listening to the UK’s anti-surveillance campaigners**

**BYLINE:** Janan Ganesh

**LENGTH:** 785 words

The latest and worst-written Bond film fires dud lines at you for 148 minutes you will never get back, but one really slices through with its badness. C, the movie's pantomime villain who all but twirls his moustache as head of British intelligence in Spectre, despairs of faint hearts who resist his quest for blanket surveillance. "And all in the name of democracy," he jeers, slowing to savour the profundity of his next three words. "Whatever that is."

Leave aside the undergraduate wit for a minute. What jars is the scriptwriters' attempt to pander to our paranoia about out-of-control spooks while hopelessly misjudging its extent. According to most survey evidence, democracy would not give C much trouble.

The demos is not liberal. Britons wanted 90-day detention without charge even as MPs voted it down 10 Novembers ago, defeating Tony Blair for the first time as prime minister. They wanted the "snooper's charter" that Theresa May is trying to steer through Parliament in revised form, starting this week. In a YouGov poll conducted in January, 63 per cent of respondents trusted the intelligence agencies to "behave responsibly" with the new surveillance measures contained in the home secretary's Investigatory Powers Bill -- more than trusted politicians and civil servants. We seem relaxed about the deep state, not just the state.

None of this means that voters are right or that governments should defer to their instincts. The public can be unanimously wrong. But the views do allow one conclusion. Judged by the depth of its imprint on popular sentiment, civil libertarianism is an almost uniquely unsuccessful political movement. Only campaigners for a British republic have had much less purchase on the national mood over the decades, and even they have the excuse of not really bothering. The jurists, celebrities and campaigners who make up the liberal lobby do exert themselves. They can coin a pejorative like "snooper's charter" and make it stick in columns such as this.

There is always a didactic film or play showing. But they never move beyond the curation of elite discourse. They have shaped media norms so that no broadcast interviewer ever asks a home secretary -- given what we know about public attitudes, or even just to hold her to account from an original angle -- why she is not seeking even more powers for the security state (just as no politician is asked why his latest cut to public spending does not go much deeper).
It is the average Briton they have failed to move. When Parliament stymied Mr Blair, it became modish to hail Liberty, the liberal pressure group, as the best campaigners in the land: folk heroes of a sort. But they lost the argument in the country. A nation of dazzling laxity on race, sex, God and so much else remained conservative on crime and security.

Libertarians are culpable for some of this. Their bludgeoning hyperbole -- government measures are "Kafkaesque", every home secretary is "draconian" -- is easy to dismiss. If they acknowledge a trade-off between freedom and safety, it is with a mealy mouth and an emotional tin ear. And they speak in a blur of abstract values to citizens who think in practical terms: it is no accident that the least popular, now forsworn, bit of Ms May's plans is the banning of encryption software, which might imperil online financial transactions. Invoking "our liberties", as if any normal person uses that possessive phrase, carries fewer people than itemising the tangible losses they stand to incur from heavy-handed government.

If civil libertarians need a consoling thought, here is one. Aside from the stylistic tweaks just mentioned -- the equivalent of revising a lousy film script -- there is not much more they can do. Voters are relaxed about the security services for reasons ingrained in their country's history. The British mainland is not scarred by experience of a police state in the way parts of continental Europe are. (Northern Ireland, with its memories of internment and the Diplock courts, is another matter.) Converting Britons to liberalism is no less a fool's errand than making them fervent Europeans. If independent nationhood has always worked for a country, supranational government will seem otiose. If the security state has not seriously menaced its life, libertarianism will smell like an answer to a question nobody asked.

The most British thing about James Bond is the very idea of a secret agent of the state who is benign. Such a character is trickier to concoct in the German, or even French or Italian, context. Britain's civil libertarians do important work in the wrong country.

Letter in response to this column:

Putting security ahead of privacy / From Joseph Grillo

LOAD-DATE: July 22, 2016
LANGUAGE: ENGLISH
PUBLICATION-TYPE: Web Publication

Copyright 2015 The Financial Times Ltd.
All Rights Reserved
Please do not cut and paste FT articles and redistribute by email or post to the web.

Return to List

12 of 104 DOCUMENTS

The Guardian

Theresa May faces fight over web browsing access; Labour and Nick Clegg prepare to contest snooper's charter plan to give intelligence agencies more powers

BYLINE: Patrick Wintour Political editor
SECTION: WORLD NEWS
LENGTH: 751 words

114
The home secretary, Theresa May, should not seek to give the intelligence agencies full access to an individual's web browsing history, Labour and the former deputy prime minister Nick Clegg are both likely to say when the government publishes its draft investigatory powers bill on Wednesday.

Keir Starmer, the former director of public prosecutions and now a shadow Home Office minister, said Labour opposed giving intelligence agencies access to web browsing history since the measure was likely to give the agencies effective access to the content of an individual's communications.

Related: The Guardian view on the draft investigatory powers bill: snooper's charter 3.0 | Editorial

He said: "There has been an agreed clear distinction between data and content, with data treated as the 'who communicated with whom and at what point', but not the content of that data.

"But by saying the agencies can collect information on pages visited, there is a sense that a difficult third category is being created that is a merger between data and content. If your browsing history is automatically accessible by the state, it is very close to granting full access to content and provides a picture of that individual's life.

"The independent reviewer of terrorism David Anderson said the case for accessing browsing history has not yet been proven and we in the Labour party are very closely aligned to what Anderson has recommended in his report since he is the expert with the fullest access to what is required. Theresa May will have to make a very compelling case for her proposals if they differ from Anderson."

Starmer has cleared his policy positions with the Labour leader, Jeremy Corbyn, and the shadow home secretary, Andy Burnham.

Starmer's warning will be a blow to the intelligence agencies before a parliamentary process that will scrutinise the plans to reach a new privacy settlement between the state and the citizen in the wake of controversy generated by the revelations of the former National Security Agency contractor Edward Snowden.

All sides in the highly charged debate acknowledge that a new set laws are required to replace the outdated Regulation of Investigatory Powers Act 2000 and the dozens of other statutes authorising the collection of communications data.

The issue of access to web browsing history is likely to prove as critical a point of contention as the weekend controversy over whether ministers or judges should grant warrants to the intelligence agencies.

It is expected that Clegg - who spent a huge amount of time on the issue in government and vetoed the so-called snooper's charter - will make the case for the government to follow the recommendations of the Anderson review. Clegg won David Cameron's agreement to commission work from the Royal United Services Institute for Defence and Security Studies that is likely to inform the debate.

In a 300-page report, Anderson said no operational case had yet been made for the retention of web logs, pointing out that no other European Union or Commonwealth country required the blanket retention of web logs and that Australia recently prohibited this in law.

Starmer said he rejected plans for a two-stage approval of in which the home secretary would make the initial decisions on authorising intercept warrants followed by clearance from a security-cleared judge if the intercept was to extend to the content of the communication.

Related: Investigatory powers bill: snooper's charter to remain firmly in place

Starmer said: "If you're going to go for contents, we should go to a judge straight off. There are roughly speaking about 2,500 warrants per year for interception. That's a very high number for a home secretary to deal with.

"It's a classically judge test: is it necessary, is it proportionate, is it focused on the right person? This is what's done in other countries. I think this would settle this dispute and it would allow everybody to move on."

Anderson proposed authorisation for all warrants be given by judicial commissioners serving in a new independent surveillance and intelligence commission (Isic). Anderson recommended that Isic should have additional powers to notify those subject to surveillance of their right to lodge an application at the Investigatory Powers Tribunal (IPT), which oversees MI5, MI6 and GCHQ.

The debate on Wednesday is likely to focus heavily on the extent to which May has backtracked since proposals were first made in 2012 and whether her concessions are substantive.
The Guardian view on the draft investigatory powers bill: snooper's charter 3.0;
The debate is getting lost in detail, amid 'concessions' on proposals that were never serious. But at core this week's draft legislation is about legitimising bulk data collection. The consequences are chilling

BYLINE: Editorial

SECTION: COMMENT IS FREE

LENGTH: 981 words

The home secretary will on Wednesday publish a draft bill to put on a statutory footing surveillance practices which the intelligence agencies still partly deny, and which they would have continued to deny completely were it not for a man they despise as a traitor.

Legislation to regularise the ubiquitous, clandestine prying that Edward Snowden revealed to the world represents an advance, even if it's an advance of an upside-down sort. Facing up to a problem is, after all, a precondition of fixing it. The airwaves are suddenly jammed with arguments about precise checks and balances, and Jesuitical distinctions between keeping records of every website visited as opposed to every page viewed. Again, it is better that such details should be chewed over than it would be to revert to the pre-Snowden blend of silence and denial. But what is bizarre in what passes for a British "debate" - in marked contrast to that in Washington and Berlin - is the one thing that's not up for discussion. Namely, whether or not it is desirable for the state to keep electronic tabs on all its citizens.

It is no accident that the discussion has grown confused. The British security state has form in spin: recall that the first draft of the infamous Iraq "intelligence dossier" turned out not to have been written by any expert but by a communications official. The agencies regularly run wild policies up the flagpole purely to create the impression of a fair-minded compromise when they are brought back down. With secret courts, for instance, the original proposal called for invisible inquests - that is, for the state to probe in private why people had died - an absurd demand, which was bartered away to get the wider legislation through. Something similar happened again between drafts one and two of the notorious snooper's charter. Back in 2012, much was made of the shift between the pre-2010 plan for an over-arching state communications database, to the subsequent scheme - which the Lib Dems blocked in coalition - for IT companies to be required to keep records that the state could then probe, a change that scarcely constrained the ability to snoop.
This week, in the run-up to the release of the snooper's charter Mark III, the Home Office is once again offering "concessions" concerning things it was never likely to do. So there will not, it is reported, be a blanket right for the police to spy on exactly what everybody has been up to on social media over the previous year, a suggestion that was never going to be effective unless foreign-owned corporations such as Google and Facebook were minded to risk worldwide reputations to help out the British bobby. There are whispers, too, of a climbdown over powers for the police to run the sort of intrusive probes that they are, in fact, quite content to leave to the security services. And there is convenient controversy about who should sign off on the 2,500 or so intercept warrants made annually, where some shift from political to judicial power is straightforward to grant, and likely already part of the plan for getting the legislation through. This noise allows for convenient silence about the 500,000-plus times a year that communications data, such as call records, is tapped without any warrant at all.

The argument that is needed, and the one that is not happening, concerns the routine collection of so-called "metadata". That term is an immediate turnoff, making it sound as if what is being discussed is profoundly prosaic information about, say, how many megawatts somebody was using, which could be of no possible interest to anybody but a technician. In fact, it reveals not only who is talking to whom and when, but may also include - depending on the precise technology being used - browsing histories, search terms and conceivably even passwords. It is information of this sort that, the novelist John Lanchester argues, may sometimes reveal that "you're gay" not only "before you tell your mum" but before you know yourself.

The bulk harvesting and routine analysis of the traces we all leave online has the potential to dissolve the very idea of privacy as it used to be understood, and it's not clear to what end. In the US, Barack Obama's surveillance panel cast doubt on the presumption that extra data would beget extra security, and the federal courts have ruled against bulk collection. In the UK, David Anderson, the terror laws watchdog, insists that a "detailed operational case" has to be made. But if Theresa May offers one this week, that will be a first. For at Westminster, there is no argument about whether the intelligence gains are worth the privacy lost, as it is complacently assumed that the only real prying will be on those who attract legitimate suspicion. It is as if the unending stream of leaks from supposedly secure databases, of which TalkTalk is only the latest, had never occurred; as if none of the myriad officials with access to such materials could ever have a corrupt motive to root around.

In other contexts, Britain has proved capable of having the argument and then striking a sensible balance between liberty from the state and freedom from crime. After Strasbourg ruled against the heavy-handed police practice of retaining DNA samples from everyone they had ever arrested, for instance, the coalition government eventually responded with a mix of time limits and a targeted focus on more serious crimes. With comms data, however, the plan continues to be to ensure that everything is collected, with a great deal being made accessible to very many state agents. The parallel is less with taking DNA during every arrest, than with taking the DNA of every new baby born. The country would never countenance that, of course, but with comms data the mood is incomparably more relaxed. That's largely because we have been artfully encouraged to talk about other things.

LOAD-DATE: November 2, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc.
All Rights Reserved

Return to List

14 of 104 DOCUMENTS

November 2, 2015 Monday 6:13 PM GMT
Lord Carlile criticises proposals for judges to approve spying warrants;
Former reviewer of terrorism legislation says it would be glib to require judicial oversight of applications by security services to intercept communications

BYLINE: Frances Perraudin

SECTION: UK NEWS

LENGTH: 872 words

It would be glib for the government to require judges to approve warrants to intercept communications, the former independent reviewer of terrorism legislation has said, as he called for an end to the "demonisation" of the security services.

Alex Carlile QC, a Liberal Democrat peer and former MP, was speaking ahead of the publication of a draft of the investigatory powers bill, due on Wednesday, amid a political debate about whether politicians should be stripped of the power to sign off intercept warrants.

"I think it is a rather glib comment to say 'get the judges to authenticate everything'," Lord Carlile told BBC Radio 4's Today programme. "Judges are, of course, very good quality men and women, [but] if judges are going to authenticate these issues, they have to learn about national security... At the moment, there is a handful of judges who have real understanding of national security."

The Home Office has so far refused to confirm whether or not the proposed legislation will include judicial approval of applications made by the security services to intercept communications. Ministers currently approve the 2,700 warrants a year to tap into the contents of messages.

Related: Online surveillance bill 'will fall without judicial oversight'

Carlile, who served as the independent reviewer of terrorism legislation between 2001 and 2011, said he could not remember seeing a politician "make a decision which was against the interests of the privacy of the public".

"One should be very careful of simply saying 'politicians are malignant therefore we must protect the public against any possible future malignancy of an individual politician'" he said.

"By and large, politicians do actually try to get things right, and they really do have an interest in the balance between the safety of the public and the privacy of the individual. That's what they agonise over."

Carlile said he was concerned that the police and security service had been demonised when they were actually "the unsung heroes" who kept Britain safe: "I think it's absurd to suggest that the police and the security services have a kind of casual desire to intrude on the privacy of the innocent."

Speaking on ITV's This Morning on Monday, David Cameron said we should not give terrorists, criminals and child abductors "safe spaces" to communicate. "It's not a safe space for them to communicate on a fixed-line telephone or a mobile phone; we shouldn't allow the internet to be a safe space for them to communicate and do bad things," he said.

Asked about the issue of judicial oversight, Cameron said: "We'll set out our plans on Wednesday, but politicians have a role - not least to get this area of law right."

The Times reports (paywall) that the investigatory powers bill could outline a two-stage approvals process in which the home secretary, Theresa May, would give the initial authorisation to intercept warrants, followed by confirmation of that decision from a senior judge with security clearance.

Labour, the Lib Dems and some backbench Conservatives have already expressed reservations about the existing system of ministerial approval.

Related: Don't be fooled by spook propaganda: the state still wants more licence to pry | Henry Porter
Speaking on BBC1’s Sunday Politics show, the former Conservative shadow home secretary David Davis said plans to grant police and intelligence officers new powers to monitor suspects online would not get through parliament without a requirement for judges to sign off on spying warrants.

"Actually I don't think this bill will get through either [the] Commons or Lords without judicial authorisation ... There's a new consensus on this right across the board - across the experts, across the spooks, across the parties, across both houses of parliament," he said.

The Home Office said it had dropped several contentious proposals from the bill, including plans to give the police and security services full access to everyone's internet browsing history. The climbdown was prompted by concerns that the government would be unable to get the legislation through parliament because of unease of its implications for civil liberties.

A report published in June by David Anderson QC recommended that judicial rather than ministerial authorisation of individual, targeted intercept warrants should be required. His position runs counter to the intelligence and security committee, which said in March that responsibility should remain with ministers. The Royal United Services Institute (pdf) favours an approach under which the government authorises some warrants and others are left to judges.

Labour's shadow cabinet has agreed that the party will not support the investigatory powers bill unless it includes judicial oversight of national security warrants. Speaking on the Murnaghan programme on Sky News on Sunday, the former Liberal Democrat leader Paddy Ashdown said the upper house would ensure that judicial oversight of warrants was added to the bill if it were not included in the draft.

"This is precisely constitutionally the kind of bill within which we should be intervening if indeed the legislation is deficient," he said.

LOAD-DATE: November 2, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc.
All Rights Reserved

Return to List

15 of 104 DOCUMENTS

The Guardian

November 2, 2015 Monday 4:57 PM GMT

New law to tell internet service providers to retain browsing data; Lobbying by police ahead of investigatory powers bill suggests ISPs will be required to keep data for 12 months

BYLINE: Owen Bowcott, Aisha Gani and Alex Hern

SECTION: LAW

LENGTH: 861 words

Powers to view the web browsing history of criminal suspects or missing people are likely to feature in the government's surveillance legislation published next week.
The **investigatory powers bill** is expected to reintroduce a requirement that telecommunication firms retain records of sites accessed by their users, known as weblogs, for a 12-month period - a key element of the "snooper's charter" that was blocked by Liberal Democrats in the last parliament.

Lobbying by senior police officers from the National Police Chiefs' Council for mandatory retention of internet connection records comes ahead of the draft bill being published.

In a statement released on Friday, the organisation which represents senior police officers said police forces did not need access to everyone's entire web history but added: "We do want to be effective in the digital world so that there aren't no-go areas online where we can't trace criminal activity or find crucial information to protect people at risk of harm. We want to do this with strong, clear privacy safeguards."

Police said they need the powers because the scale of online activity meant traditional methods of surveillance and investigation were becoming less effective.

Related: Theresa May named internet villain of the year

Civil liberty groups and privacy campaigners, however, have responded with alarm at the prospect of a key feature of the snooper's charter being reintroduced. Rachel Robinson, policy officer for Liberty, said: "It defies belief that the government continues to seek powers so extraordinarily intrusive that none of our major intelligence allies think them acceptable to use on their people."

"These measures have already been rejected by a cross-party parliamentary committee and the independent reviewer of terrorism legislation [David Anderson QC]. We will resist them in the strongest terms and urge right-thinking parliamentarians to do the same." Anderson has not been enthusiastic about such an enhancement of search powers. No other EU or Commonwealth country requires the blanket retention of weblogs, he has pointed out; the practice was recently prohibited by law in Australia.

Anderson has commented that "a detailed operational case" needs to be made out for retaining weblogs along with "a rigorous assessment" of the "lawfulness, likely effectiveness, intrusiveness and cost" involved.

Weblogs record which web addresses users have visited, though they do not keep track of what was viewed on any particular site.

The address of a website often contains far more detail than simply the name of the company being visited. A record of browsing history would necessarily contain all internet searches made using websites including Google, Bing and DuckDuckGo, since the address for the search results page contains the search terms within it.

Any requirement that firms retain browsing histories for a year is likely to be presented with Home Office assurances that it will be carefully controlled by additional safeguards preventing mass surveillance.

GCHQ, the government's monitoring agency, and the intelligence services say they carry out bulk interception of online data only in order to investigate or read communications that are the subject of search warrants.

Internet service providers have warned that any new powers introduced by the government to allow broader surveillance of web browsing behaviour must come with adequate oversight to protect civil liberties.

Related: DuckDuckGo traffic soars in wake of Snowden revelations

The Internet Service Providers' Association (ISPA) said it had sent a checklist of principles to MPs that it believes any new legislation must adhere to.

The section on transparency and oversight reads: "We encourage parliamentarians to be wary of arguments that the **investigatory powers bill** will merely update existing powers and fill a gap in data availability.

"The nature of surveillance, investigatory powers and technology have changed as communications have evolved from phone and post to online communication, leading to even existing powers becoming more intrusive over time."

Andrew Kernahan, ISPA spokesman, said: "Once the bill is published we will be going through it with a fine-toothed comb."
"What we do know is that internet connection records that the government wanted was included in the
draft communications data bill that was rejected by parliament."

In September Andrew Parker, director-general of MI5, took the unprecedented step of giving a live
broadcast interview with BBC Radio 4's Today programme, in which he called for "the cooperation of
the companies who run and provide services over the internet" to help tackle the use of encrypted
communications by terrorists.

Parker said: "MI5 and others need to be able to navigate the internet to find terrorist communication.
We need to be able to use datasets to be able to join the dots to be able to find and stop the terrorists
who mean us harm before they are able to bring plots to fruition.

"We have been pretty successful at that in recent years but it is becoming more difficult to do it as
technology changes faster and faster [and] encryption comes in."

Lord Carlile criticises proposals for judges to approve spying
warrants;  
Former reviewer of terrorism legislation says it would be glib to
require judicial oversight of applications by security services to
intercept communications

BYLINE: Frances Perraudin

It would be glib for the government to require judges to approve warrants to intercept
communications, the former independent reviewer of terrorism legislation has said, as he called for
an end to the "demonisation" of the security services.

Alex Carlile QC, a Liberal Democrat peer and former MP, was speaking ahead of the publication of a
draft of the investigatory powers bill, due on Wednesday, amid a political debate about whether
politicians should be stripped of the power to sign off intercept warrants.

"I think it is a rather glib comment to say 'get the judges to authenticate everything',' Lord Carlile told
BBC Radio 4's Today programme. "Judges are, of course, very good quality men and women, [but] if
judges are going to authenticate these issues, they have to learn about national security... At the
moment, there is a handful of judges who have real understanding of national security."
The Home Office has so far refused to confirm whether or not the proposed legislation will include judicial approval of applications made by the security services to intercept communications. Ministers currently approve the 2,700 warrants a year to tap into the contents of messages.

Related: Online surveillance bill 'will fall without judicial oversight'

Carlile, who served as the independent reviewer of terrorism legislation between 2001 and 2011, said he could not remember seeing a politician "make a decision which was against the interests of the privacy of the public".

"One should be very careful of simply saying 'politicians are malignant therefore we must protect the public against any possible future malignancy of an individual politician','" he said.

"By and large, politicians do actually try to get things right, and they really do have an interest in the balance between the safety of the public and the privacy of the individual. That's what they agonise over."

Carlile said he was concerned that the police and security service had been demonised when they were actually "the unsung heroes" who kept Britain safe: "I think it's absurd to suggest that the police and the security services have a kind of casual desire to intrude on the privacy of the innocent."

The Times reports (paywall) that the investigatory powers bill could outline a two-stage approvals process in which the home secretary, Theresa May, would give the initial authorisation to intercept warrants, followed by confirmation of that decision from a senior judge with security clearance.

Labour, the Lib Dems and some backbench Conservatives have already expressed reservations about the existing system of ministerial approval.

Related: Don't be fooled by spook propaganda: the state still wants more licence to pry | Henry Porter

Speaking on BBC1's Sunday Politics show, the former Conservative shadow home secretary David Davis said plans to grant police and intelligence officers new powers to monitor suspects online would not get through parliament without a requirement for judges to sign off on spying warrants.

"Actually I don't think this bill will get through either [the] Commons or Lords without judicial authorisation ... There's a new consensus on this right across the board - across the experts, across the spooks, across the parties, across both houses of parliament," he said.

The Home Office said it has dropped several contentious proposals from the bill, including plans to give the police and security services full access to everyone's internet browsing history. The climbdown was prompted by concerns that the government would be unable to get the legislation through parliament because of unease of its implications for civil liberties.

A report published in June by David Anderson QC recommended that judicial rather than ministerial authorisation of individual, targeted intercept warrants should be required. His position runs counter to the intelligence and security committee, which said in March that responsibility should remain with ministers. The Royal United Services Institute (pdf) favours an approach under which the government authorises some warrants and others are left to judges.

Labour's shadow cabinet has agreed that the party will not support the investigatory powers bill unless it includes judicial oversight of national security warrants. Speaking on the Murnaghan programme on Sky News on Sunday, the former Liberal Democrat leader Paddy Ashdown said the upper house would ensure that judicial oversight of warrants was added to the bill if it were not included in the draft. "This is precisely constitutionally the kind of bill within which we should be intervening if indeed the legislation is deficient," he said.

LOAD-DATE: November 2, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc.
All Rights Reserved
Grant the spies their powers - but force them to speak up; When a tiny light is shone on MI5 and MI6, as in the Commons' hearing two years ago, there is no threat

BYLINE: Steve Richards

SECTION: VOICES

LENGTH: 1057 words

We are hearing a lot of noise about what is known -in an example of how political language can distort an issue - as the Snooper's Charter. The noise distorts the facts almost as much as that misleading piece of terminology.

No one wants or expects spies or the police to follow all of us as we plan what to do on a foggy night in November. But there is little dispute over the proposition that in an era where the internet and mobile phones are the main source of communication, spies and the police need greater access to such material. The main area of debate is over the theoretically dry topic of accountability. In the UK the question of who is accountable to whom is almost as emotive a theme as privacy and surveillance. Who should oversee the overseers? Should it be a Home Secretary? Should it be a judge? The questions are highly charged because they are linked to the role of the state, a debate that begins in virtually every policy area with assumptions of sinister intent.

The broadest concerns of Theresa May's critics are understandable and must be addressed. Powers can be abused and no institution is free from individuals or a culture that is capable of abusing them. From what we know, the intelligence agencies and the police are flawed institutions, capable of terrible error or worse. Any organisation that worked on the deranged assumption that the former Labour Prime Minister, Harold Wilson, was a communist - as some foolish spies assumed in the late 1960s and early 1970s - needs to be kept under intense scrutiny. Goodness knows what parts of MI6 would make of Jeremy Corbyn's internet details if some thought Wilson dangerously left wing. The police too are far from error-free and some will no doubt make mistakes or deliberately abuse access to records. But again no supporter of May's latest proposals, to be unveiled tomorrow, will disagree with the need for accountability. The thorny question becomes how agencies, more often than not used to functioning in the dark, can be held to account.

The former adviser on security legislation, Lord Carlile, a Liberal Democrat, pointed out on the BBC that a Home Secretary will challenge the intelligence agencies at least as much as a judge in granting access in emergency situations. He added that the home secretaries he had worked with always had been robust in the past. This is hardly surprising. There will always be immense countervailing pressures on home secretaries to show that they are not "invading" people's privacy unnecessarily. An elected Home Secretary is more accountable than a judge, who does not have to answer in any arena as to why he or she has made a decision.

In response to such powerful arguments the senior Conservative MP, David Davis, and smartly forensic critic, points out that home secretaries do not explain in public either, hiding behind the convenient shield that responding to questions might threaten national security. Davis argues there is no greater accountability when a Home Secretary oversees sensitive security decisions. He is one of the few MPs who recognises the centrality of accountability as a way of keeping many different institutions and agencies on their toes.
When writing about refugees, be more sensitive than Teresa May

But that is not necessarily a case for insisting on judicial oversight and ceding all political control. In both the case of the silent Home Secretary and the lack of public scrutiny in relation to intelligence agencies, there are ways to provide much higher levels of transparency. When a tiny amount of daylight is shone on the security services, such as the rare public hearing two years ago of the Commons’ intelligence committee questioning spy chiefs, there is no threat to national security. With greater access to internet and phone information must come more public explanation as to why and how the new powers are being used. "We cannot say anything in order to protect national security" must be protective words deployed rarely.

The feverish paranoia about "surveillance" reflects an unsurprising suspicion of the state in all its manifestations. In the UK of the 21st century the attitudes follow a familiar pattern: a Home Secretary cannot be trusted because he or she is a politician, a judge can be trusted because he or she is not an elected politician and the state is always an instrument of stifling oppression and never one that can act benevolently.

Most of the time ministers imply by their actions that the state in the UK can never be a force for good. The Chinese can finance the UK's nuclear power stations, but not the poor old UK state. The German and Dutch governments can own train companies, but the British Government cannot. Charities are hailed as innovative deliverers of services, until they go bust when the state agonises about why it regulated so complacently. When a Home Secretary proclaims the need for the state to have access to private information there is understandable anxiety, heightened by the proposition that an elected politician will have some oversight.

Concessions to surveillance bill unlikely to head off peer revolt

UK Government forced into huge climbdown over giving spies new powers

New hacking laws for spies to be introduced in coming weeks

But the wariness is based partly on a disproportionate self-importance. I have met some of the most boring people in the Western world who pompously assume they must be protected from the probing interests of the snoopers. They should be so lucky that anyone would be remotely interested in them. The snoopers will be too busy following 10,000 other trails to bother with what any of us get up to.

As with the bankrupt charity Kids Company, the "free" school that underperforms and the hospital that fails its patients, questions of accountability are complex. But in each case a greater level of scrutiny would act as a deterrent against incompetence or abuse. In the case of national security, let the spies spy and be held to account more fully for what they do and how they do it. Elected politicians must have a role in the decision making and in challenging the decision makers.
Ministers have dropped pledge to crack down on secret messaging apps
Jihadi recruiters use services with encryption to recruit new people
Online banking and sites like Facebook and WhatsApp rely on encryption
Theresa May said decision to not ban encryption was made because the process was vital to all modern communications

 Ministers have dropped a pledge to crack down on secret messaging apps used by jihadi recruiters to groom British children.

In January, David Cameron indicated he wanted to ban 'encryption' or weaken it, to allow security services to read what terrorists are saying.

But yesterday, the Home Secretary revealed that the draft Investigatory Powers Bill, to be published this week, will not ban encryption.

Theresa May said this was because the process was vital to all modern communications.

Online banking, as well as social media sites such as Facebook and WhatsApp, rely on encryption.

In May, a Daily Mail investigation revealed encrypted mobile phone apps are at the heart of attempts by Islamic State recruiters to target teenagers in Britain and prime them for jihad.

Among those using such apps were former Cardiff students Nasser Muthana, 20, and Reyaad Khan, 21, who joined IS and featured in a recruitment video for the terror group. Khan was later killed in an RAF drone strike.

The apps were developed by extremists to send messages that cannot be read by the authorities.

Security experts have warned it would not be possible to ban messaging apps that use encryption.

The Prime Minister spoke of his desire to see an end to encryption after the Charlie Hebdo massacre in January.

He said: 'In extremis, it has been possible to read someone's letter, to listen to someone's call... The question remains: are we going to allow a means of communications where it simply is not possible to do that? My answer to that question is: no, we must not.'

A year before, he had said: 'Are we prepared to have a means of communication, the internet and a number of modern methods, that we are not able to intercept? My answer is clear: we should not accept that. We should legislate to ensure that that is the case.'

But computer security expert Graham Cluley said at the time: 'Cameron is living in cloud cuckoo land if he thinks that this is a sensible idea ... it wouldn't be possible to implement properly.'

Yesterday, Mrs May told BBC1's Andrew Marr Show: 'We're not banning encryption. Encryption is important for people to be able to keep themselves safe when they're dealing with these modern communications in the digital age.

'But what we'll be doing is setting out the current position, which does enable the authorities with proper authorisation to issue warrants.'

Pressed on Mr Cameron's comments, she said: 'The first duty of any government is to keep our country and our people safe, which is precisely why we are bringing forward the Investigatory Powers Bill... [and] setting out a very clear legal framework, clearer than previously.'

Internet experts say encryption technology used by terrorists is also used for legitimate functions such as keeping online banking data safe and ensuring messages are read only by the intended recipients.
Robin Simcox, of think-tank the Henry Jackson Society, said an increase in encryption, enabling terrorists to communicate in a more secure way, was a 'huge challenge for our security services'.

He added: 'I don't believe the Conservatives ever really were considering banning it. It's not practical ... A hole in encryption for our security services' benefit is also one that could be exploited by our adversaries.'

A Home Office spokesman said encryption was 'ensuring safe online commerce and protecting people's personal data'. But she added that companies must be able to 'access the content of communications on their networks when presented with a warrant, as many of them already do for their own business purposes'.

"The Investigatory Powers Bill will give protection to journalists' sources. Theresa May has vowed to stop police using anti-terror powers to access reporters' email or phone records unless they have broken the law or serious crime is being investigated.

LOAD-DATE: November 2, 2015
LANGUAGE: ENGLISH
PUBLICATION-TYPE: Web Publication
JOURNAL-CODE: WEBDM

Copyright 2015 Associated Newspapers Ltd.  
All Rights Reserved

Return to List

19 of 104 DOCUMENTS

telegraph.co.uk

November 2, 2015 Monday 5:12 PM GMT

Internet firms to be banned from offering unbreakable encryption under new laws;
Companies such as Apple, Google and others will no longer be able to offer encryption so advanced that even they cannot decipher it when asked to under the Investigatory Powers Bill

BYLINE: By Tom Whitehead Security Editor
SECTION: NEWS
LENGTH: 705 words

Internet and social media companies will be banned from putting customer communications beyond their own reach under new laws to be unveiled on Wednesday.

Companies such as Apple, Google and others will no longer be able to offer encryption so advanced that even they cannot decipher it when asked to, the Daily Telegraph can disclose.

Measures in the Investigatory Powers Bill will place in law a requirement on tech firms and service providers to be able to provide unencrypted communications to the police or spy agencies if requested through a warrant.

∑ Councils and taxman to be given power to view your internet history
The move follows concerns that a growing number of encryption services are now completely inaccessible apart from to the users themselves.

It came as David Cameron, the Prime Minister, pleaded with the public and MPs to back his raft of new surveillance measures.

He said terrorists, paedophiles and criminals must not be allowed a "safe space" online.

Ministers have no plans to ban encryption services because they have an important role in the protection of legitimate online activity such as banking and personal data.

But there is concern over some aspects of so-called end-to-end encryption where only the sender and recipient of messages can decipher them.

Terrorists and criminals are increasingly using such technology to communicate beyond the reach of MI5 or the police.

On its website, Apple promotes the fact that it has, for example, "no way to decrypt iMessage and FaceTime data when it's in transit between devices".

It adds: "So unlike other companies' messaging services, Apple doesn't scan your communications, and we wouldn't be able to comply with a wiretap order even if we wanted to."

Last month, Metropolitan assistant commissioner Mark Rowley, the country's most senior counter-terrorism officer, warned that for some firms it was "a part of their strategy - they design their products in full recognition that they will be unable to help us because of the way they have designed them".

However, proposals to be published on Wednesday will, for the first time, place a duty on companies to be able to access their customer data in law.

A Home Office spokesman said: "The Government is clear we need to find a way to work with industry as technology develops to ensure that, with clear oversight and a robust legal framework, the police and intelligence agencies can access the content of communications of terrorists and criminals in order to resolve police investigations and prevent criminal acts.

"That means ensuring that companies themselves can access the content of communications on their networks when presented with a warrant, as many of them already do for their own business purposes, for example to target advertising. These companies' reputations rest on their ability to protect their users' data."

The Investagatory Powers Bill is also expected to maintain the current responsibility for signing off requests to snoop with the Home Secretary but with extra judicial oversight - a move that is likely to anger civil liberty campaigners and some Tory backbenchers.

It will also require internet companies to retain the web browsing history of their customers for up to a year.

The bill is expected to face a tough route through parliament but Mr Cameron urged critics to back the measures.

He told ITV's This Morning: "As Prime Minister I would just say to people 'please, let's not have a situation where we give terrorists, criminals, child abductors, safe spaces to communicate'.

"It's not a safe space for them to communicate on a fixed line telephone or a mobile phone, we shouldn't allow the internet to be a safe space for them to communicate and do bad things."

Lord Carlile, the former terrorism laws watchdog, said there had been a "lot of demonization" of the police and security services over their intentions for such information.

"I think it is absurd to suggest the police and the security services have a kind of casual desire to intrude on the privacy of the innocent," he said.

"They have enough difficulty finding the guilty. No-one has produced any evidence of casual curiosity on part of the security services."
Nobody is listening to the anti-surveillance campaigners

BYLINE: Janan Ganesh on Politics

SECTION: COMMENT; Pg. 9

LENGTH: 773 words

The latest and worst-written Bond film fires dud lines at you for 148 minutes you will never get back, but one really slices through with its badness. C, the movie's pantomime villain who all but twirls his moustache as head of British intelligence in Spectre, despairs of faint hearts who resist his quest for blanket surveillance. "And all in the name of democracy," he jeers, slowing to savour the profundity of his next three words. "Whatever that is."

Leave aside the undergraduate wit for a minute. What jars is the scriptwriters' attempt to pander to our paranoia about out-of-control spooks while hopelessly misjudging its extent. According to most survey evidence, democracy would not give C much trouble.

The demos is not liberal. Britons wanted 90-day detention without charge even as MPs voted it down 10 Novembers ago, defeating Tony Blair for the first time as prime minister. They wanted the "snooper's charter" that Theresa May is trying to steer through Parliament in revised form, starting this week. In a YouGov poll conducted in January, 63 per cent of respondents trusted the intelligence agencies to "behave responsibly" with the new surveillance measures contained in the home secretary's Investigatory Powers Bill - more than trusted politicians and civil servants. We seem relaxed about the deep state, not just the state.

None of this means that voters are right or that governments should defer to their instincts. The public can be unanimously wrong. But the views do allow one conclusion. Judged by the depth of its imprint on popular sentiment, civil libertarianism is an almost uniquely unsuccessful political movement. Only campaigners for a British republic have had much less purchase on the national mood over the decades, and even they have the excuse of not really bothering. The jurists, celebrities and campaigners who make up the liberal lobby do exert themselves. They can coin a pejorative like "snooper's charter" and make it stick in columns such as this.

There is always a didactic film or play showing. But they never move beyond the curation of elite discourse. They have shaped media norms so that no broadcast interviewer ever asks a home secretary - given what we know about public attitudes, or even just to hold her to account from an original angle - why she is not seeking even more powers for the security state (just as no politician is asked why his latest cut to public spending does not go much deeper).

It is the average Briton they have failed to move. When Parliament stymied Mr Blair, it became modish to hail Liberty, the liberal pressure group, as the best campaigners in the land: folk heroes of a sort. But they lost the argument in the country. A nation of dazzling laxity on race, sex, God and so much else remained conservative on crime and security.

Libertarians are culpable for some of this. Their bludgeoning hyperbole - government measures are "Kafkaesque", every home secretary is "draconian" - is easy to dismiss. If they acknowledge a trade-off between freedom and safety, it is with a mealy mouth and an emotional tin ear. And they speak in a blur of abstract values to citizens who think in practical terms: it is no accident that the least popular,
now forsworn, bit of Ms May's plans is the banning of encryption software, which might imperil online financial transactions. Invoking "our liberties", as if any normal person uses that possessive phrase, carries fewer people than itemising the tangible losses they stand to incur from heavy-handed government.

If civil libertarians need a consoling thought, here is one. Aside from the stylistic tweaks just mentioned - the equivalent of revising a lousy film script - there is not much more they can do. Voters are relaxed about the security services for reasons ingrained in their country's history. The British mainland is not scarred by experience of a police state in the way parts of continental Europe are. (Northern Ireland, with its memories of internment and the Diplock courts, is another matter.)

Converting Britons to liberalism is no less a fool's errand than making them fervent Europeans. If independent nationhood has always worked for a country, supranational government will seem otiose. If the security state has not seriously menaced its life, libertarianism will smell like an answer to a question nobody asked.

The most British thing about James Bond is the very idea of a secret agent of the state who is benign. Such a character is trickier to concoct in the German, or even French or Italian, context. Britain's civil libertarians do important work in the wrong country.

janan.ganesh@ft.com

LOAD-DATE: November 2, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

Copyright 2015 The Financial Times Ltd.
All Rights Reserved
Please do not cut and paste FT articles and redistribute by email or post to the web.

Return to List

21 of 104 DOCUMENTS

The Guardian

November 3, 2015 Tuesday 11:00 PM GMT

May calls for internet companies to store details of website visits; Home secretary tries to sweeten snooper's charter by stating that police will need judicial approval to access internet connection records

BYLINE: Alan Travis

SECTION: WORLD NEWS

LENGTH: 970 words

Theresa May is to propose a major extension of the surveillance state when she publishes legislation requiring internet companies to store details of every website visited by customers over the previous year.

The home secretary will try to sweeten the pill of her revived snooper's charter on Wednesday by announcing that the police will need to get judicial authorisation before they can access the internet connection records of an individual - something that is currently banned in the US and every European country, including Britain.
She will also try to strengthen the oversight of Britain's surveillance by replacing the current fragmented system of three separate commissioners with an investigatory powers commissioner who will be a senior judge appointed by the prime minister on the recommendation of the lord chief justice.

Two and a half years after the disclosures by the whistleblower Edward Snowden of the scale of secret mass surveillance undertaken by Britain's security agency GCHQ, the bill will for the first time put into "comprehensive and comprehensible" legislation the existing bulk-collection powers of the security and intelligence services.

The draft investigatory powers bill will also enshrine in statute GCHQ's licence to hack into computers worldwide, including powers to sweep up content of a computer or smartphone, listen to phonecalls, track locations or even switch on the microphones or cameras on mobile phones. The powers, known as "computer network exploitation", even allow them to record conversations or snap pictures of anyone nearby the device.

May will tell the Commons that the powers are crucial to the security and intelligence agencies and police dealing with serious crime, including murder, child sexual exploitation and tracking online fraudsters and locating missing people.

She will insist that the new surveillance law will only amount to "updating existing powers while strengthening oversight and transparency", but privacy groups regard the requirement that everyone's internet connection records be stored by web and phone companies as a major extension of surveillance powers.

At the heart of the draft bill is the proposal that the records of every website visited by every British citizen are retained. It stops short of a detailed history of their web browsing as it will not record every page visited or every click, but the measure is banned as too intrusive a method of surveillance in the USA, Canada, Australia and every other European country. It is also banned in Britain under the terms of the 2015 Counter-Terrorism and Security Act because of fears that such data might fall into the wrong hands.

David Anderson QC, the terror legislation watchdog commissioned to report on the state of Britain's surveillance laws in the aftermath of Snowden's disclosures, has previously said that internet connection records included storing details of every website visited up to the first forward slash in their address - but not a detailed record of all web pages on a particular site. The internet connection records will also include times of contacts and the addresses of the other computers or services with which the user made contact.

"Under this definition a web log would reveal that a user had visited eg google.com or bbc.co.uk but not the specific page," said Anderson in his report, A Question of Trust. "It could also of course reveal... that a user has visited a pornography site or a site for sufferers of a particular medical condition, though the Home Office tells me it is in practice very difficult to piece together a browsing history."

The home secretary is also to propose a two-stage compromise over the current system of ministerial authorisation of the 2,700 warrants each year that allow the security services and police to intercept the content of calls and messages, with a panel of vetted judges having the power to veto her decisions.

She is also expected to announce that the police will need pre-authorisation from the same panel of vetted judges to access website viewing histories, the so-called individual internet connection records.

The current system under which more than 500,000 requests a year to access personal communications data - the who, what, where and when of our phone and web use - by the police will continue without the need for any warrant. Only local authorities and some other public bodies will need permission of a magistrate to access this metadata.

Government sources said that a new criminal offence carrying a two-year prison sentence will be created to prevent abuse of such communications data by public authorities, and local authorities will be banned entirely from acquiring internet connection records. They confirmed that "strong controls" will be imposed on access to these records.

Jim Killock of the Open Rights Group, which is part of the Don't Spy on Us coalition of privacy campaign groups in Britain, said the bill would be seen by many as a return of the snooper's charter blocked by Nick Clegg and the Liberal Democrats in the coalition.

"There is no doubt that our surveillance laws need to be reformed and it is unlikely that we will oppose this bill in its entirety," he said.
"However, the bulk retention of British citizens' data, whether or not they are suspected of a crime, is highly intrusive. We expect this bill will increase the types of personal data that is retained and many people will see that as a return of the snooper's charter.

"Ensuring that the police have to go to judges for access to this data is a welcome step but we also need to see restriction on what information is kept about each of us in the first place," he added.

"This bill will redefine the relationship between the state and the public for a generation and it is vital that the government gets it right."

LOAD-DATE: November 3, 2015
LANGUAGE: ENGLISH
PUBLICATION-TYPE: Newspaper
JOURNAL-CODE: WEBGNS

The key elements of the snooper's charter, including the bulk collection and storage for 12 months of everyone's personal data, tracking their use of the web, phones and social media, will remain firmly in place when the government publishes its new investigatory powers bill on Wednesday.

The legislation, to be introduced by the home secretary, Theresa May, will provide the security services with an explicit licence to "snoop on the web" for the first time.

Until the disclosures of the whistleblower Edward Snowden, these powers and mass surveillance programmes remained hidden in the complex undergrowth of the pre-digital age Regulation of Investigatory Powers Act 2000 (Ripa) and other arcane surveillance laws.

The new, comprehensive, surveillance legislation will provide the security services and police with access to personal web and phone data using bulk-collection powers and will also put on a fresh legal footing spies' mass computer hacking, known as "computer network exploitation".

Related: Lord Carlile criticises proposals for judges to approve spying warrants

In the runup to the bill's publication May has made much of having removed some of the more contentious elements from her previous attempt to introduce the snooper's charter in parliament,
which was blocked by her Liberal Democrat coalition partners. So is this week's new surveillance law a climbdown or is it still a snooper's charter?

What personal data does Theresa May want companies to collect?

Internet and phone companies are expected to be required to keep the communications data of all their customers' use of the web, their phones and social media for 12 months. This is not the content, which has to be authorised by a ministerial intercept warrant, but the who, what, where and when of everyone's use of the web.

It is often the case that the "who sent what to whom from where" can be more useful to the security services and police than the actual content of messages because it can tell them a lot about an individual's life, and represents hard evidence.

It is easy to lie in the writing of an instant message but far harder to lie over when and to whom it was sent. This is reflected in the fact that communications data can be used as evidence in court while information obtained via interception is not admissible and can only be used for intelligence.

The Home Office will pay the internet and phone companies an as-yet unspecified (but no doubt large) sum to store this data and to provide access to the security services and the police according to specified regimes.

What will GCHQ be able to do with that data?

The security and intelligence services will use the bulk collection of personal internet data by the web and phone companies as the basis of GCHQ's powerful data-mining programs to generate intelligence data.

Related: Don't be fooled by spook propaganda: the state still wants more licence to pry | Henry Porter

It is the activity of the hundreds of such programs that campaigners say amounts to the snooper's charter invasion of privacy.

The police, who make the bulk of the 500,000 external requests for communications data each year, have a separate regime with approval at inspector or superintendent level depending on the kind of data being requested for use in crime investigations. This includes terrorism investigations but also stalking and missing persons cases.

The bill is expected to add a category of internet connection records that will allow the police to trace which websites a suspect has visited, but not the content of pages. This is expected to require judicial authorisation, which is likely to be in the form of a panel of specially trained retired judges and requests will have to be targeted and limited.

They may also be required to authorise police requests for the communications data of journalists, lawyers or other legally privileged professions.

A further 40 public bodies also get different levels of access but often will need a magistrate's authorisation. But the vast majority of the 500,000 requests made each year will continue as now without the need for a judicial or ministerial warrant.

Will US internet companies such as Google and Facebook be affected by the new law?

The home secretary has given up trying to force overseas web companies to meet British requests to hand over their customers' data. She has also dropped her plan to get UK-based companies to keep "third party" data that passes over their networks if the US companies refused to cooperate.

Instead, May has decided to rely on the recommendations of Sir Nigel Sheinwald, the former British ambassador to Washington, who earlier this year told the government that the only way to solve this problem was to negotiate a new treaty with the US to secure a rapid response to requests.

Does David Cameron still want to ban encryption?

When the prime minister visited Washington earlier this year he gave the impression that he wanted to ban encryption on the web, arguing that there should be no safe space for terrorists or paedophiles. Ministers have ruled out for now any such ban or restriction on encryption, which would have severely undermined Britain as a global business centre.

What will the security services get out of it?
The bill will enshrine the security services' licence to hack, bug and burgle their way across the web. Britain's security services only officially admitted that they had worldwide powers to attack computers this year.

As a result of a court case, an innocuous-sounding "draft equipment interference code of practice" was published by the Home Office. This put into the public domain the rules and safeguards surrounding the use of computer hacking outside the UK by the security services for the first time.

Privacy campaigners said the powers outlined in the draft guidance detailed the powers of intelligence services to sweep up content of a computer or smartphone, listen to their phone calls, track their locations or even switch on the microphones or cameras on mobile phones. The last would allow them to record conversations near the phone or laptop and snap pictures of anyone nearby.

Who will oversee this new regime?

Theresa May faces strong parliamentary opposition to continued ministerial authorisation of the 2,400-a-year intercept warrants she currently signs. She has already offered a two-stage compromise by floating the idea of a judicial veto on her authorisations. She is also expected to announce that the fragmented system of five separate oversight commissioners is replaced with a single investigatory powers commissioner, who would be a senior judge, to hold the security services and police to account.

LOAD-DATE: November 3, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Give spies power, but make them explain why they need it

BYLINE: STEVE RICHARDS

SECTION: COMMENT; Pg. 27

LENGTH: 975 words

We are hearing a lot of noise about what is known - in an example of how political language can distort an issue - as the Snooper's Charter. The noise distorts the facts almost as much as that misleading piece of terminology.

No one wants or expects spies or the police to follow all of us as we plan what to do on a foggy night in November. But there is little dispute over the proposition that in an era where the internet and mobile phones are the main source of communication, spies and the police need greater access to such material. The main area of debate is over the apparently dry topic of accountability. In the UK the question of who is accountable to whom is almost as emotive a theme as privacy and surveillance. Who should oversee the overseers? Should it be a Home Secretary? Should it be a judge? The
questions are highly charged because they are linked to the role of the state, a debate that begins in virtually every policy area with assumptions of sinister intent.

The broadest concerns of Theresa May's critics are understandable and must be addressed. Powers can be abused and no institution is free from individuals or a culture that is capable of abusing them. From what we know, the intelligence agencies and the police are flawed institutions, capable of terrible error or worse. Any organisation that worked on the deranged assumption that the former Labour Prime Minister, Harold Wilson, was a communist - as some foolish spies assumed in the late 1960s and early 1970s - needs to be kept under intense scrutiny. Goodness knows what parts of MI6 would make of Jeremy Corbyn's internet details if some thought Wilson dangerously left wing. The police, too, are far from error-free and some will no doubt make mistakes or deliberately abuse access to records. But again no supporter of May's latest proposals, to be unveiled tomorrow, will disagree with the need for accountability. The thorny question becomes how agencies, more often than not used to functioning in the dark, can be held to account.

The former adviser on security legislation, Lord Carlile, a Liberal Democrat, pointed out on the BBC that a Home Secretary will challenge the intelligence agencies at least as much as a judge in granting access in emergency situations. He added that the home secretaries he had worked with always had been robust in the past. This is hardly surprising. There will always be immense countervailing pressures on Home Secretaries to show that they are not "invading" people's privacy unnecessarily. An elected home secretary is more accountable than a judge, who does not have to answer in any arena as to why he or she has made a decision.

In response to such powerful arguments, the senior Conservative MP, David Davis, a smartly forensic critic of state surveillance, points out that Home Secretaries do not explain in public either, hiding behind the convenient shield that responding to questions might threaten national security. Davis argues there is no real accountability when a home secretary oversees sensitive security decisions. He is one of the few MPs who recognises the centrality of accountability as a way of keeping many different institutions and agencies on their toes.

But that is not necessarily a case for insisting on judicial oversight and ceding all political control. In both the case of the silent home secretary and the lack of public scrutiny in relation to intelligence agencies, there are ways to provide much higher levels of transparency. When a tiny amount of daylight is shone on the security services, such as the rare public hearing two years ago in which the Commons' intelligence committee questioned spy chiefs, there is no threat to national security. With greater access to internet and phone information must come more public explanation as to why and how the new powers are being used. "We cannot say anything in order to protect national security" must be protective words deployed rarely.

The feverish paranoia about "surveillance" reflects an unsurprising suspicion of the state in all its manifestations. In the UK of the 21st century the attitudes follow a familiar pattern: a home secretary cannot be trusted because he or she is a politician, a judge can be trusted because he or she is not an elected politician and the state is always an instrument of stifling oppression and never one that can act benevolently.

Most of the time ministers imply by their actions that the state in the UK can never be a force for good. The Chinese can finance the UK's nuclear power stations, but not the poor old UK state. The German and Dutch governments can own train companies, but the British Government cannot. Charities are hailed as innovative deliverers of services, until they go bust when the state agonises about why it regulated so complacently. When a Home Secretary proclaims the need for the state to have access to private information there is understandable anxiety, heightened by the proposition that an elected politician will be in ultimate control.

But the wariness is based partly on a disproportionate self-importance. I have met some of the most boring people in the Western world who assume they must be protected from the probing interests of the snoopers. They should be so lucky. The snoopers will be too busy following 10,000 other trails to bother with what any of us get up to.

As with the bankrupt charity Kids Company, the "free" school that underperforms and the hospital that fails its patients, questions of accountability are complex. But in each case a greater level of scrutiny would act as a deterrent against incompetence or abuse. In the case of national security, let the spies spy and be held to account more fully for what they do and how they do it. Elected politicians must have a role in the decision making and in challenging the decision makers.
What is the snooper’s charter?

The Investigatory Powers Bill, a revamp of the "snooper's charter" Data Communications Bill, is to be published on Wednesday

BYLINE: By Charlotte Krol and agency, video source ITN

SECTION: NEWS

LENGTH: 459 words

The new spying laws published tomorrow will be "one of the most important pieces of legislation" considered by MPs over the next five years, David Cameron has told ministers.

The Prime Minister said the package of measures "goes to the heart of the Government's duty to keep the British public safe".

His comments came as the Cabinet was briefed about the Investigatory Powers Bill covering the tools available to police and intelligence agencies to fight terrorism and serious crime in the digital age.

In a potential area of controversy, measures requiring internet firms to store internet connection records (ICR) to respond to the increasing use of apps and social media for communication are expected to be included in the draft Investigatory Powers Bill.

However, sources said access to ICRs will be controlled and they will not include a full browsing history or reveal every web page visited, with strict limits on accessing the records.

Security services will retain the capacity to intercept the content of communications after obtaining a warrant.

It is understood that ministers have ruled out any proposal to restrict encryption or ban it, despite fears in the intelligence community that advanced online security measures risk leaving them locked out of some areas of cyber space.

The Prime Minister's official spokeswoman said Home Secretary Theresa May talked colleagues through the powers contained in the legislation.

The independent reviewer of terrorism legislation, David Anderson QC, gave a comprehensive 370-page report in June that heavily influenced Government thinking and the Investigatory Powers Bill.
This week the Home Office will be launching the new Investigatory Powers Bill. It had previously sought to obtain these powers under the "Snoopers' Charter" proposals in the last parliament but it failed.

This time the government is sensibly not relying on the brute strength of parliamentary votes or the standard "FUD" tactic of promoting fear, uncertainty and doubt. Such methods of stealth and FUDery may not be sufficient, so something more is needed to get the Bill over the bumps of this first week or two. The Home Office wants your heads to nod along too.

Many people say that the problem with politics is that there is too much cynicism. The problem with UK politics, however, is not that people are too cynical but that they are too gullible. Our politics is beset and bedeviled by the phenomenon of mass nodding along. Just get the catchphrases correct, and you will get all the audience applause you need. The trick is saying the right things at the right time.

So the Home Office has launched a proactive PR campaign, the results of which you will see already in many news titles even before the Bill is published. Journalists have been invited in for high-level background briefing (some have refused). Helpful access is being provided, there is selective leaking and queries promptly answered. If the Home Office could physically hand out trumpets this week to journalists so that the Bill could have a fanfare it would do so.

We are not yet allowed to know what the Bill contains. Not even journalists have been able to see the draft yet. But we are to be reassured through the media that this Bill is a "climb down" (even though it seems that the government has merely chosen not to ask the impossible over encryption). We are to be relieved and reassured by what the media tell us: the Bill is not as extreme as it could be.
naturally tend to like a compromise, so that is what is being sold. Everyone is being encouraged to nod; soon we will not be able to help ourselves.

There are one or two critical voices being added to reports as "balance" somewhere down among the bottom paragraphs of pieces that few will ever read to the end. But these objections will get little traction. Some of the concerns will be repeated in committee or in the House of Lords; and no doubt the government has already anticipated which concessions it will make to get the Bill safely though both houses of the legislature. This whole legislative exercise will have been planned with care, from this week's preemptive media feeding to the Bill's enactment.

A similar -- but smaller -- political field manoeuvre was executed when the DRIP (Data Retention and Investigatory Powers ) Bill was forced through in days last year (on this, see my June 2014 post); for after having failed to get the "Snooper's Charter" through, those who want the measure are not going to make any mistakes this time. One would not be surprised if more planning by senior officials has gone into getting this Bill through than into any one anti-terrorism exercise in the last few months.

So we will nod until the Bill reaches the statute book. Some will carry on nodding, perhaps carried away with the momentum. The government will then have a solid legal basis for far more intrusion than it has now; it will be able to get what it wants when it wants about all your electronic communications, and so too will anyone else who get access to this data. All the data the government would ever want will be there for the taking.

And one day someone will notice and will begin to shake their head, but then it will be too late. For in a gullible political culture, power is always with those who can get other people nodding; and the odd person shaking their head has no political power at all.
Journalists' sources must be protected from the authorities, the Society of Editors has said, after Theresa May announced a host of proposals that would allow access to reporters' communications data without prior judicial approval.

While the provisions of the draft *investigatory powers bill* would normally require authorisation for such access to come from both the home secretary and a judicial commissioner, they would also give May the power to sign off urgent requests alone - only submitting the decision to review in retrospect.

The SoE, which has campaigned to protect the rights of journalists against creeping state control, believes sources need to be shielded from such powers.

Related: *Investigatory powers bill: the key points*

"The police need to understand that journalists are not criminals and that they need to think very carefully before they do anything to search their records," said Bob Satchwell, the executive director of SoE.

"Accessing journalists' call records should be a rare exception for police rather than the rule it seems to have become in recent years."

According to May, the draft bill is necessary to ensure there is "no area of cyberspace which is a haven for those who seek to harm us to plot, poison minds and peddle hatred under the radar".

If it eventually becomes law, the bill would define "sensitive professions" that handle important information, such as that carried out by doctors, lawyers, MPs and journalists. Many journalists rely on a confidentiality agreement when trying to convince vulnerable people to speak out in the public interest. The draft bill would create the legal framework by which the security services could violate that confidentiality.

May said a "double-lock" system, under which the secretary of state and a judicial commissioner - usually a former judge - would need to agree to issue a warrant, would provide protection. But she clarified that in urgent cases the system would change.

Related: The Guardian view on the draft *investigatory powers bill: snooper's charter 3.0* | Editorial

"There will be an urgent process, so it will be possible for a secretary of state to sign an urgent warrant for it to come immediately into effect, and then there will be a period of time within which the judge will have to review that and then make a decision as to whether it should continue or not," she said.

No warning would be given to a journalist, making it impossible to contest the decision. "There also needs to be a clear rule that media organisations get fair warning so that they can challenge any requests if required," Satchwell said in response.

He added that the new proposals did not represent an improvement on the interim measures put in place after it emerged the Metropolitan police had obtained the phone records of the Sun journalist Tom Newton Dunn while trying to identify a source in the Plebgate case. The provisions were criticised by the media industry.
Theresa May unveils UK surveillance measures in wake of Snowden claims;
Spy agencies free to track everyone's internet use without warrant
UK governments have signed secret orders on data collection for years Snowden says bill is most intrusive surveillance regime in the west

BYLINE: Alan Travis Patrick Wintour and Ewen MacAskill

SECTION: WORLD NEWS

LENGTH: 1409 words

New surveillance powers will be given to the police and security services, allowing them to access records tracking every UK citizen's use of the internet without any judicial check, under the provisions of the draft investigatory powers bill unveiled by Theresa May.

It includes new powers requiring internet and phone companies to keep "internet connection records" - tracking every website visited but not every page - for a maximum of 12 months but will not require a warrant for the police, security services or other bodies to access the data. Local authorities will be banned from accessing internet records.

The proposed legislation will also introduce a "double-lock" on the ministerial approval of interception warrants with a new panel of seven judicial commissioners - probably retired judges - given a veto before they can come into force.

But the details of the bill make clear that this new safeguard for the most intrusive powers to spy on the content of people's conversations and messages will not apply in "urgent cases" - defined as up to five days - where judicial approval is not possible.

The draft investigatory powers bill published on Wednesday by the home secretary aims to provide a "comprehensive and comprehensible" overhaul of Britain's fragmented surveillance laws. It comes two-and-a-half years after the disclosures by the whistleblower Edward Snowden of the scale of secret mass surveillance of the global traffic in confidential personal data carried out by Britain's GCHQ and the US's National Security Agency (NSA).

It will replace the current system of three separate commissioners with a single investigator powers commissioner.

May told MPs that the introduction of the most controversial power - the storage of everyone's internet connection records tracking the websites they have visited, which is banned as too intrusive in the US and every European country including Britain - was "simply the modern equivalent of an itemised phone bill".

Snowden, however, took a different view:

May's recommendations were broadly welcomed by the shadow home secretary, Andy Burnham, but received a more cautious welcome from the former Conservative shadow home secretary David Davis, the former shadow home secretary Yvette Cooper and Nick Clegg, the former deputy prime minister.

Some former ministers pressed May on the nature of the double-lock, whereby a warrant could be issued first by the home secretary and then endorsed by a specially appointed judge. They also asked whether some warrants could be issued by the home secretary outside this dual-lock process.

Burnham said it was important to stress the proposals were "neither a snooper's charter nor a plan for mass surveillance". The Labour frontbencher said the UK's laws were outdated given that changes in technology had made the jobs of the security services and police much harder.

Burnham said: "In a world where the threats we face internationally and domestically are growing, parliament cannot sit on its hands and leave blind spots where the authorities can't see."
He said strong powers must be balanced by strong protections for the public, adding: "What the home secretary has said today, it seems clear to me both she and the government have been listening carefully to the concerns that were expressed about the original legislation presented in the last parliament."

Burnham added: "I think it would help the future conduct of this important public debate if this House sent out a unified message today that this is neither a snooper's charter nor a plan for mass surveillance."

Parliament cannot sit on its hands and leave blind spots where the authorities can't see

Andy Burnham

Davis questioned whether the new warrant process would cover all the current mechanisms for the intercept and use of communications data. He also questioned the independence of the judiciary, asking if they would be appointed by the prime minister or by the Judicial Appointments Commission.

Clegg, who in government blocked previous attempts to give spies sweeping new powers, was cautious, saying the proposals were much improved compared with the snooper's charter. But he warned: "I have a feeling under the bonnet it still retains some of the flaws of its predecessor."

The Lib Dem MP suggested it might be simpler and faster to provide for direct judicial authorisation, rather than retaining a role for ministers. He also queried why it was necessary to hold so much internet browsing data.

The draft bill explicitly includes in statute for the first time powers for the bulk collection of large volumes of communications and other personal data by MI5, GCHQ, MI6 and for their use of "equipment interference powers" - the ability to hack computers and phones around the world - for purposes of national security, serious crime and economic wellbeing.

**UK has secretly collected data in bulk since 2001**

In her statement, May also revealed for the first time that successive governments since 2001 have issued secret directions to internet and phone companies to hand over the communications data of British citizens in bulk to the security services.

She said these secret "directions" had allowed the security services to thwart a number of attacks in Britain, including the plot to attack the London Stock Exchange in 2010.

May revealed that the use of these powers - which show that GCHQ was also engaged in mass surveillance programmes on British citizens using their communications data - under the 1984 Telecommunications Act will be put on a more explicit footing in the new legislation and be subject to the same safeguards as other bulk powers.

Related: Theresa May gives police powers to view UK citizens' web browser history - live

Home Office estimates put the extra costs of storing internet connection records and the new judicial oversight regime at £245m to £250m over 10 years after the legislation comes into force in December next year. This includes £175m for the cost of storing everyone's internet records and £60m for the extra judicial oversight.

Welcoming the bill as a decisive moment in updating Britain's surveillance laws, May said: "There should be no area of cyberspace which is a haven for those who seek to harm us to plot, poison minds and peddle hatred under the radar."

"But I am also clear that the exercise and scope of investigatory powers should be clearly set out and subject to stringent safeguards and robust oversight, including 'double-lock' authorisation for the most intrusive capabilities. This bill will establish world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world."

She said it could not be used to determine whether somebody had visited a mental health website or even a news website but only for the purpose of finding out whether they had visited a communications website, such as WhatsApp, an illegal website or to link their device to a specific website as part of a specific investigation.

Related: These internet surveillance powers risk undermining the judiciary | Joshua Rozenberg

But the detail of the bill makes clear that the authorisation arrangements for internet connection records will remain exactly the same as the current 517,000 requests for communications data made last year. These requests are made without any kind of warrant and signed off by either a police inspector or superintendent depending on the kind of data.
Jim Killock, the executive director of the privacy campaigning body Open Rights Group, sees the draft bill as an attempt to secure even more intrusive powers. "At first glance, it appears that this bill is an attempt to grab even more intrusive surveillance powers and does not do enough to restrain the bulk collection of our personal data by the secret services," he said.

"It proposes an increase in the blanket retention of our personal communications data, giving the police the power to access web logs. It also gives the state intrusive hacking powers that can carry risks for everyone's internet security."

A Microsoft spokesperson tentatively welcomed the bill while adding caveats about private data and protection for customers, saying: "We appreciate the government's willingness to engage in an open debate about these important issues, and as this process unfolds, we will work to ensure that legislation respects these principles and protects the privacy of our customers."

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Surveillance Q&A: what web data is affected - and how to foil the snooper's charter will give police and spies access to a year's worth of your web browsing history

BYLINE: Samuel Gibbs

SECTION: WORLD NEWS

LENGTH: 1076 words

Critics call it a revived snooper's charter, because the government wants police and spies to be given access to the web browsing history of everyone in Britain.

However, Theresa May says her measures would require internet companies to store data about customers that amount to "simply the modern equivalent of an itemised phone bill".

Who is right? And is there anything you can do to make your communications more secure?

What exactly is the government after?

Related: Theresa May unveils surveillance measures in wake of Snowden claims

The government is attempting to push into law the ability for law enforcement agencies to be able to look at 12 months of what they are calling "internet connection records", limited to the website domains that UK internet users visit.
This is the log of websites that you visit through your internet service provider (ISP), commonly called internet browsing history, and is different from the history stored by your internet browser, such as Microsoft's Edge, Apple's Safari or Google's Chrome.

It does not cover specific pages: so police and spies will not be able to access that level of detail. That means they would know that a person has spent time on the Guardian website, but not what article they read.

Clearing your browser history or using private or incognito browsing modes do nothing to affect your browsing history stored by the ISP.

What will they be able to learn about my internet activity?

Information about the sites you visit can be very revealing. The data would show if a person has regularly visited Ashley Madison - the website that helped facilitate extramarital affairs. A visit to an Alcoholics Anonymous website or an abortion advice service could reveal far more than you would like the government or law enforcement to know.

The logged internet activity is also likely to reveal who a person banks with, the social media they use, whether they have considered travelling (eg by visiting an airline homepage) and a range of information that could in turn link to other sources of personal information.

Who will store my web browsing data?

The onus is on ISPs - the companies that users pay to provide access to the internet - to store the browsing history of its customers for 12 months. That includes fixed line broadband providers, such as BT, TalkTalk, Sky and Virgin, but also mobile phone providers such as EE, O2, Three and Vodafone.

But after what happened with TalkTalk, can ISPs keep my data safe?

TalkTalk may have been hacked by a group of teenagers, going on recent arrests. The customer data targeted was not all encrypted, a practice for which TalkTalk was roundly criticised.

But the most worrying aspect of the TalkTalk hack is that the company's chief executive, Dido Harding, said the company's cybersecurity was "head and shoulders" above its competitors.

Consumers are likely to need reassurance from the companies and government that all ISPs can maintain the security of customer data.

Will that push up the prices of phone bills?

May announced that the government would cover the costs of storing internet connection records and establishing the new judicial oversight regime. She estimated it would cost between £245m and £250m over 10 years.

This includes £175m for the cost of storing everyone's internet records, which means ISPs should not have to put up prices to cover their costs.

Don't ISPs already store this data?

They already store a limited amount of data on customer communications for a minimum of one year and have done for some time, governed by the EU's data retention directive. That data can be accessed under the Regulation of Investigatory Powers Act 2000 (Ripa).

The new bill will enshrine the storage of browsing history and access to that data in law.

Can people hide their internet browsing history?

There are a few ways to prevent the collection of your browsing history data, but each way is a compromise.

The most obvious way is the use of virtual private networks (VPNs). They channel your data from your computer through your ISP to a third-party service before immersing on the internet. In doing so they can obfuscate your data from your ISP and therefore the government's collection of browsing history.

Companies routinely use VPNs to secure connections to services when off-site such as home workers. Various companies such as HotspotShield offer both free or paid-for VPN services to users.
Using the Tor browser, freely available from the Tor project, is another way to hide what you're doing from your ISP and takes things a stage further. It allows users to connect directly to a network of computers that route your traffic by bouncing it around other computers connected to Tor before emerging on the open internet.

Your ISP will see that you are connected to Tor, but not what you are doing with it. But not everybody has the technical skills to be comfortable using Tor.

**Is there any downside to using a VPN?**

In using a VPN you are placing all your trust in the company that operates the VPN to both secure your data and repel third parties from intercepting your connection. A VPN based in the UK may also be required to keep a log of your browsing history in the same way an ISP would.

The speed of your internet connection is also limited by the VPN. Most free services are slow, some paid-for services are faster.

Tor also risks users having their data intercepted, either at the point of exit from the Tor network to the open internet or along the path. This is technically tricky, however. Because your internet traffic is bounced between computers before reaching you, Tor can be particularly slow.

**Can I protest-browse to show I'm unhappy with the new law?**

One way to prevent an accurate profile of your browsing history from being built could be to visit random sites. Visiting nine random domains for every website you actually want to visit would increase the amount of data that your ISP has to store tenfold. But not everybody has the patience for that.

At some point it will be very difficult to store that much data, should everyone begin doing so.

**What about smartphones?**

Hiding your browsing history while using a smartphone or tablet is harder. Most devices, including Apple’s iPhone and Google’s Android devices can use both VPN services and Tor, but the service is at risk of slowing down and not protecting every connection made by every app.

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc.
All Rights Reserved

Return to List

29 of 104 DOCUMENTS

The Guardian

November 4, 2015 Wednesday 2:01 PM GMT

Theresa May secures backing of Labour and Lib Dems for surveillance plans - live;
Home secretary publishes draft investigatory powers billLabour says legislation is not a 'snoopers' charter"Key points of May’s
David Anderson, the independent reviewer of terror legislation, says on Twitter that he will be responding to the draft bill on the PM programme after 5pm.

But, judging by what he has been tweeting, he seems quite pleased with it. Here are some of those tweets.

enltrHome Sec has just said "We have taken virtually everything David Anderson asked for on board".
- David Anderson (@terrorwatchdog) November 4, 2015

enltrHSec's words on MI5's use of s94 Telecoms Act 1984 to collect domestic comms data in bulk were a significant and necessary avowal. 1/2
- David Anderson (@terrorwatchdog) November 4, 2015

enltrIf powers such as these are required, it is right that Parliament should have the chance to debate them. 2/2
- David Anderson (@terrorwatchdog) November 4, 2015

And Anderson retweeted this.

enltrBulk domestic data mining of phone records avowed. pic.twitter.com/84BMceA8sQ
- Eric King (@e3i5) November 4, 2015

(What this means, I think, it that GCHQ has been hoovering up bulk data for years, but that at least this bill is explicit about this, and that that is a good thing.)

enltrDon't forget the new transparency report: goes well beyond investigatory powers. A new development. https://t.co/Z8UaCeZ4Jo
- David Anderson (@terrorwatchdog) November 4, 2015

enltrI said an operational case was the minimum starting point for internet connection records. Here it is, for scrutiny: https://t.co/ZQCdSPP2FT
- David Anderson (@terrorwatchdog) November 4, 2015

enltrA huge quantity of "overarching documents" have been published with the #IPBill : impact assessments, factsheets etc. https://t.co/qn2OMxkGuF
- David Anderson (@terrorwatchdog) November 4, 2015

Steve McCabe, a Labour MP, asks why internet companies are being asked to retain web browsing information for 12 months. May says 12 months that current obligations on data retention apply for. It was felt 24 months would be too long, she says.

Theresa May's statement about the draft investigatory powers bill - Summary

Here are the main points from Theresa May’s statement.

May insisted that today's draft bill was quite different from the 2012 draft communications data bill that was branded the snoopers' charter.
Let me be clear, the draft Bill we are publishing today is not a return to the draft Communications Data Bill of 2012.

It will not include powers to force UK companies to capture and retain third party internet traffic from companies based overseas. It will not compel overseas communications service providers to meet our domestic retention obligations for communications data. And it will not ban encryption or do anything to undermine the security of people's data. And the substance of all of the recommendations by the Joint Scrutiny Committee which examined that draft Bill have been accepted.

So today's Bill represents a significant departure from the proposals of the past.

She said the government was not proposing to give the police access to people's full web browsing history.

Mr Speaker, some have characterised this power as law enforcement having access to people's full web browsing histories. Let me be clear - this is simply wrong. An Internet Connection Record is a record of the communications service that a person has used, not a record of every web page they have accessed.

So, if someone has visited a social media website, an Internet Connection Record will only show that they accessed that site, not the particular pages they looked at, who they communicated with, or what they said. It is simply the modern equivalent of an itemised phone bill.

She said "strict limits" would apply to when the police could access this information.

Law enforcement agencies would not be able to make a request for the purpose of determining - for example - whether someone had visited a mental health website, a medical website or even a news website.

They would only be able to make a request for the purpose of determining whether someone had accessed a communications website, an illegal website or to resolve an IP address where it is necessary and proportionate to do so in the course of a specific investigation.

She confirmed that a new "double lock" would apply to the issuing of warrants allowing the interception of communications.

While there was a good deal of agreement in the three independent reviews I have referenced, all three reached different conclusions on the question of who should authorise interception warrants.

The Intelligence and Security Committee supported authorisation by a Secretary of State. David Anderson said judges should carry out the authorisation. And RUSI said the authorisation of warrants should have a judicial element, but also recognised the important role of the Secretary of State.

I have considered the very good arguments put forward by the three reviews. My response is one that I hope the House agrees will provide the reassurance of both democratic accountability and judicial accountability.

So, as now, the Secretary of State will need to be satisfied that an activity is necessary and proportionate before a warrant can be issued. But in future, the warrant will not come into force until it has been formally approved by a judge.

This will place a "double lock" on the authorisation of our most intrusive investigatory powers. Democratic accountability, through the Secretary of State, to ensure our intelligence agencies operate in the interests of the citizens of this country, and the public reassurance of independent, judicial authorisation.

This will be one of the strongest authorisation regimes anywhere in the world.

She said the prime minister would have to approve any warrant to intercept the communications of an MP.

For Parliamentarians we will go even further. This Bill will for the first time put into law the Prime Minister’s commitment that in any case where it is proposed to intercept the communications of a Parliamentarian - including members of this House, members of the House of Lords, UK MEPs and the members of the devolved legislatures - the Prime Minister would also be consulted.

She claimed the new oversight arrangements - involving a new investigatory powers commissioner - would be "world-leading".
I am clear we need a significantly strengthened regime to govern how these powers are authorised and overseen. So we will replace the existing oversight with a powerful and independent Investigatory Powers Commissioner. This will be a senior judge, supported by a team of expert inspectors with the authority and resources to effectively, and visibly, hold the intelligence agencies and law enforcement to account. These will be world-leading oversight arrangements.

She claimed the draft bill contained some of the "strongest protections and safeguards" in the world.

Today, we are setting out a modern legal framework which brings together current powers in a clear and comprehensible way. A new Bill that provides some of the strongest protections and safeguards anywhere in the democratic world. And an approach that sets new standards for openness, transparency and oversight.

She said the draft bill would be scrutinised by a joint committee of MPs and peers and that a revised bill would then come to parliament in the spring, with a view to it becoming law before the end of 2016.

Andrew Mitchell, the former international development secretary, says he used to sign warrants when he was in government on behalf of May and others. He says he backs the "dual key" approach proposed by May. But he wants an assurance that the judges authorising warrants are seen as independent, and that they are not judges seen as too close to the police.

May agrees with this point.

David Winnick, the Labour MP, says he is concerned about the "excessive powers" being given to the security services. If this were to be passed without amendment, it would be a "bitter blow to civil liberties".

May says Winnick claimed there were substantial new powers in the bill. He is wrong, she says. Most of the powers in the bill exist in current legislation, she says.

But she admits that the powers relating to the retention of internet browsing history are new.

May says most of the powers given to the police and intelligence services in the draft bill are not new.

Here's a clip from May's statement.

Keith Vaz, the Labour chair of the home affairs committee, asks who will train the judges to do this work.

May says this is not the first time judges have been asked to take on new national security responsibilities. Judges are used to taking difficult decisions, she says. She says she has more faith in the judiciary than perhaps Vaz does.

Owen Paterson, the Conservative former Northern Ireland secretary, says he is worried that the "double-lock" process for warrants will slow things down. He suggests it would be better to carry on with the existing system.

May says the question about timeliness is a good one. There will be guidelines saying how quickly judges need to respond to requests for a warrant.

But there will be a provision allowing a secretary of state to approve a warrant in an emergency. When this happens, a judge will have to confirm it within five days.
In response to a question from the SNP’s Joanna Cherry, May says there is a "question mark" over whether a legislative consent motion is required for this bill (ie, whether the Scottish parliament has to approve it because it covers devolved matters).

The home secretary revealed for the first time in her statement that successive governments since 1994 have issued secret directions to internet and phone companies to hand over the communications data of British citizens in bulk to the security services.

She said these secret "directions" had allowed the security services to thwart a number of attacks in Britain, including the plot to attack the London Stock Exchange in 2010.

May said the use of these powers - which show that GCHQ was also engaged in mass surveillance programmes on British citizens using their communications data - under the 1984 Telecommunications Act will be put on a more explicit footing in the new legislation and be subject to the same safeguards as other bulk powers.

And here is the full text of Theresa May's statement on the draft bill.

Here is the 299-page draft investigatory powers bill (pdf).

And here is the page on the Home Office website with links to more than 20 documents being published alongside the bill.

Nick Clegg, the former Lib Dem leader, says this bill is a "much improved model" compared to the 2012 draft bill, although he says he thinks there may be flaws "under the bonnet".

He says the double-lock compromise on judicial authorisation is a compromise. But it may be cumbersome. Why did May rule out simple judicial authorisation.

He says the provisions on internet browsing data are a big improvement on the 2012 bill.

May says not all the reports about the draft bill that appeared before today were the result of briefing.

Some of the most contentious plans from the 2012 model, such as the retention of third party data, have been dropped.

She says, if a child is abducted, the police can see from their phone records who they were in contact with. But currently the police cannot see who they contacted via the internet.

May welcomes the tone of Burnham's response. But she says that she does not accept what Burnham said about David Cameron.

She says she has discussed this with David Anderson. It is not for her to say what he thinks, but she has taken on board most of his recommendations.

She says the content-interception plans will only cover serious crimes, as now.

On encryption, she says the government is not banning encryption. But it is asking providers to take reasonable steps to be able to read communications.

She says there will be something in the bill saying that judicial authorisation is needed for the police to access a journalist's source.

On the double-lock, she says both the judge and the secretary of state will have to approve a warrant. But there will be a process where a warrant applies after a secretary of state has approved it, provided that a judge subsequently confirms it.

Burnham says May has 'broadly' got the balance right
Andy Burnham, the shadow home secretary, says May has been listening to the concerns expressed in the last parliament. She has brought forward stronger safeguards, he says.

He says it would help if MPs sent out a unified message that this is neither a snoopers’ charter nor a plan for mass surveillance.

Has David Anderson expressed a view on the draft bill?

Can May assure MPs that the powers for content-interception will only be used for the most serious crimes?

What information will be stored by internet firms? Does May understand the concern the TalkTalk hack has generated?

If this bill does not apply to firms overseas, doesn’t that create a large hole? Will there be voluntary arrangements covering them?

Will there be protection for journalists too?

Burnham says he is pleased to see that May has shifted on authorisation. But having a two-stage process could bring in time delays? So how will it work? And what happens if the secretary of state and the judge come to different conclusions? Who will have the final say?

He says there are fears in the Muslim community that these powers will be used against them. It does not help when the prime minister implies Muslims condone extremism. And there fears about these powers being used against trade unionists. So will the government drop some of its more divisive measures, including those in the trade union bill.

Burnham says the plans in this bill go beyond party politics.

He says May has "responded to legitimate concerns and broadly got that balance right".

Burnham says May has "broadly" got the balance right.

He says the draft bill does not amount to a snoopers’ charter or mass surveillance.

Andy Burnham Photograph: BBC Parliament

May says there will be a "double-lock" process applying before the most intrusive warrants are approved.

They will have to be approved by a secretary of state, but then confirmed by a judge too.

This will be one of the strongest authorisation arrangements in the world, she says.

And there will be extra protection for MPs and members of the devolved legislatures. The prime minister would have to approve a warrant approving them, he says.

May says any interception warrant covering an MP would have be be approved by prime minister.

May says there will be new oversight arrangements - a new commissioner, she says.

These will be "world-leading" oversight arrangements, she says.

May says the bill will make explicit provision for the intelligence agencies to acquire information in bulk. This is not a new power. It will replace a power under the Telecommunications Act 1984.

Bulk communications data has played a huge role in investigating terror attacks, she says.

These powers do not cover content, she says.
May says a transparency report is being published with the bill today.

Back in the Commons May says the provisions about accessing internet browsing history are just the modern equivalent of allowing the authorities to see an itemised phone bill.

Here is the first take of my colleague Alan Travis’s story about the draft bill.

New surveillance powers will be given to the police and security services, allowing them to access records tracking every UK citizen’s use of the internet without any need for any judicial check, under the provisions of the draft investigatory powers bill unveiled on Wednesday lunchtime.

It includes new powers requiring internet and phone companies to keep "internet connection records" - tracking every website visited but not every page - for a maximum of 12 months but will not require a warrant for the police, security services or other bodies to access the data. Local authorities will be banned from accessing internet records.

The proposed legislation will also introduce a "double lock" on the ministerial approval of interception warrants with a new panel of seven judicial commissioners - probably retired judges - given a veto before they can come into force.

But the details of the bill make clear that this new safeguard for the most intrusive powers to spy on the content of people’s conversations and messages will not apply in "urgent cases" - defined as up to five days - where judicial approval is not possible.

May says today's bill is not a return to the 2012 'snoopers’ charter’

May says the bill published today is not a return to the draft communications data bill of 2012 she says.

It does not require the retention of third-party data.

It does not oblige overseas firms to comply with domestic retention obligations.

And it does not ban encryption, she says.

She says it also accepts all the recommendations of the joint committee that looked at the 2012 bill.

A joint committee will look at this draft bill.

And a proper bill will be published in the spring, she says.
In the last 12 months alone six significant threats have been detected in the UK.
More companies are under cyber-attack. And it is estimated that there are 50,000 people downloading images of children.

PMQs is over. Theresa May's statement is about to start. On the microphones Cameron can be heard saying PMQs is taking longer and longer.

Nigel Dodds, the DUP, asks about the loss of jobs from a closure of a factory in Northern Ireland, partly due to high energy costs. And will the prime minister reverse the thrust of the policy on tax credits?
Cameron says firms deemed part of energy intensive industries do qualify for help.
He says Northern Ireland has powers to set its own rate of corporation tax. He wants a stronger private sector there.
On tax credits, he says the answer he gave to Corbyn applies; the plans will be announced three weeks today.

Andrew Mitchell, a Conservative, says the mental health campaign is an all-party one.
Cameron says more is being invested in mental health than ever before. Mental health should no longer be treated as a Cinderella service, he says.

Norman Lamb, a Lib Dem, thanks Cameron for backing the campaign that he, Andrew Mitchell and Alastair Campbell are leading asking for equality for mental health. Will Cameron ensure the spending review delivers the extra funding necessary?
Cameron praises Lamb for his work on this. There are now twice as many talking therapies as five years ago. But there is more to do, he says.

Steve Double, a Conservative, asks about Newquay airport.
Cameron says he is a huge fan of the airport, and a frequent user.

Labour's Paul Flynn asks about the British servicemen and women who died in Iraq and Afghanistan. Will Cameron rethink his plans to join a four-sided civil war in Syria?

On Armistice Day we should put aside political debates like this, says Cameron.

Cameron confirms that government considering plans to part-privatise Channel 4
John Nicolson, the SNP MP, asks Cameron to confirm he has no plans to sell Channel 4.
Cameron says he is a huge fan of Channel 4. It was a great Conservative innovation. He wants to make sure it has a strong and secure future. He wants to look at all the options, including options for getting private investment into it. It would be wrong to "close our minds", he says. He wants it to have a great future.

Cameron confirms that government considering plans to part-privatise Channel 4.

Kevin Hollinrake, a Conservative, asks Cameron to confirm that he is committed to the north.
Cameron says the north needs a better deal on roads and rail. Some £13bn is now being spent, he says.

Cameron confirms that government considering plans to part-privatise Channel 4.
Labour's Diana Johnson asks about a case involving parents in her constituency whose child died and who were then not able to find out what happened to the ashes.

Cameron says he will look into this.

block-time published-time 12.28pm GMT

Anne-Marie Trevelyan, a Conservative, says there are 150 patients in Bucharest needing expert burns treatment following the nightclub fire. But they do not have enough beds there. Can the UK help?

Cameron says this is a good suggestion. He will look into it.

block-time published-time 12.27pm GMT

Labour's Gordon Marsden asks about the cuts to police funding. Cameron quotes a report saying Lancashire Police is exceptionally well placed to meet its police obligations.

block-time published-time 12.26pm GMT

Stephen Metcalfe, a Conservative, asks about apprenticeships and the skills gap. Will Cameron redouble his efforts to hit the 3m new apprenticeships target.

Cameron says he will. Many firms find that many people apply for apprenticeships, but that too many of them do not have the right qualifications. He says Nadhim Zahawi will be his new adviser on apprenticeships.

block-time published-time 12.22pm GMT

Snap PMQs verdict

Snap PMQs verdict: A scrappy, inconclusive PMQs. Cameron mocked Corbyn for returning to the tax credit question that worked so well for him last week, but there can be merit in persistence and, although Cameron had better answers than he did last week, Corbyn made his point effectively. Corbyn was probably less successful with his final three questions on the NHS, but Cameron's attempts to shift the subject were not edifying either, and neither side can claim a win. But the high-minded, policy-focused tone seems to be slipping. This sounded very like an old-fashioned, Cameron/Miliband PMQs, and Cameron can no longer hide the scorn he clearly feels for Corbyn. But letting it show is not necessarily a good idea.

block-time published-time 12.17pm GMT

Corbyn says the prime minister did not reply to his point about the winter crisis.

John Bercow intervenes to stop the shouting, which seems particularly loud.

Corbyn says, if Cameron won't answer his question, then perhaps he will address a point from the Kings Fund. It said the NHS was facing an inevitable decline in patient care unless something was done. Which is rising faster? NHS waiting lists or NHS deficits?

Cameron says Simon Stevens, the NHS England chief executive, asked for £8bn extra in funding. The government has offered £10bn. The number of treatments are going up. If you want to know what is in crisis, it is Labour. Corbyn's media adviser is a Stalinist, and his policy adviser is a Communist, he says.

Corbyn says if Cameron's party cannot match its actions with its words, it should get rid of him. The NHS is in crisis. Will Cameron ensure everyone can rely on it. It is the jewel in everyone's crown.

Cameron says, since he became prime minister, the number of doctors has gone up by more than 10,000, and the number of nurses up by more than 5,000. The UK is able to fund the NHS. But the countries Corbyn admires, with crazy socialist plans, have to cut their health service, he says.

block-time published-time 12.12pm GMT

Corbyn says the prime minister makes choices. A private in the army would lose over £2,000 next April. Surely the whole point of parliament is to put questions to those in authority. He asks a question from Kieron, a veteran of the first Gulf War. Is this how the government treats veterans?

Cameron says many soldiers will benefit from the £11,000 personal allowance coming in next year. Soldiers with children will benefit from the free childcare announcements. And he will see the full plans in three weeks time. That serving soldier is now dealing with an opposition leader who said he could see no point in the armed forces.
Corbyn turns to junior doctors' pay. He quotes a doctor saying this winter will be worse than last winter. Can Cameron guarantee there will be no winter crisis this year.

Cameron says the Royal College of Emergency Medicine supports what the government is doing. He urges doctors to go on the NHS website and see what their pay will be. No one will lose out. The NHS has the resources that it needs. It is a much stronger NHS, because we have a strong economy.

Jeremy Corbyn says he concurs with the prime minister's remarks about Remembrance Sunday. We should all try to build a peaceful world.

Last week he asked the same question six times. Cameron has now had a week to think about it, so he will ask again. Can he guarantee no one will be worse off from the tax credit changes.

Cameron says he can guarantee that there will be a tax allowance that saves people money, and that there will be a national living wage of £7.20. As for the tax credit changes, he will answer details about them when they are announced. If Corbyn wants to ask the same question, that will be very entertaining.

Corbyn says this is not about entertainment. It is not funny for those affected. What about this question from a Tory MP who said any mitigation should be full mitigation. What is his answer to that?

Very much the same answer, says Cameron. The government will announce its plans to move to a low tax, high pay economy then. But, if we don't reform welfare, how will we fund the police service, or the health service, or defence? If we listened to Corbyn, we would still have families in London getting £100,000 in housing benefit.

Craig Tracey, a Conservative, says he is looking forward to his Armistice Day parade. Does Cameron agree it is important to maintain the 2% of GDP defence spending commitment.

Cameron does agree. The defence spending commitment, and the 0.7% aid one, and Trident are all important, he says.

David Cameron says this is the last PMQs before Armistice Day. He wants to pay tribute to those who gave their lives for their country.

Labour has just put out a statement from Jeremy Corbyn criticising the government's decision to invite the Egyptian president, Abdel Fatah al-Sisi, to London. Corbyn said:

David Cameron's invitation to Britain today of the Egyptian president and coup leader Abdel Fatah al-Sisi shows contempt for human and democratic rights and threatens, rather than protects, Britain's national security.
Support for dialogue and negotiated conflict resolution in the Middle East is vital to us all. But to welcome and bolster with military support the coup leader who overthrew a democratically elected president in 2013 and has presided over the killing and jailing of many thousands since makes a mockery of government claims to be promoting peace and justice in the region.

Support for dictatorial regimes in the Middle East has been a key factor fuelling the spread of terrorism. Rather than rolling out the red carpet to President Sisi, the prime minister should suspend arms exports to Egypt until democratic and civil rights are restored.

Have some thought for the journalists who will have to make sense of the draft investigatory powers bill quickly. This is from the BBC’s Gordon Corera.

enlr Fun day ahead involving reading a 200 clause bill on technical surveillance powers and then condensing it into an easy to understand 2 mins

- Gordon Corera (@gordoncorera) November 4, 2015

Julian Huppert, the former Lib Dem MP, agrees with Henry Porter (see 11.12am) that who sits on the committee scrutinising the bill will be crucial.

enlr One key thing is who will sit on the Joint Committee to study the draft #ipbill. Last time we absolutely slated the previous version! #fb

- Julian Huppert (@julianhuppert) November 4, 2015

enlr Will the draft #ipbill committee have more securocrats on it? Any people knowledgeable about and interested in tech or privacy? #fb

- Julian Huppert (@julianhuppert) November 4, 2015

Henry Porter, the journalist and privacy campaigner, says there are rumours that Paul Murphy, the former Northern Ireland secretary, may chair a joint committee being set up to scrutinise the draft investigatory powers bill.

Murphy is a former chair of the intelligence and security committee, and would be seen as sympathetic to the concerns of the security services.

enlr @AndrewSparrow Who will chair joint committee to examine May bill? Rumours are it is ISC trusty Paul Murphy - not good news for scrutiny.

- henry porter (@HenryCPorter) November 4, 2015

Draft investigatory powers bill - A background reading list

For more background, here’s a internet surveillance reading list.

The Guardian story about the draft communications data bill in 2012. And here is the bill itself (pdf).

The report from a joint committee of MPs and peers set up to consider the draft communications data bill (pdf). The report, which was published in December 2012, was very critical, saying the draft bill went too far. Here’s an excerpt.

We accept that there is a case for legislation which will provide the law enforcement agencies with some further access to communications data, but we believe that the draft bill pays insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data. Clause 1 would give the secretary of state sweeping powers to issue secret notices to communications service providers (CSPs) requiring them to retain and disclose potentially limitless categories of data. We have been told that she has no intention of using the powers in this way. Our main recommendation is therefore that her powers should be limited to those categories of data for which a case can now be made. If in future a case can be made for the power to be increased, this should not be done without effective parliamentary scrutiny. We recommend the procedure for this.
A report from the intelligence and security committee in March this year calling for an overhaul of surveillance laws. Here is the report (pdf) and here is the news release (pdf).

The report from David Anderson, the government's independent reviewer of terrorism legislation, in June this year called A Question of Trust. This 373-page report set out detailed proposals for a new bill. Here is the press release about it (pdf), here is the report (pdf), and here is the Guardian story about its publication. And here is a Martin Kettle column praising it. This is how it starts:

Occasionally in the long history of British policymaking someone manages to break through the confusion and reset the terms of an apparently unresolvable public argument. Edwin Chadwick on the poor law and public health, William Beveridge on the welfare system and Leslie Scarman on the police all changed things for generations - and for the public good - in their respective fields. The question today is whether the name of David Anderson - Britain's watchdog on terrorism laws - should be added to the list of these national reformer-reconcilers.

With a fair wind behind it, his report on the future of surveillance laws, published yesterday, may eventually prove to have poured calming oils on a stormy argument that British governments have often seemed incapable of resolving. If Anderson's plea is taken seriously, and we wipe the slate clean and start again on Britain's efforts to balance security and privacy in the pursuit of crime in the borderless online world, his report really could be the turning point that policymakers have looked for and missed ever since 9/11.

A 28-page briefing paper from the House of Commons library about the background to the publication of the draft investigatory powers bill (pdf).

On the Today programme morning Sara Thornton, chair of the National Police Chiefs' Council, used an interview to explain why the police wanted internet surveillance laws to be updated.

Law enforcement needs access to communications data to protect the public and to investigate crime. We use communications data in day to day investigations. This is about what ordinary detectives do; they make the vast majority of applications for communications data.

The bottom line is we are just not keeping up with technology. Five or six years ago it used to be about phone records; just about who's calling who and where, not about the content at all. Of course, more and more of us are using the internet for those communications now. And therefore we need to have those internet communications records to find out what communication platforms people are using.

She also insisted that the police were not interested in looking about people's website browsing histories.

Can I just say, it is categorically not the case that we want to see people's internet browsing histories. It is not about that. It is about what communications platforms people are using, such as Facebook or WhatsApp.

I'll give you a good example. You might remember Operation [Voicer?], a case of a paedophile ring who were jailed earlier this year. They had been filming the abuse of babies and toddlers and they had been streaming it on the internet. The gang are all in prison. But we know that over 260 people viewed that abuse online. We've identified quite a lot of them. But 38 we are still unable to identify. Now, if we had access to internet connection records, we would be able to find their IP addresses, their internet protocol addresses, and find them. We are not able to do that at the moment.

Sara Thornton Photograph: Steve Parsons/PA Wire/Press Association Images

Several of the papers have stories previewing today's draft investigatory powers bill, but only two of them have splashed on it.

In the Times (paywall) Sean O'Neill says Theresa May will give judges the power to veto ministers' decisions about interception warrants.

A handful of judges will get the power to veto ministers' decisions on all top-level antiterrorism spying operations under proposals being put forward by the home secretary today.
The panel of specially trained judges - expected to number at least ten - should review thousands of national security warrants each year and hold the intelligence agencies to account, according to draft surveillance laws to be presented to parliament.

The move represents a significant concession by ministers to the privacy lobby's demand for greater scrutiny of spy agencies after the Edward Snowden leaks scandal. It is contained in the draft Investigatory Powers Bill, which aims to set out in more detail than ever before the state's powers to spy on citizens, alongside a new range of safeguards for individuals.

enlrWednesday's Times front page: Judges get right to veto anti-terror operations #tomorrowspaperstoday#bbcpaperspic.twitter.com/E15LenmORZ

- Nick Sutton (@suttonnick) November 3, 2015

And in the Daily Telegraph Tom Whitehead says the draft bill will allow council officials to be jailed if they misuse snooping powers. (The Daily Mail focuses on the same line in its preview story.) The Telegraph reports:

Town hall officials will face up to two years in prison if they abuse snooping powers under a crackdown on council surveillance to be unveiled on Wednesday.

A new offence is to be created to target public authorities who inappropriately access phone and email records.

Local authorities will also be banned from accessing the web histories of members of the public when ministers publish the biggest overhaul of spying laws for 15 years.

The measures will be included in the Investigatory Powers Bill which includes a raft of proposals to expand the ability of the police and spy agencies to monitor suspects.

enlrWednesday's Telegraph front page: Prison for officials who abuse snooping powers #tomorrowspaperstoday#bbcpaperspic.twitter.com/HvJsBln9DK

- Nick Sutton (@suttonnick) November 3, 2015

There is a lot of jargon in internet surveillance legislation that is hard to follow. The BBC has a handy guide translating some of the more difficult terms at the end of this Q&A.

There are few issues more fundamental in a liberal democracy than privacy and surveillance, and what powers we decide to give the state to allow it to monitor our communications. But none of this is easy or straightforward. A report earlier this year described one of the key Act's governing this area as "obscure since its inception" and "incomprehensible to all but a tiny band of initiates".

Today Theresa May, the home secretary, is announcing plans for a major overhaul of the legislation governing internet surveillance. We'll be trying to ensure that what she proposes is fully comprehensible, and not just to "initiates".

May's announcement is the culmination of a process lasting more than three years. I will post more on the background later, but here are the key milestones.

In June 2012 the coalition government published a draft communications data bill. This was published because the Home Office believed that changing technology meant it needed to update surveillance laws, but it included plans to monitor internet use, critics dubbed it the "snoopers' charter", the Lib Dems said they would never approve it and it was shelved. The legislation never came to parliament.

In June 2013 the Guardian started publishing stories based on leaked information from Edward Snowden revealing the full extent of internet surveillance carried out by the National Security Agency in America and GCHQ in the UK. The revelations triggered a worldwide debate about privacy and security (although the debate was much more muted in the UK than it was in America and continental Europe, where lawmakers seemed to take privacy concerns more seriously.)

This year, following the election of a majority Conservative government, David Cameron and May promised to bring the communications data bill back in a revised form. The result is the investigatory powers bill being published this afternoon.
My colleague Alan Travis has written a preview of what we will get. Here is his story, and here is how it starts.

Theresa May is to propose a major extension of the surveillance state when she publishes legislation requiring internet companies to store details of every website visited by customers over the previous year.

The home secretary will try to sweeten the pill of her revived snooper's charter on Wednesday by announcing that the police will need to get judicial authorisation before they can access the internet connection records of an individual - something that is currently banned in the US and every European country, including Britain.

She will also try to strengthen the oversight of Britain's surveillance by replacing the current fragmented system of three separate commissioners with an investigatory powers commissioner who will be a senior judge appointed by the prime minister on the recommendation of the lord chief justice.

I will mostly be focusing on the investigatory powers bill today, although I will also be covering PMQs. Here are the timings.

12pm: David Cameron faces Jeremy Corbyn at PMQs.
12.30pm: Theresa May makes a statement to MPs about the investigatory powers bill. The full bill is published simultaneously by the Home Office.

If you want to follow me on Twitter, I'm on @AndrewSparrow.

block-time updated-timeUpdated at 9.10am GMT

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc.
All Rights Reserved

Return to List

30 of 104 DOCUMENTS

The Guardian

November 4, 2015 Wednesday 1:22 PM GMT

Theresa May unveils surveillance measures in wake of Snowden claims;
Home secretary announces new powers for police and security services tracking UK citizens' internet use without need for judicial check

BYLINE: Alan Travis Home affairs editor

SECTION: WORLD NEWS

LENGTH: 998 words
New surveillance powers will be given to the police and security services, allowing them to access records tracking every UK citizen's use of the internet without any need for any judicial check, under the provisions of the draft investigatory powers bill unveiled by Theresa May.

It includes new powers requiring internet and phone companies to keep "internet connection records" - tracking every website visited but not every page - for a maximum of 12 months but will not require a warrant for the police, security services or other bodies to access the data. Local authorities will be banned from accessing internet records.

Related: Theresa May gives police powers to view UK citizens' web browser history - live

The proposed legislation will also introduce a "double-lock" on the ministerial approval of interception warrants with a new panel of seven judicial commissioners - probably retired judges - given a veto before they can come into force.

But the details of the bill make clear that this new safeguard for the most intrusive powers to spy on the content of people's conversations and messages will not apply in "urgent cases" - defined as up to five days - where judicial approval is not possible.

The draft investigatory powers bill published on Wednesday by the home secretary aims to provide a "comprehensive and comprehensible" overhaul of Britain's fragmented surveillance laws. It comes two-and-a-half years after the disclosures by the whistleblower Edward Snowden of the scale of secret mass surveillance of the global traffic in confidential personal data carried out by Britain's GCHQ and the US's National Security Agency (NSA).

It will replace the current system of three separate commissioners with a senior judge as a single investigatory powers commissioner.

Related: Investigatory powers bill: the key points

The draft bill explicitly includes in statute for the first time powers for the bulk collection of large volumes of communications and other personal data by MI5, GCHQ, MI6 and for their use of "equipment interference powers" - the ability to hack computers and phones around the world - for purposes of national security, serious crime and economic wellbeing.

In her statement, May also revealed for the first time that successive governments since 1994 have issued secret directions to internet and phone companies to hand over the communications data of British citizens in bulk to the security services.

She said these secret "directions" had allowed the security services to thwart a number of attacks in Britain, including the plot to attack the London Stock Exchange in 2010.

May revealed that the use of these powers - which show that GCHQ was also engaged in mass surveillance programmes on British citizens using their communications data - under the 1984 Telecommunications Act will be put on a more explicit footing in the new legislation and be subject to the same safeguards as other bulk powers.

Home Office estimates put the extra costs of storing internet connection records and the new judicial oversight regime at £245m to £250m over 10 years after the legislation comes into force in December next year. This includes £175m for the cost of storing everyone's internet records and £60m for the extra judicial oversight.

Welcoming the bill as a decisive moment in updating Britain's surveillance laws, May said: "There should be no area of cyberspace which is a haven for those who seek to harm us to plot, poison minds and peddle hatred under the radar."

"But I am also clear that the exercise and scope of investigatory powers should be clearly set out and subject to stringent safeguards and robust oversight, including 'double-lock' authorisation for the most intrusive capabilities. This bill will establish world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world."

May told MPs that the introduction of the most controversial power - the storage of everyone's internet connection records tracking the websites they have visited, which is banned as too intrusive in the US and every European country including Britain - was "simply the modern equivalent of an itemised phone bill".

She said it could not be used to determine whether somebody had visited a mental health website or even a news website but only for the purpose of finding out whether they had visited a communications website, such as WhatsApp, an illegal website or to link their device to a specific website as part of a specific investigation.
But the detail of the bill makes clear that the authorisation arrangements for internet connection records will remain exactly the same as the current 517,000 requests for communications data made last year. These requests are made without any kind of warrant and signed off by either a police inspector or superintendent depending on the kind of data.

**Key points of the bill**

∑ Requires web and phone companies to store records of websites visited by every citizen for 12 months for access by police, security services and other public bodies.

∑ Makes explicit in law for the first time security services’ powers for the “bulk collection” of large volumes of personal communications data.

∑ Makes explicit in law for the first time powers of the security services and police to hack and bug into computers and phones. Places new legal obligation on companies to assist in these operations to bypass encryption.

∑ New “double-lock” on ministerial authorisation of intercept warrants with panel of seven judicial commissioners given power of veto. But exemptions allowed in “urgent cases” of up to five days.

∑ Existing system of three oversight commissioners replaced with single investigatory powers commissioner who will be a senior judge.

∑ Prime minister to be consulted in all cases involving interception of MPs’ communications. Safeguards on requests for communications data in other ‘sensitive professions’ such as journalists to be written into law.
PMQs starts in just under 15 minutes.

Labour has just put out a statement from Jeremy Corbyn criticising the government's decision to invite the Egyptian president, Abdel Fatah al-Sisi, to London. Corbyn said:

David Cameron's invitation to Britain today of the Egyptian president and coup leader Abdel Fatah al-Sisi shows contempt for human and democratic rights and threatens, rather than protects, Britain's national security.

Support for dialogue and negotiated conflict resolution in the Middle East is vital to us all. But to welcome and bolster with military support the coup leader who overthrew a democratically elected president in 2013 and has presided over the killing and jailing of many thousands since makes a mockery of government claims to be promoting peace and justice in the region.

Support for dictatorial regimes in the Middle East has been a key factor fuelling the spread of terrorism. Rather than rolling out the red carpet to President Sisi, the prime minister should suspend arms exports to Egypt until democratic and civil rights are restored.

Have some thought for the journalists who will have to make sense of the draft investigatory powers bill quickly. This is from the BBC's Gordon Corera.

Fun day ahead involving reading a 200 clause bill on technical surveillance powers and then condensing it into an easy to understand 2 mins

- Gordon Corera (@gordoncorera) November 4, 2015

Julian Huppert, the former Lib Dem MP, agrees with Henry Porter (see 11.12am) that who sits on the committee scrutinising the bill will be crucial.

One key thing is who will sit on the Joint Committee to study the draft #ipbill. Last time we absolutely slated the previous version! #fb

- Julian Huppert (@julianhuppert) November 4, 2015

Will the draft #ipbill committee have more securocrats on it? Any people knowledgeable about and interested in tech or privacy? #fb

- Julian Huppert (@julianhuppert) November 4, 2015

Henry Porter, the journalist and privacy campaigner, says there are rumours that Paul Murphy, the former Northern Ireland secretary, may chair a joint committee being set up to scrutinise the draft investigatory powers bill.

Murphy is a former chair of the intelligence and security committee, and would be seen as sympathetic to the concerns of the security services.

@AndrewSparrow Who will chair joint committee to examine May bill? Rumours are it is ISC trusty Paul Murphy - not good news for scrutiny.

- henry porter (@HenryCPorter) November 4, 2015

Draft investigatory powers bill - A background reading list

For more background, here's a internet surveillance reading list.

The Guardian story about the draft communications data bill in 2012. And here is the bill itself (pdf).

The report from a joint committee of MPs and peers set up to consider the draft communications data bill (pdf). The report, which was published in December 2012, was very critical, saying the draft bill went too far. Here's an excerpt.

We accept that there is a case for legislation which will provide the law enforcement agencies with some further access to communications data, but we believe that the draft bill pays insufficient
attention to the duty to respect the right to privacy, and goes much further than it need or should for
the purpose of providing necessary and justifiable official access to communications data. Clause 1
would give the secretary of state sweeping powers to issue secret notices to communications service
providers (CSPs) requiring them to retain and disclose potentially limitless categories of data. We
have been told that she has no intention of using the powers in this way. Our main recommendation is
therefore that her powers should be limited to those categories of data for which a case can now be
made. If in future a case can be made for the power to be increased, this should not be done without
effective parliamentary scrutiny. We recommend the procedure for this.

A report from the intelligence and security committee in March this year calling for an overhaul
of surveillance laws. Here is the report (pdf) and here is the news release (pdf).

The report from David Anderson, the government's independent reviewer of terrorism legislation, in June this year called A Question of Trust. This 373-page report set out detailed proposals for a new bill. Here is the press release about it (pdf), here is the report (pdf), and here is the Guardian story about its publication. And here is a Martin Kettle column praising it. This is how it starts:

Occasionally in the long history of British policymaking someone manages to break through the
crudification and reset the terms of an apparently unresolvable public argument. Edwin Chadwick on
the poor law and public health, William Beveridge on the welfare system and Leslie Scarman on the
police all changed things for generations - and for the public good - in their respective fields. The
question today is whether the name of David Anderson - Britain's watchdog on terrorism laws - should
be added to the list of these national reformer-reconcilers.

With a fair wind behind it, his report on the future of surveillance laws, published yesterday, may
eventually prove to have poured calming oils on a stormy argument that British governments have
often seemed incapable of resolving. If Anderson's plea is taken seriously, and we wipe the slate
clean and start again on Britain's efforts to balance security and privacy in the pursuit of crime in the
borderless online world, his report really could be the turning point that policymakers have looked for
and missed ever since 9/11.

A 28-page briefing paper from the House of Commons library about the background to the
publication of the draft investigatory powers bill (pdf).

On the Today programme morning Sara Thornton, chair of the National Police Chiefs’ Council, used
an interview to explain why the police wanted internet surveillance laws to be updated.

Law enforcement needs access to communications data to protect the public and to investigate crime.
We use communications data in day to day investigations. This is about what ordinary detectives do; they
make the vast majority of applications for communications data.

The bottom line is we are just not keeping up with technology. Five or six years ago it used to be
about phone records; just about who's calling who and where, not about the content at all. Of course,
more and more of us are using the internet for those communications now. And therefore we need to
have those internet communications records to find out what communication platforms people are
using.

She also insisted that the police were not interested in looking about people's website browsing
histories.

Can I just say, it is categorically not the case that we want to see people's internet browsing histories.
It is not about that. It is about what communications platforms people are using, such as Facebook or
WhatsApp.

I'll give you a good example. You might remember Operation [Voicer?], a case of a paedophile ring
who were jailed earlier this year. They had been filming the abuse of babies and toddlers and they
had been streaming it on the internet. The gang are all in prison. But we know that over 260 people
viewed that abuse online. We've identified quite a lot of them. But 38 we are still unable to identify.
Now, if we had access to internet connection records, we would be able to find their IP addresses,
their internet protocol addresses, and find them. We are not able to do that at the moment.

Sara Thornton Photograph: Steve Parsons/PA Wire/Press Association Images
Several of the papers have stories previewing today's draft investigatory powers bill, but only two of them have splashed on it.

In the Times (paywall) Sean O'Neill says Theresa May will give judges the power to veto ministers' decisions about interception warrants.

A handful of judges will get the power to veto ministers' decisions on all top-level antiterrorism spying operations under proposals being put forward by the home secretary today.

The panel of specially trained judges - expected to number at least ten - should review thousands of national security warrants each year and hold the intelligence agencies to account, according to draft surveillance laws to be presented to parliament.

The move represents a significant concession by ministers to the privacy lobby's demand for greater scrutiny of spy agencies after the Edward Snowden leaks scandal. It is contained in the draft Investigatory Powers Bill, which aims to set out in more detail than ever before the state's powers to spy on citizens, alongside a new range of safeguards for individuals.

And in the Daily Telegraph Tom Whitehead says the draft bill will allow council officials to be jailed if they misuse snooping powers. (The Daily Mail focuses on the same line in its preview story.) The Telegraph reports:

Town hall officials will face up to two years in prison if they abuse snooping powers under a crackdown on council surveillance to be unveiled on Wednesday.

There is a lot of jargon in internet surveillance legislation that is hard to follow. The BBC has a handy guide translating some of the more difficult terms at the end of this Q&A.
debate about privacy and security (although the debate was much more muted in the UK than it was in America and continental Europe, where lawmakers seemed to take privacy concerns more seriously.)

This year, following the election of a majority Conservative government, David Cameron and May promised to bring the communications data bill back in a revised form. The result is the investigatory powers bill being published this afternoon.

My colleague Alan Travis has written a preview of what we will get. Here is his story, and here is how it starts.

Theresa May is to propose a major extension of the surveillance state when she publishes legislation requiring internet companies to store details of every website visited by customers over the previous year.

The home secretary will try to sweeten the pill of her revived snooper's charter on Wednesday by announcing that the police will need to get judicial authorisation before they can access the internet connection records of an individual - something that is currently banned in the US and every European country, including Britain.

She will also try to strengthen the oversight of Britain's surveillance by replacing the current fragmented system of three separate commissioners with an investigatory powers commissioner who will be a senior judge appointed by the prime minister on the recommendation of the lord chief justice.

I will mostly be focusing on the investigatory powers bill today, although I will also be covering PMQs. Here are the timings.

12pm: David Cameron faces Jeremy Corbyn at PMQs.
12.30pm: Theresa May makes a statement to MPs about the investigatory powers bill. The full bill is published simultaneously by the Home Office.

If you want to follow me on Twitter, I'm on @AndrewSparrow.
Julian Huppert, the former Lib Dem MP, agrees with Henry Porter (see 11.12am) that who sits on the committee scrutinising the bill will be crucial.

One key thing is who will sit on the Joint Committee to study the draft ipbill. Last time we absolutely slated the previous version! #fb

- Julian Huppert (@julianhuppert) November 4, 2015

Will the draft ipbill committee have more securocrats on it? Any people knowledgeable about and interested in tech or privacy? #fb

- Julian Huppert (@julianhuppert) November 4, 2015

Henry Porter, the journalist and privacy campaigner, says there are rumours that Paul Murphy, the former Northern Ireland secretary, may chair a joint committee being set up to scrutinise the draft investigatory powers bill.

Murphy is a former chair of the intelligence and security committee, and would be seen as sympathetic to the concerns of the security services.

@AndrewSparrow Who will chair joint committee to examine May bill? Rumours are it is ISC trusty Paul Murphy - not good news for scrutiny.

- henry porter (@HenryCPorter) November 4, 2015

For more background, here’s a internet surveillance reading list.

The Guardian story about the draft communications data bill in 2012. And here is the bill itself (pdf).

The report from a joint committee of MPs and peers set up to consider the draft communications data bill (pdf). The report, which was published in December 2012, was very critical, saying the draft bill went too far. Here’s an excerpt.

We accept that there is a case for legislation which will provide the law enforcement agencies with some further access to communications data, but we believe that the draft bill pays insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data. Clause 1 would give the secretary of state sweeping powers to issue secret notices to communications service providers (CSPs) requiring them to retain and disclose potentially limitless categories of data. We have been told that she has no intention of using the powers in this way. Our main recommendation is therefore that her powers should be limited to those categories of data for which a case can now be made. If in future a case can be made for the power to be increased, this should not be done without effective parliamentary scrutiny. We recommend the procedure for this.

A report from the intelligence and security committee in March this year calling for an overhaul of surveillance laws. Here is the report (pdf) and here is the news release (pdf).

The report from David Anderson, the government’s independent reviewer of terrorism legislation, in June this year called A Question of Trust. This 373-page report set out detailed proposals for a new bill. Here is the press release about it (pdf), here is the report (pdf), and here is the Guardian story about its publication. And here is a Martin Kettle column praising it. This is how it starts:

Occasionally in the long history of British policymaking someone manages to break through the confusion and reset the terms of an apparently unresolvable public argument. Edwin Chadwick on
the poor law and public health, William Beveridge on the welfare system and Leslie Scarman on the police all changed things for generations - and for the public good - in their respective fields. The question today is whether the name of David Anderson - Britain's watchdog on terrorism laws - should be added to the list of these national reformer-reconcilers.

With a fair wind behind it, his report on the future of surveillance laws, published yesterday, may eventually prove to have poured calming oils on a stormy argument that British governments have often seemed incapable of resolving. If Anderson's plea is taken seriously, and we wipe the slate clean and start again on Britain's efforts to balance security and privacy in the pursuit of crime in the borderless online world, his report really could be the turning point that policymakers have looked for and missed ever since 9/11.

A 28-page briefing paper from the House of Commons library about the background to the publication of the draft **investigatory powers bill** (pdf).

On the Today programme morning Sara Thornton, chair of the National Police Chiefs' Council, used an interview to explain why the police wanted internet surveillance laws to be updated.

Law enforcement needs access to communications data to protect the public and to investigate crime. We use communications data in day to day investigations. This is about what ordinary detectives do; they make the vast majority of applications for communications data.

The bottom line is we are just not keeping up with technology. Five or six years ago it used to be about phone records; just about who's calling who and where, not about the content at all. Of course, more and more of us are using the internet for those communications now. And therefore we need to have those internet communications records to find out what communication platforms people are using.

She also insisted that the police were not interested in looking about people's website browsing histories.

Can I just say, it is categorically not the case that we want to see people's internet browsing histories. It is not about that. It is about what communications platforms people are using, such as Facebook or WhatsApp.

I'll give you a good example. You might remember Operation [Voicer?], a case of a paedophile ring who were jailed earlier this year. They had been filming the abuse of babies and toddlers and they had been streaming it on the internet. The gang are all in prison. But we know that over 260 people viewed that abuse online. We've identified quite a lot of them. But 38 we are still unable to identify. Now, if we had access to internet connection records, we would be able to find their IP addresses, their internet protocol addresses, and find them. We are not able to do that at the moment.

Sara Thornton Photograph: Steve Parsons/PA Wire/Press Association Images

Several of the papers have stories previewing today's draft **investigatory powers bill**, but only two of them have splashed on it.

In the Times (paywall) Sean O'Neill says Theresa May will give judges the power to veto ministers' decisions about interception warrants.

A handful of judges will get the power to veto ministers' decisions on all top-level antiterrorism spying operations under proposals being put forward by the home secretary today.

The panel of specially trained judges - expected to number at least ten - should review thousands of national security warrants each year and hold the intelligence agencies to account, according to draft surveillance laws to be presented to parliament.

The move represents a significant concession by ministers to the privacy lobby's demand for greater scrutiny of spy agencies after the Edward Snowden leaks scandal. It is contained in the draft **Investigatory Powers Bill**, which aims to set out in more detail than ever before the state's powers to spy on citizens, alongside a new range of safeguards for individuals.

enltr#Wednesday's Times front page: Judges get right to veto anti-terror operations
#tomorrowspaperstoday#bbcpaperspic.twitter.com/E15LenmORZ

- Nick Sutton (@suttonnick) November 3, 2015
And in the Daily Telegraph Tom Whitehead says the draft bill will allow council officials to be jailed if they misuse snooping powers. (The Daily Mail focuses on the same line in its preview story.) The Telegraph reports:

Town hall officials will face up to two years in prison if they abuse snooping powers under a crackdown on council surveillance to be unveiled on Wednesday.

A new offence is to be created to target public authorities who inappropriately access phone and email records.

Local authorities will also be banned from accessing the web histories of members of the public when ministers publish the biggest overhaul of spying laws for 15 years.

The measures will be included in the Investigatory Powers Bill which includes a raft of proposals to expand the ability of the police and spy agencies to monitor suspects.

There is a lot of jargon in internet surveillance legislation that is hard to follow. The BBC has a handy guide translating some of the more difficult terms at the end of this Q&A.

There are few issues more fundamental in a liberal democracy than privacy and surveillance, and what powers we decide to give the state to allow it to monitor our communications. But none of this is easy or straightforward. A report earlier this year described one of the key Act's governing this area as "obscure since its inception" and "incomprehensible to all but a tiny band of initiates".

Today Theresa May, the home secretary, is announcing plans for a major overhaul of the legislation governing internet surveillance. We'll be trying to ensure that what she proposes is fully comprehensible, and not just to "initiates".

May's announcement is the culmination of a process lasting more than three years. I will post more on the background later, but here are the key milestones.

In June 2012 the coalition government published a draft communications data bill. This was published because the Home Office believed that changing technology meant it needed to update surveillance laws, but it included plans to monitor internet use, critics dubbed it the "snooper's charter", the Lib Dems said they would never approve it and it was shelved. The legislation never came to parliament.

In June 2013 the Guardian started publishing stories based on leaked information from Edward Snowden revealing the full extent of internet surveillance carried out by the National Security Agency in America and GCHQ in the UK. The revelations triggered a worldwide debate about privacy and security (although the debate was much more muted in the UK than it was in America and continental Europe, where lawmakers seemed to take privacy concerns more seriously.)

This year, following the election of a majority Conservative government, David Cameron and May promised to bring the communications data bill back in a revised form. The result is the Investigatory powers bill being published this afternoon.

My colleague Alan Travis has written a preview of what we will get. Here is his story, and here is how it starts.

Theresa May is to propose a major extension of the surveillance state when she publishes legislation requiring internet companies to store details of every website visited by customers over the previous year.

The home secretary will try to sweeten the pill of her revived snooper's charter on Wednesday by announcing that the police will need to get judicial authorisation before they can access the internet connection records of an individual - something that is currently banned in the US and every European country, including Britain.
She will also try to strengthen the oversight of Britain's surveillance by replacing the current fragmented system of three separate commissioners with an investigatory powers commissioner who will be a senior judge appointed by the prime minister on the recommendation of the lord chief justice.

I will mostly be focusing on the **investigatory powers bill** today, although I will also be covering PMQs. Here are the timings.

12pm: David Cameron faces Jeremy Corbyn at PMQs.
12.30pm: Theresa May makes a statement to MPs about the **investigatory powers bill**. The full bill is published simultaneously by the Home Office.

If you want to follow me on Twitter, I'm on @AndrewSparrow.

block-time updated-timeUpdated at 9.10am GMT

**LOAD-DATE**: November 4, 2015

**LANGUAGE**: ENGLISH

**PUBLICATION-TYPE**: Newspaper

**JOURNAL-CODE**: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc. 
All Rights Reserved

**Return to List**

33 of 104 DOCUMENTS

The Guardian

**November 4, 2015 Wednesday 10:32 AM GMT**

**Theresa May publishes internet surveillance plans - Politics live; Rolling coverage of the day's political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised 'snoopers' charter'**

**BYLINE**: Andrew Sparrow

**SECTION**: POLITICS

**LENGTH**: 1283 words

block-time published-time 10.18am GMT

On the Today programme morning Sara Thornton, chair of the National Police Chiefs' Council, used an interview to explain why the police wanted internet surveillance laws to be updated.

Law enforcement needs access to communications data to protect the public and to investigate crime. We use communications data in day to day investigations. This is about what ordinary detectives do; they make the vast majority of applications for communications data.

The bottom line is we are just not keeping up with technology. Five or six years ago it used to be about phone records; just about who's calling who and where, not about the content at all. Of course, more and more of us are using the internet for those communications now. And therefore we need to have those internet communications records to find out what communication platforms people are using.
She also insisted that the police were not interested in looking about people's website browsing histories.

Can I just say, it is categorically not the case that we want to see people’s internet browsing histories. It is not about that. It is about what communications platforms people are using, such as Facebook or WhatsApp.

I'll give you a good example. You might remember Operation [Voicer?], a case of a paedophile ring who were jailed earlier this year. They had been filming the abuse of babies and toddlers and they had been streaming it on the internet. The gang are all in prison. But we know that over 260 people viewed that abuse online. We've identified quite a lot of them. But 38 we are still unable to identify. Now, if we had access to internet connection records, we would be able to find their IP addresses, their internet protocol addresses, and find them. We are not able to do that at the moment.

Sara Thornton
Photograph: Steve Parsons/PA Wire/Press Association Images

Several of the papers have stories previewing today’s draft investigatory powers bill, but only two of them have splashed on it.

In the Times (paywall) Sean O'Neill says Theresa May will give judges the power to veto ministers' decisions about interception warrants.

A handful of judges will get the power to veto ministers' decisions on all top-level antiterrorism spying operations under proposals being put forward by the home secretary today.

The panel of specially trained judges - expected to number at least ten - should review thousands of national security warrants each year and hold the intelligence agencies to account, according to draft surveillance laws to be presented to parliament.

The move represents a significant concession by ministers to the privacy lobby's demand for greater scrutiny of spy agencies after the Edward Snowden leaks scandal. It is contained in the draft Investigatory Powers Bill, which aims to set out in more detail than ever before the state’s powers to spy on citizens, alongside a new range of safeguards for individuals.

enltrWednesday's Times front page: Judges get right to veto anti-terror operations
#tomorrowspaperstoday#bbcpaperspic.twitter.com/E15LenmORZ

- Nick Sutton (@suttonnick) November 3, 2015

And in the Daily Telegraph Tom Whitehead says the draft bill will allow council officials to be jailed if they misuse snooping powers. (The Daily Mail focuses on the same line in its preview story.) The Telegraph reports:

Town hall officials will face up to two years in prison if they abuse snooping powers under a crackdown on council surveillance to be unveiled on Wednesday.

A new offence is to be created to target public authorities who inappropriately access phone and email records.

Local authorities will also be banned from accessing the web histories of members of the public when ministers publish the biggest overhaul of spying laws for 15 years.

The measures will be included in the Investigatory Powers Bill which includes a raft of proposals to expand the ability of the police and spy agencies to monitor suspects.

enltrWednesday's Telegraph front page: Prison for officials who abuse snooping powers
#tomorrowspaperstoday#bbcpaperspic.twitter.com/HvJsBln9DK

- Nick Sutton (@suttonnick) November 3, 2015

There is a lot of jargon in internet surveillance legislation that is hard to follow. The BBC has a handy guide translating some of the more difficult terms at the end of this Q&A.

There are few issues more fundamental in a liberal democracy than privacy and surveillance, and what powers we decide to give the state to allow it to monitor our communications. But none of this is easy or straightforward. A report earlier this year described one of the key Act’s governing this area as “obscure since its inception” and “incomprehensible to all but a tiny band of initiates”.

167
Today Theresa May, the home secretary, is announcing plans for a major overhaul of the legislation governing internet surveillance. We’ll be trying to ensure that what she proposes is fully comprehensible, and not just to “initiates”.

May’s announcement is the culmination of a process lasting more than three years. I will post more on the background later, but here are the key milestones.

In June 2012 the coalition government published a draft communications data bill. This was published because the Home Office believed that changing technology meant it needed to update surveillance laws, but it included plans to monitor internet use, critics dubbed it the "snoopers’ charter", the Lib Dems said they would never approve it and it was shelved. The legislation never came to parliament.

In June 2013 the Guardian started publishing stories based on leaked information from Edward Snowden revealing the full extent of internet surveillance carried out by the National Security Agency in America and GCHQ in the UK. The revelations triggered a worldwide debate about privacy and security (although the debate was much more muted in the UK than it was in America and continental Europe, where lawmakers seemed to take privacy concerns more seriously.)

This year, following the election of a majority Conservative government, David Cameron and May promised to bring the communications data bill back in a revised form. The result is the investigatory powers bill being published this afternoon.

My colleague Alan Travis has written a preview of what we will get. Here is his story, and here is how it starts.

Theresa May is to propose a major extension of the surveillance state when she publishes legislation requiring internet companies to store details of every website visited by customers over the previous year.

The home secretary will try to sweeten the pill of her revived snoopers charter on Wednesday by announcing that the police will need to get judicial authorisation before they can access the internet connection records of an individual - something that is currently banned in the US and every European country, including Britain.

She will also try to strengthen the oversight of Britain’s surveillance by replacing the current fragmented system of three separate commissioners with an investigatory powers commissioner who will be a senior judge appointed by the prime minister on the recommendation of the lord chief justice.

I will mostly be focusing on the investigatory powers bill today, although I will also be covering PMQs. Here are the timings.

12pm: David Cameron faces Jeremy Corbyn at PMQs.

12.30pm: Theresa May makes a statement to MPs about the investigatory powers bill. The full bill is published simultaneously by the Home Office.

If you want to follow me on Twitter, I'm on @AndrewSparrow.
Theresa May publishes internet surveillance plans - Politics live; Rolling coverage of the day's political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised 'snoopers' charter'

BYLINE: Andrew Sparrow

SECTION: POLITICS

LENGTH: 968 words

Several of the papers have stories previewing today's draft investigatory powers bill, but only two of them have splashed on it.

In the Times (paywall) Sean O'Neill says Theresa May will give judges the power to veto ministers' decisions about interception warrants.

A handful of judges will get the power to veto ministers' decisions on all top-level antiterrorism spying operations under proposals being put forward by the home secretary today.

The panel of specially trained judges - expected to number at least ten - should review thousands of national security warrants each year and hold the intelligence agencies to account, according to draft surveillance laws to be presented to parliament.

The move represents a significant concession by ministers to the privacy lobby's demand for greater scrutiny of spy agencies after the Edward Snowden leaks scandal. It is contained in the draft Investigatory Powers Bill, which aims to set out in more detail than ever before the state's powers to spy on citizens, alongside a new range of safeguards for individuals.

And in the Daily Telegraph Tom Whitehead says the draft bill will allow council officials to be jailed if they misuse snooping powers. (The Daily Mail focuses on the same line in its preview story.) The Telegraph reports:

Town hall officials will face up to two years in prison if they abuse snooping powers under a crackdown on council surveillance to be unveiled on Wednesday.

A new offence is to be created to target public authorities who inappropriately access phone and email records.

Local authorities will also be banned from accessing the web histories of members of the public when ministers publish the biggest overhaul of spying laws for 15 years.

The measures will be included in the Investigatory Powers Bill which includes a raft of proposals to expand the ability of the police and spy agencies to monitor suspects.

There is a lot of jargon in internet surveillance legislation that is hard to follow. The BBC has a handy guide translating some of the more difficult terms at the end of this Q&A.
There are few issues more fundamental in a liberal democracy than privacy and surveillance, and what powers we decide to give the state to allow it to monitor our communications. But none of this is easy or straightforward. A report earlier this year described one of the key Act's governing this area as "obscure since its inception" and "incomprehensible to all but a tiny band of initiates".

Today Theresa May, the home secretary, is announcing plans for a major overhaul of the legislation governing internet surveillance. We'll be trying to ensure that what she proposes is fully comprehensible, and not just to "initiates".

May's announcement is the culmination of a process lasting more than three years. I will post more on the background later, but here are the key milestones.

In June 2012 the coalition government published a draft communications data bill. This was published because the Home Office believed that changing technology meant it needed to update surveillance laws, but it included plans to monitor internet use, critics dubbed it the "snooper's charter", the Lib Dems said they would never approve it and it was shelved. The legislation never came to parliament.

In June 2013 the Guardian started publishing stories based on leaked information from Edward Snowden revealing the full extent of internet surveillance carried out by the National Security Agency in America and GCHQ in the UK. The revelations triggered a worldwide debate about privacy and security (although the debate was much more muted in the UK than it was in America and continental Europe, where lawmakers seemed to take privacy concerns more seriously.)

This year, following the election of a majority Conservative government, David Cameron and May promised to bring the communications data bill back in a revised form. The result is the investigatory powers bill being published this afternoon.

My colleague Alan Travis has written a preview of what we will get. Here is his story, and here is how it starts.

Theresa May is to propose a major extension of the surveillance state when she publishes legislation requiring internet companies to store details of every website visited by customers over the previous year.

The home secretary will try to sweeten the pill of her revived snooper's charter on Wednesday by announcing that the police will need to get judicial authorisation before they can access the internet connection records of an individual - something that is currently banned in the US and every European country, including Britain.

She will also try to strengthen the oversight of Britain's surveillance by replacing the current fragmented system of three separate commissioners with an investigatory powers commissioner who will be a senior judge appointed by the prime minister on the recommendation of the lord chief justice.

I will mostly be focusing on the investigatory powers bill today, although I will also be covering PMQs. Here are the timings.

12pm: David Cameron faces Jeremy Corbyn at PMQs.

12.30pm: Theresa May makes a statement to MPs about the investigatory powers bill. The full bill is published simultaneously by the Home Office.

If you want to follow me on Twitter, I'm on @AndrewSparrow.
Theresa May publishes internet surveillance plans - Politics live; Rolling coverage of the day's political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised 'snoopers' charter'

BYLINE: Andrew Sparrow

SECTION: POLITICS

LENGTH: 593 words

There is a lot of jargon in internet surveillance legislation that is hard to follow. The BBC has a handy guide translating some of the more difficult terms at the end of this Q&A.

There are few issues more fundamental in a liberal democracy than privacy and surveillance, and what powers we decide to give the state to allow it to monitor our communications. But none of this is easy or straightforward. A report earlier this year described one of the key Act's governing this area as "obscure since its inception" and "incomprehensible to all but a tiny band of initiates".

Today Theresa May, the home secretary, is announcing plans for a major overhaul of the legislation governing internet surveillance. We'll be trying to ensure that what she proposes is fully comprehensible, and not just to "initiates".

May's announcement is the culmination of a process lasting more than three years. I will post more on the background later, but here are the key milestones.

In June 2012 the coalition government published a draft communications data bill. This was published because the Home Office believed that changing technology meant it needed to update surveillance laws, but it included plans to monitor internet use, critics dubbed it the "snoopers' charter", the Lib Dems said they would never approve it and it was shelved. The legislation never came to parliament.

In June 2013 the Guardian started publishing stories based on leaked information from Edward Snowden revealing the full extent of internet surveillance carried out by the National Security Agency in America and GCHQ in the UK. The revelations triggered a worldwide debate about privacy and security (although the debate was much more muted in the UK than it was in America and continental Europe, where lawmakers seemed to take privacy concerns more seriously.)

This year, following the election of a majority Conservative government, David Cameron and May promised to bring the communications data bill back in a revised form. The result is the investigatory powers bill being published this afternoon.

My colleague Alan Travis has written a preview of what we will get. Here is his story, and here is how it starts.
Theresa May is to propose a major extension of the surveillance state when she publishes legislation requiring internet companies to store details of every website visited by customers over the previous year.

The home secretary will try to sweeten the pill of her revived snooper’s charter on Wednesday by announcing that the police will need to get judicial authorisation before they can access the internet connection records of an individual - something that is currently banned in the US and every European country, including Britain.

She will also try to strengthen the oversight of Britain’s surveillance by replacing the current fragmented system of three separate commissioners with an investigatory powers commissioner who will be a senior judge appointed by the prime minister on the recommendation of the lord chief justice.

I will mostly be focusing on the investigatory powers bill today, although I will also be covering PMQs. Here are the timings.

12pm: David Cameron faces Jeremy Corbyn at PMQs.

12.30pm: Theresa May makes a statement to MPs about the investigatory powers bill. The full bill is published simultaneously by the Home Office.

If you want to follow me on Twitter, I'm on @AndrewSparrow.

block-time updated-time Updated at 9.10am GMT

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc. All Rights Reserved

Return to List

36 of 104 DOCUMENTS

The Guardian

November 4, 2015 Wednesday 9:12 AM GMT

Theresa May publishes internet surveillance plans - Politics live; Rolling coverage of the day's political developments as they happen, including Theresa May publishing the draft investigatory powers bill, seen as the revised 'snoopers' charter'

BYLINE: Andrew Sparrow

SECTION: POLITICS

LENGTH: 556 words

block-time published-time 9.09am GMT

There are few issues more fundamental in a liberal democracy than privacy and surveillance, and what powers we decide to give the state to allow it to monitor our communications. But none of this is easy or straightforward. A report earlier this year described one of the key Act's governing this area as "obscure since its inception" and "incomprehensible to all but a tiny band of initiates".
Today Theresa May, the home secretary, is announcing plans for a major overhaul of the legislation governing internet surveillance. We’ll be trying to ensure that what she proposes is fully comprehensible, and not just to “initiates”.

May’s announcement is the culmination of a process lasting more than three years. I will post more on the background later, but here are the key milestones.

In June 2012 the coalition government published a draft communications data bill. This was published because the Home Office believed that changing technology meant it needed to update surveillance laws, but it included plans to monitor internet use, critics dubbed it the "snoopers’ charter", the Lib Dems said they would never approve it and it was shelved. The legislation never came to parliament.

In June 2013 the Guardian started publishing stories based on leaked information from Edward Snowden revealing the full extent of internet surveillance carried out by the National Security Agency in America and GCHQ in the UK. The revelations triggered a worldwide debate about privacy and security (although the debate was much more muted in the UK than it was in America and continental Europe, where lawmakers seemed to take privacy concerns more seriously.)

This year, following the election of a majority Conservative government, David Cameron and May promised to bring the communications data bill back in a revised form. The result is the investigatory powers bill being published this afternoon.

My colleague Alan Travis has written a preview of what we will get. Here is his story, and here is how it starts.

Theresa May is to propose a major extension of the surveillance state when she publishes legislation requiring internet companies to store details of every website visited by customers over the previous year.

The home secretary will try to sweeten the pill of her revived snoopers charter on Wednesday by announcing that the police will need to get judicial authorisation before they can access the internet connection records of an individual - something that is currently banned in the US and every European country, including Britain.

She will also try to strengthen the oversight of Britain’s surveillance by replacing the current fragmented system of three separate commissioners with an investigatory powers commissioner who will be a senior judge appointed by the prime minister on the recommendation of the lord chief justice.

I will mostly be focusing on the investigatory powers bill today, although I will also be covering PMQs. Here are the timings.

12pm: David Cameron faces Jeremy Corbyn at PMQs.
12.30pm: Theresa May makes a statement to MPs about the investigatory powers bill. The full bill is published simultaneously by the Home Office.

If you want to follow me on Twitter, I'm on @AndrewSparrow.

block-time updated-timeUpdated at 9.10am GMT

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc. All Rights Reserved
The Government's Investigatory Powers Bill, outlined by the Home Secretary, has been dubbed a "snooper's charter" by critics. It may, in fact, offer a licence to security agencies and to criminals that we come to regret.

Existing legislation is less than satisfactory, either because it has been abused by the authorities - as in the case of the Regulation of Investigatory Powers Act - or because it is out of step with modern technology. It is perfectly reasonable that the Government should want to initiate a thorough overhaul.

Yet there is a paradox in the approach taken by Theresa May and her officials. We are told that the authorities need to stay one step ahead of terrorists and criminal minds, and that they cannot do so unless underlying legislation is responsive to the reality of today's internet world. But it is precisely that reality - of hacking and data breaches - which will cause many people to be anxious about the mass retention of their data by communications companies.

The failure by TalkTalk to keep its customer data secure brought home just how vulnerable big corporations are to hackers. While civil liberties campaigners focus on the invidious potential for the state to examine our private internet browsing history, for ordinary people the greater worry may be the ability (or otherwise) of commercial giants to hang on to data securely for the year demanded by the Government.

That's not to say that the fundamental anxiety about state snooping should be underplayed. Nor should we be fooled by the notion that the new proposals amount to a vastly watered-down version of the plans Ms May sought to bring forward during the last parliament and which were stymied by the Liberal Democrats. This time, the Lib Dems are thwarted themselves by lack of numbers and appear to have acquiesced in the Government's plans. Likewise, Labour has swung behind the measures: the shadow Home Secretary, Andy Burnham, says the Bill is "neither a snooper's charter nor a plan for mass surveillance".

Such a lack of political opposition is surprising, and it may be left to the Lords once again to raise some sage eyebrows. After all, whatever safeguards are in place, the idea that every citizen of the UK will now have their internet browsing history kept on file for a year by their broadband provider, for perusal by security agencies should the need arise, is surely staggering.

As always, there will be those who contend that people who do no wrong have nothing to fear. That is facile, and, in any case, the authorities are hardly infallible.

Ms May urges us not to worry: for the most part, we're told, the police won't be able to access our full browsing history, just the basics about which sites we visit - the "modern equivalent of an itemised phone bill". Except that it isn't. Once again the Government demonstrates that, in endeavouring to...
bring difficult legislation up to date, it has little real comprehension of how fundamental the internet has become to most people’s lives. To proclaim it simply the telephone of the 21st century is either obtuse or a deliberate attempt to mislead.

None of this should be taken as a lack of support for Britain’s security services. They do a difficult job and, on occasion, will require controlled access to the communications data of suspects. But let’s not pretend that the Government’s Bill does not have the potential to impact on our civil liberties in fundamental ways.

**LOAD-DATE:** November 4, 2015

**LANGUAGE:** ENGLISH

**PUBLICATION-TYPE:** Newspaper; Web Publication

**JOURNAL-CODE:** WEBI

Theresa May was accused of overseeing a "breath-taking attack" on privacy as she set out plans to give the police and security services the power to access records of every Briton’s use of the internet without requiring a warrant.

The Home Secretary won praise from political rivals for abandoning elements of the "snooper's charter", which was blocked during the Coalition Government, and for giving judges a key role in approving surveillance exercises.

Read more

May vows to make internet a no-go area for terrorists and paedophiles

But she came under fire from civil liberties groups over moves to force communications companies to hold data about internet use for up to 12 months and to require them to help spies to hack into suspects’ smartphones and computers. Critics raised fears that the bulk collection could leave huge tranches of personal information vulnerable to attacks similar to the hacking last week of TalkTalk’s customer database.

The draft Investigatory Powers Bill will overhaul the existing legislation, putting all hacking and bugging by the state on a statutory basis. The move reflects widespread agreement that current laws are outdated because of technological advances. It is also a response to pressure for the Government
to be more transparent about surveillance after Edward Snowden's revelations about mass "data-mining" exercises by GCHQ.

Ms May told the Commons the proposed Bill would provide some of the "strongest protections and safeguards anywhere in the democratic world". She said: "There should be no area of cyberspace which is a haven for those who seek to harm us, to plot, poison minds and peddle hatred under the radar."

The measures were backed by the shadow Home Secretary Andy Burnham, potentially putting him at odds with Jeremy Corbyn. He agreed the proposed Bill was not "a plan for mass surveillance".

Nick Clegg, who as Liberal Democrat leader blocked the snooper's charter, said the revised proposals were much improved, but warned: "I have a feeling that under the bonnet it still retains some of the flaws of its predecessor."

While Nick Clegg said the charter's proposals have been improved, the former Lib Dem leader remains sceptical (Getty)

Ms May announced a new "double lock" approval system under which agencies are allowed to see the content of communications or bug telephone calls. Initial approval would be given by a Cabinet minister - usually the Home Secretary - but have to be approved by a "judicial commissioner", a security-cleared senior judge. The only exception would be in operations deemed urgent because lives could be put at risk without rapid action. Web and phone companies would retain "internet connection records", listing websites visited but not every page visited, for a year.

The security services, police and other public bodies - but not local councils - would be allowed to examine the information on the authority of a senior officer. There would be no need for ministerial or judicial approval.

The companies would also be legally required to assist the authorities in "giving effect to equipment interference", such as hacking operations to download the contents of a mobile phone's memory. All police forces will be permitted to use the tactic under the new regime, with a code of practice to regulate the "more sensitive and intrusive techniques".

Read more

UK Government forced into huge climbdown over giving spies new powers

The Met chief is caught in the crossfire between Johnson and May

Snooper's charter calls on firms to store clients' data for a year

Liberty said the Bill gave extensive new powers to the authorities to track and hack private information with few privacy safeguards. It said the promise of judicial approval of surveillance warrants would in practice amount to a "rubber-stamping exercise". Its director, Shami Chakrabarti, said: "This long-awaited Bill constitutes a breath-taking attack on the internet security of every man, woman and child in our country. We must now look to Parliament to step in where ministers have failed, and strike a better balance between privacy and surveillance."

Anne Jellenna, chief executive officer of the Web Foundation, said: "The Bill seeks to introduce mass surveillance of every Briton's internet connection records without warrants, something which should be unthinkable in a modern democracy."

She said the requirement for firms to store records of every citizen's computer use was "deeply misguided and is neither necessary nor proportionate. It will hurt UK businesses, create new vulnerabilities for criminals to attack, and ride roughshod over the right to privacy."

The Green MP Caroline Lucas said: "The cosy consensus on surveillance that appears to have taken hold in Westminster is troubling. Many of the aspects of this Bill need far more scrutiny."
Theresa May today promised there would be nowhere for terrorists and paedophiles to hide in
cyberspace as she detailed sweeping powers for security services and police to fight crime in the
digital age.

But she insisted new legislation governing surveillance of mobile phones, emails and internet use did
not amount to a revival of her "snooper's charter" plans which were blocked in the last government.
She reassured MPs: "This is not surveillance."

The new draft Investigatory Powers Bill has been described by the Prime Minister as one of the most
important pieces of legislation of the next five years.

It follows widespread acknowledgement that current legislation has failed to keep pace with rapid
changes in technology.

Read more

Internet companies will be required to store records of web and social media use for up to 12 months,
but not their full browsing history. For instance police would be able to see they have visited Google,
but not see what searches they have made.

Firms will be legally required to help the security services to hack into suspects' smartphones and
computers. Powers enshrined in the legislation will enable the agencies to gain access to computers
to covertly download the contents of a mobile phone during a search.

Ms May announced a new "double lock" approval system under which agencies can see the content
of communications or hack into computers and phones. Initial approval for operations would be
initially given by a Cabinet minister - usually the Home Secretary - but have to be approved by a
"judicial commissioner", security-cleared senior judge. The only exception would be in operations
deemed urgent because lives could be put at risk without rapid action.

The Home Secretary told MPs that while the "digital society" had presented all with benefits but had
also been "exploited by serious and organised criminals, online fraudsters and terrorists" that posed
serious challenges for the security agencies.

She said: "The threat is clear. In the past 12 months alone six significant terrorist plots have been
disrupted here in the UK, as well as a number of further plots overseas."

She said of the Bill "It will not include powers to force UK companies to capture and retain third party
internet traffic from companies based overseas. It will not compel overseas communications service
providers to meet our domestic retention obligations for communications data."
And it will not ban encryption or do anything to undermine the security of people's data. And the substance of all of the recommendations by the Joint Scrutiny Committee which examined that draft Bill have been accepted.

"So today's Bill represents a significant departure from the proposals of the past."

She said the bill provide some of the "strongest protections and safeguards anywhere in the democratic world".

Andy Burnham, the shadow home secretary, welcomed the proposals laid out in the draft bill, praising Ms May for reconsidering plans set out in the 'snooper's charter' and the two-stage accountability process. "We are pleased to see that the Home Secretary has listened," Mr Burnham said. "This is neither a snooper's charter, nor a plan for mass surveillance."

However he received an immediate backlash on Twitter for being so quick to back the plans before fully scrutinising the bill and is likely to come under fire from some of the party's more libertarian voices.

Theresa May today promised there would be nowhere for terrorists and paedophiles to hide in cyberspace as she detailed sweeping powers for security services and police to fight crime in the digital age.

But she insisted new legislation governing surveillance of mobile phones, emails and internet use did not amount to a revival of her "snooper's charter" plans which were blocked in the last government. She reassured MPs: "This is not surveillance."

The new draft Investigatory Powers Bill has been described by the Prime Minister as one of the most important pieces of legislation of the next five years.
It follows widespread acknowledgement that current legislation has failed to keep pace with rapid changes in technology.

Read more

Government to hack into phones easily, get data on internet use

Government already has wide-sweeping surveillance powers

**Snooper's** charter calls on firms to store clients' data for a year

Internet companies will be required to store records of web and social media use for up to 12 months, but not their full browsing history. For instance police would be able to see they have visited Google, but not see what searches they have made.

Firms will be legally required to help the security services to hack into suspects' smartphones and computers. Powers enshrined in the legislation will enable the agencies to gain access to computers to covertly download the contents of a mobile phone during a search.

Ms May announced a new "double lock" approval system under which agencies can see the content of communications or hack into computers and phones. Initial approval for operations would be initially given by a Cabinet minister - usually the Home Secretary - but have to be approved by a "judicial commissioner", security-cleared senior judge. The only exception would be in operations deemed urgent because lives could be put at risk without rapid action.

The Home Secretary told MPs that while the "digital society" had presented all with benefits but had also been "exploited by serious and organised criminals, online fraudsters and terrorists" that posed serious challenges for the security agencies.

She said: "The threat is clear. In the past 12 months alone six significant terrorist plots have been disrupted here in the UK, as well as a number of further plots overseas."

She said of the Bill "It will not include powers to force UK companies to capture and retain third party internet traffic from companies based overseas. It will not compel overseas communications service providers to meet our domestic retention obligations for communications data.

And it will not ban encryption or do anything to undermine the security of people's data. And the substance of all of the recommendations by the Joint Scrutiny Committee which examined that draft Bill have been accepted.

"So today's Bill represents a significant departure from the proposals of the past."

She said the bill provide some of the "strongest protections and safeguards anywhere in the democratic world".

Andy Burnham, the shadow home secretary, welcomed the proposals laid out in the draft bill, praising Ms May for reconsidering plans set out in the 'snooper's charter' and the two-stage accountability process. "We are pleased to see that the Home Secretary has listened," Mr Burnham said. "This is neither a snooper's charter, nor a plan for mass surveillance."

However he received an immediate backlash on Twitter for being so quick to back the plans before fully scrutinising the bill and is likely to come under fire from some of the party's more libertarian voices.

**LOAD-DATE:** November 4, 2015

**LANGUAGE:** ENGLISH

**PUBLICATION-TYPE:** Newspaper; Web Publication

**JOURNAL-CODE:** WEBI
PMQs live: Jeremy Corbyn accuses David Cameron of ignoring a looming ‘winter crisis’ in the NHS; Draft Bill will increase ability of intelligence services to obtain access to personal internet use of citizens

BYLINE: Adam Withnall

SECTION: UK POLITICS

LENGTH: 366 words

Here are the latest politics updates:

- **Snooper's Charter** calls on communications firms to store clients’ phone and internet data for a year
  - Junior doctors offered 11% pay rise as Jeremy Hunt bids to avoid NHS strike
  - HMRC has made 'little or no progress' on tax avoidance transparency, MPs warn
  - Trade Union Bill: Sajid Javid drops social media measures as part of Government climb down

David Cameron faces PMQs amid controversy over his support for a so-called "Snooper's Charter", which he describes as plans to ensure terrorists and child snatchers cannot have a "safe space" to communicate online beyond the reach of the authorities.

The Prime Minister insisted the UK's spies and police needed to be able to see who suspects had communicated with over the internet.

Proposed new laws will be published today covering the tools available to police and intelligence agencies to fight terrorism and serious crime in the digital age.

In a potential area of controversy, measures requiring internet firms to store internet connection records (ICRs) to respond to the increasing use of apps and social media for communication are expected to be included in the draft Investigatory Powers Bill.

However, sources said access to ICRs will be controlled and they will not include a full browsing history or reveal every web page visited, with strict limits on accessing the records.

Security services will retain the capacity to intercept the content of communications after obtaining a warrant.

It is understood that ministers have ruled out any proposal to restrict encryption or ban it, despite fears in the intelligence community that advanced online security measures risk leaving them locked out of some areas of cyber space.

Mr Cameron told ITV's This Morning on Tuesday: "At heart what this whole Investigatory Powers Bill is really about is actually something quite simple, because we all know when it comes to missing children or hideous crimes and the like we all know it's absolutely vital for the police to be able to know who called who and when."

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI
Record of EVERY website you visit to be held for a year with tech firms forced to help spies hack phones and computers

BYLINE: MATT CHORLEY, POLITICAL EDITOR FOR MAILONLINE

SECTION: NEWS

LENGTH: 1447 words

Home Secretary Theresa May wants more powers for MI5, MI6 and GCHQ to prepare agencies to tackle crime in digital age. Web firms will keep record of all websites visited in previous 12 months, Spooks will need a warrant signed off by ministers to obtain the list, Panel of judges to have a veto over thousands of national security warrants.

Details of every website visited will be stored for up to a year to be accessed by police and spooks under new spying laws unveiled today.

Home Secretary Theresa May told MPs that in the ‘digital age’ MI5, MI6, GCHQ and the police should be able to see which websites suspected terrorists and criminals have logged on to.

Communications firms will also be legally required to help spies hack into suspects' smartphones and computers.

Stressing that it will not mean spy agencies seeing every web page visited, Mrs May promised the 'strongest protections and safeguards anywhere in the democratic world'.

A 'powerful and independent' senior judge will hold intelligence agencies to account with the power to overrule warrants signed off by senior ministers.

Unveiling the draft Investigatory Powers Bill, Mrs May told the Commons that the internet and mobile technology had brought huge benefits to millions of people.

But she said some of the benefits are being 'exploited by serious organised criminals, fraudsters and terrorists'.

Mrs May said it was wrong that police investigating the abduction of a child are able to access phone records to help track the victim but not web and social media contacts.

She said: 'Never before has so much information been in the public domain about the activities of our police and security services, as well as the oversight, safeguard and authorisation arrangements which govern them.

'I am clear we need to update our legislation to ensure it is modern, fit for purpose and can respond to emerging threats as technology advances.

'There should be no area of cyberspace which is a haven for those who seek to harm us to plot, poison minds and peddle hatred under the radar.

'But I am also clear that the exercise and scope of investigatory powers should be clearly set out and subject to stringent safeguards and robust oversight.'
She argued that the bill will establish 'world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world'.

Internet firms will have to keep records of website use for 12 months, detailing when emails were sent or when people connected to social media sites, such as Twitter, Facebook and WhatsApp.

With a warrant MI5, MI6, GCHQ and the police will be able to find out details of the website a person has visited, but not which pages they have viewed within that site.

This would mean, for example, police can see someone has visited Google.co.uk, but not what searches they have made.

A further warrant would be required to view the content of any communications. However, councils will be barred from having any access to the internet records.

The draft bill will also force web giants to hand over the contents of encrypted apps and emails on production of a warrant.

UK technology firms will be legally obliged to help intelligence agencies in ‘giving effect to equipment interference’ - allowing them to hack smartphones, laptops and computers.

It can involve remote access to computers to covertly download the contents of a mobile phone during a search.

It will end a voluntary agreement with firms and will make them legally obliged to provide assistance in future.

However, firms based overseas will not be affected by the new laws, which Labour said meant there was a ‘big hole’ in the plans.

The bill also confirmed plans for a panel of seven High Court judges to have a veto over ministers including Mrs May, Foreign Secretary Philip Hammond and Northern Ireland Secretary Theresa Villiers who last year authorised 2,700 spying operations.

An overhaul of the oversight arrangements which will be headed by a new Investigatory Powers Commissioner, who will be a senior judge.

In a significant concession to allay privacy concerns, the judges will review all of the thousands of national security warrants signed off every year.

The decisions by ministers to allow MI5, MI6 and GCHQ to tap phones or hack computers could be overturned by the judges.

Ministers have ruled out any proposal to restrict encryption or ban it, despite fears in the intelligence community that advanced online security measures risk leaving them locked out of some areas of cyberspace.

A number of proposals from the abandoned ‘Snooper’s charter’ have been ruled out, such as powers to demand UK-based communications service providers (CSPs) to capture and store internet traffic from companies based in the US.

In the Commons earlier David Cameron told MPs that communications data had been ‘absolutely vital’ in catching criminals including rapists and child abductors.

He said the power for intelligence agencies to see who criminals had contacted must continue.

David Cameron’s official spokesman said: ‘The Prime Minister underlined that this is about maintaining the agencies’ current capabilities, that this is about - in a nutshell - the powers we need to keep us safe and about increasing public confidence in what they do in the process.’

Mr Cameron told ministers ‘this would be one of the most important pieces of legislation during this parliament because it goes to the heart of the Government’s duty to keep the British public safe’.

Officials claim the Bill will set ‘new standards for openness and transparency’, including ‘world-leading oversight arrangements’.

But Whitehall insiders are braced for a ferocious fight with civil liberties groups, campaigning MPs and the House of Lords.

Labour’s shadow home secretary Andy Burnham said there was a ‘broad acceptance’ that a new law was needed.

He told Sky News: ‘The online world has created blind spots the authorities can’t see any more.'
'I'm not going to play politics with this issue,' he added.

WHAT THE NEW SNOOPING LAWS WILL ALLOW... AND WHAT IS NOT INCLUDED

The draft Investigatory Powers Bill is published today. Here are some of the key questions surrounding the legislation.

What is it?
New legislation drawn up in an attempt to bring the snooping powers available to police and intelligence agencies to tackle terrorism and serious crime in the digital age under one legal umbrella for the first time.

Why do we need a new Bill?
The current system is seen as an unwieldy patchwork of different powers covered by different laws. But there is also a logistical reason - the current laws expire at the end of 2016.

What powers will the Bill cover?
Current tactics such as access to communications data - the who, when and where but not the content, targeted interception of electronic communications, the collection of bulk data and the ability to mount IT attacks - known as equipment interference - will all be retained.

Will there be anything new in it?
A number of the Bill's proposals have trickled out. Firms will now be required to store data relating to people's web and social media use, but officials stressed internet connection records (ICRs) will not cover users' full browsing history or include the actual content of a communication. Councils, which can request communications data, will be banned from accessing ICRs. The Bill is expected to introduce a role for judges in the process for authorising the more intrusive capabilities, such as interception operations, while a new criminal offence will be created to prevent abuse by public authorities of communications data powers.

What is not in it?
Ministers have ruled out any attempt to ban encryption, despite concerns that it risks leaving authorities locked out of some areas of cyberspace. A number of proposals from the abandoned 'Snooper's charter' have been ruled out, such as powers to demand UK-based communications service providers (CSPs) to capture and store internet traffic from companies based in the US.

Will the Bill get through Parliament easily?
The Conservatives now have the majority they did not have when the Communications Data Bill was ditched in 2013, but the new laws are still likely to be controversial, with privacy campaigners, opposition MPs and backbenchers primed to examine its contents closely.

How long will it be before this set of laws is out of date?
The Regulation of Investigatory Powers Act, the central piece of legislation in this arena, was passed 15 years ago. Given the pace of technological change today, it is questionable whether the new Bill could last until 2030 without revision.
Could Apple stop selling the iPhone in the UK? Government considers ban of end-to-end encryption method used by devices

Jimmy Wales, founder of Wikipedia, tweeted: ‘I would like to see Apple refuse to sell iPhone in the UK if gov’t bans end-to-end encryption’

This type of encryption - when only the sender and recipient of messages can decipher them - could be banned in the Investigatory Powers Bill. Draft bill to give security services better access to online communications, will be published later today, and voted on next year.

Wikipedia's founder has questioned whether Apple will continue to be able to sell its latest iPhones in the UK if Parliament bans end-to-end encryption.

The handset offers this type of encryption - when only the sender and recipient of messages can decipher them - meaning there is no way for law enforcement agencies to access hidden criminal messages, for example.

Jimmy Wales raised the issue on Twitter ahead of the publication of the Investigatory Powers Bill, which is set to give the police and security services more powers to access online messages.

He tweeted: ‘I would like to see Apple refuse to sell iPhone in UK if gov’t bans end-to-end encryption. Does Parliament dare be that stupid?’

Under the draft bill, tech companies such as Apple and Facebook will no longer be able to offer customers encryption that’s so good they cannot decipher messages if they are asked to by security agencies.

This means the forthcoming law could force firms to hand over customers’ unencrypted communications if requested by police and spy agencies, The Telegraph reported.

The move follows concerns that an increasing number of encryption messaging apps and devices are now inaccessible to anyone other than the users themselves.

Last month, Apple told a US judge that accessing data stored on a locked iPhone running the latest software is impossible.

Apple’s position came to light after a federal magistrate judge in Brooklyn, New York, sought Apple’s input as he weighed a US Justice Department request to force the company to help authorities access a seized iPhone.

In court papers, Apple said that for the 90 per cent of its devices running iOS 8 or higher, granting the Justice Department’s request ‘would be impossible to perform’ after it strengthened encryption methods.

I would like to see Apple refuse to sell iPhone in UK if gov’t bans end-to-end encryption. Does Parliament dare be that stupid?

- Jimmy Wales (@jimmy_wales) November 3, 2015

iPhones running iOS 8 or 9 have a feature that prevents anyone without a device’s passcode from accessing its data, including Apple itself.

The feature was adopted in 2014 amid heightened privacy concerns following leaks by former National Security Agency contractor Edward Snowden about NSA surveillance programs.

WHAT IS THE INVESTIGATORY POWERS BILL?
The Investigatory Powers Bill will be published in the House of Commons later today. It will be examined by MPS and Lords before a final vote next year.

The draft bill is designed to give the police and security services better access to online communications and bring different government surveillance powers under one law, Metro reported.

While Home Secretary Theresa May said it won't ban encryption, which is needed for online banking, for example, it could prevent end-to-end encryption, which means only a sender and recipient, but no-one else, can ever read a message.

The draft bill includes the requirement that internet firms store details of people's online activity for 12 months.

While they could not hand over details of a browsing history to security services if requested, they will be able to see which sites were visited and when.

David Cameron has pleaded that terrorists and criminals should not be allowed a 'safe space' online.

Ministers have no plans to ban all encryption services because they have an important role in the protection of legitimate online activity such as banking and personal data.

Earlier this week, the Home Secretary said the draft bill will not ban encryption per se.

Theresa May said this is because the process was vital to all modern communications such as online banking as well as some social media sites.

Apple is not the only handset manufacturer or service to use end-to-end encryption and if future UK surveillance laws did ban it, the move could mean Apple would either need to pull its smartphone from the UK or make it less secure.

Commenting on Wales' tweet, Forbes' Ian Morris wrote that Apple can 'happily manage without a dent in its profits.'

'Losing Europe would hurt, but the UK alone it could quite easily deal with.'

Apple has yet to respond to MailOnline's request for comment.

Even if the Investigatory Powers Bill, which seeks to pull together all new surveillance rules into a single law, does ban end-to-end encryption, a final vote on it will not take place until next year - so the iPhone will be sold in the UK for some time yet.

One of the most contentious parts of the draft bill is that it will require internet companies to store details of people's online activity for 12 months.

Pulina Whitaker, Data Protection Partner at Morgan Lewis said: 'The Government has proposed that the new Data Retention and Investigatory Powers Act (DRIPA) to be published in draft today, requires internet service providers to retain details about an individual's web browsing, not the specific pages they had viewed, for 12 months so the records are available on request by law enforcement.

'The Government considers that requests can be authorised by ministers rather than by judges alone.

'The perceived risk to privacy rights is that the content of the data - in addition to the website details - would, in fact, be accessible by law enforcement authorities.

'Europe is currently in the course of passing a new General Data Protection Regulation, which re-enforces the existing 'right to be forgotten' and to have personal data erased on request by the individual.

'DRIPA, if enacted in its intended form, is likely to be a source of tension for Internet service providers between compliance with data protection obligations and compliance with DRIPA.'

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

JOURNAL-CODE: WEBDM

Copyright 2015 Associated Newspapers Ltd.
Record of EVERY website you visit to be held for a year under new spying laws which also give spooks power to hack computers

BYLINE: MATT CHORLEY, POLITICAL EDITOR FOR MAILONLINE

SECTION: NEWS

LENGTH: 1085 words

Home Secretary Theresa May wants more powers for MI5, MI6 and GCHQ
Investigatory Powers Bill to prepare agencies to tackle crime in digital age
Web firms will keep record of all websites visited in previous 12 months
Spooks will need a warrant signed off by ministers to obtain the list
Panel of judges to have a veto over thousands of national security warrants

Details of every website visited will be stored for up to a year to be accessed by police and spooks under new spying laws unveiled today.

Home Secretary Theresa May argues that MI5, MI6, GCHQ and the police should be able to see which sites suspected terrorists and criminals have logged on to.

It forms part of the controversial Investigatory Powers Bill, which ministers claim is one of the most important pieces of legislation for the next five years.

Internet firms will have to keep records of website use for 12 months, detailing when emails were sent or when people connected to social media sites, such as Twitter, Facebook and WhatsApp.

With a warrant MI5, MI6, GCHQ and the police will able to find out details of the website a person has visited, but not which pages they have viewed within that site.

A further warrant would be required to view the content of any communications. However, councils will be barred from having any access to the internet records.

The draft bill will also force web giants to hand over the contents of encrypted apps and emails on production of a warrant.

The security services will also be able to hack into personal computers and monitor the contents while GCHQ will have the right to hoover up millions of pieces of people's personal data - including mobile phone numbers and internet searches.

A panel of judges will have a veto over ministers including Mrs May, Foreign Secretary Philip Hammond and Northern Ireland Secretary Theresa Villiers who last year authorised 2,700 spying operations.

In a significant concession to allay privacy concerns, the judges will review all of the thousands of national security warrants signed off every year.

The decisions by ministers to allow MI5, MI6 and GCHQ to tap phones or hack computers could be overturned by the judges.

Ministers have ruled out any proposal to restrict encryption or ban it, despite fears in the intelligence community that advanced online security measures risk leaving them locked out of some areas of cyber space.
A number of proposals from the abandoned 'Snooper's charter' have been ruled out, such as powers to demand UK-based communications service providers (CSPs) to capture and store internet traffic from companies based in the US.

In the Commons earlier David Cameron told MPs that communications data had been 'absolutely vital' in catching criminals including rapists and child abductors.

He said the power for intelligence agencies to see who criminals had contacted must continue.

David Cameron's official spokesman said: 'The Prime Minister underlined that this is about maintaining the agencies' current capabilities, that this is about - in a nutshell - the powers we need to keep us safe and about increasing public confidence in what they do in the process.'

Mr Cameron told ministers 'this would be one of the most important pieces of legislation during this parliament because it goes to the heart of the Government's duty to keep the British public safe'.

Officials claim the Bill will set 'new standards for openness and transparency', including 'world-leading oversight arrangements'.

But Whitehall insiders are braced for a ferocious fight with civil liberties groups, campaigning MPs and the House of Lords.

Labour's shadow home secretary Andy Burnham said there was a 'broad acceptance' that a new law was needed.

He told Sky News: 'The online world has created blind spots the authorities can't see any more. 'I'm not going to play politics with this issue,' he added.

WHAT THE NEW SNOOPING LAWS WILL ALLOW... AND WHAT IS NOT INCLUDED

The draft Investigatory Powers Bill is published today. Here are some of the key questions surrounding the legislation.

What is it?

New legislation drawn up in an attempt to bring the snooping powers available to police and intelligence agencies to tackle terrorism and serious crime in the digital age under one legal umbrella for the first time.

Why do we need a new Bill?

The current system is seen as an unwieldy patchwork of different powers covered by different laws. But there is also a logistical reason - the current laws expire at the end of 2016.

What powers will the Bill cover?

Current tactics such as access to communications data - the who, when and where but not the content, targeted interception of electronic communications, the collection of bulk data and the ability to mount IT attacks - known as equipment interference - will all be retained.

Will there be anything new in it?

A number of the Bill's proposals have trickled out. Firms will now be required to store data relating to people's web and social media use, but officials stressed internet connection records (ICRs) will not cover users' full browsing history or include the actual content of a communication. Councils, which can request communications data, will be banned from accessing ICRs. The Bill is expected to introduce a role for judges in the process for authorising the more intrusive capabilities, such as interception operations, while a new criminal offence will be created to prevent abuse by public authorities of communications data powers.

What is not in it?

Ministers have ruled out any attempt to ban encryption, despite concerns that it risks leaving authorities locked out of some areas of cyberspace. A number of proposals from the abandoned 'Snooper's charter' have been ruled out, such as powers to demand UK-based communications service providers (CSPs) to capture and store internet traffic from companies based in the US.

Will the Bill get through Parliament easily?

The Conservatives now have the majority they did not have when the Communications Data Bill was ditched in 2013, but the new laws are still likely to be controversial, with privacy campaigners, opposition MPs and backbenchers primed to examine its contents closely.
How long will it be before this set of laws is out of date?

The Regulation of Investigatory Powers Act, the central piece of legislation in this arena, was passed 15 years ago. Given the pace of technological change today, it is questionable whether the new Bill could last until 2030 without revision.

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

JOURNAL-CODE: WEBDM

Copyright 2015 Associated Newspapers Ltd.
All Rights Reserved

Return to List

45 of 104 DOCUMENTS

mirror.co.uk

November 4, 2015 Wednesday 5:53 PM GMT

7 reasons you should be worried about the Tory snooper's charter; Theresa May wants to make absolutely sure the police can get to your naked Snapchat pictures if they need to. Here's why the Investigatory Powers Bill is terrifying

BYLINE: By Mikey Smith

SECTION: NEWS, UK NEWS

LENGTH: 870 words

Theresa May is set to unveil the Investigatory Powers Bill - or as many have taken to calling it, the snooper's charter - this afternoon.

The Home Secretary says the measures in the bill are essential to keep the British people safe from terrorists, paedophiles and serious criminals.

Even David Cameron called it "one of the most important pieces of legislation" set to go on the books in this parliament.

But critics say the powers it would grant to government, police and security agencies licence them to invade the privacy of anyone in the country with little oversight to whether the snooping is justified.

Here's why you should be worried about the snooper's charter.

Under the new rules, every internet service provider and mobile phone network will be required to store a list of the websites you've visited and the messaging apps you've used, and when you've used them, for a year.

They won't be able to get the content of your messages without a warrant. An independent review of the plans recommended that these warrants should be approved by a judge, but it seems like Theresa May is set to ignore this advice and let ministers - or even mid-level police officers - decide if the more intrusive spying is justified.

snoop tweet
And to give you an idea of how much attention is paid to these warrants, the Home Secretary is currently asked to approve more than 1,400 requests a year.

That's very nearly 4 every day.

David Cameron has argued that the new powers are a natural update of powers the police have always had to look at the phone records of suspects.

But the internet isn't the same as making phone calls.

In 2015, we do almost everything online. We do our work online. We meet our friends online. We learn, read and watch TV online. We get medical advice, meet potential sexual partners and build relationships online.

The ability to follow your every movement online isn't like someone seeing who you've made phone calls to, it's like someone following you around 24 hours a day and checking the addresses on every letter you send.

Even Orwell's Telescreens didn't work in the dark...

Let's make one thing clear. The Investigatory Powers Bill is not just intended to stop terrorists, paedophiles and serious criminals, regardless of what David Cameron and Theresa May say.

As well as the police and security services, the very same powers will be available to local councils and the taxman.

The new bill replaces the Regulation of Investigatory Powers Act (RIPA), which was introduced in the last parliament in a climbdown from the original snooper's charter, which was vetoed by the Lib Dems.

And as with the old law, the powers in the new snooper's charter will be available to 38 public bodies, for the purposes of "detecting or preventing crime".

Your emails and browsing history will have to be held by internet companies for a year.

Not by the government, by the internet companies.

That'll be safe, right? Teenagers are hardly ever arrested on suspicion of hacking internet companies' data.

Incidentally, Theresa May came up with some fantastically circuitous logic for why this isn't anything to worry about.

On the BBC's Andrew Marr show on Sunday, she said the very fact that police will have access to the data will make it easier to catch anyone who steals it. Genius.

The Government wanted to include a ban on certain kinds of encryption in the bill - the kind of encryption used to keep messages sent using WhatsApp, Snapchat and iMessage private.

Over the weekend it was widely reported that the Government had 'climbed down' on this proposal - but they haven't, really.

They don't want to ban encryption outright, but they do want to ban so-called 'end to end' encryption - which can only be decoded by the sender and receiver. Not even Apple can read your iMessages, and the cops don't like that. They might not be bothered by your WhatsApp sexts or the d**k pics you send on SnapChat, but they want the option of demanding them unencrypted.

This won't just apply to messaging services, it'll also apply to banks, healthcare providers, employers. There are loads of people who want to communicate with privately, for perfectly legitimate reasons.

And the snooper's charter will ensure that those communications are vulnerable to hackers.

History shows us governments can't be trusted with this much power.

According to a report by Big Brother Watch, local councils committed data breaches, on average, four times a day over the last four years. That's council workers looking at people's private data illegally, for their own personal interest.

Or putting personal information on laptops and leaving them on trains.

Then there's the surveillance of journalists - often using the aforementioned "watered down" RIPA powers. The Metropolitan police, it was revealed in 2013, kept files on journalists - including details of sexual preferences, childhood and family medical history - who were simply doing their job.
The National Union of Journalists described the snooping as "outrageous".
And of course there's the case of the family of Stephen Lawrence, who had done nothing wrong, and who the police spied on and tried to smear in public in the wake of his death.
"Trust us," says Theresa May.

Snooper's Charter plans revealed: Government wants your to track your porn viewing, Facebook stalking and online shopping; Whether it's a casual text message or a personal image you've shared, it will ALL be stored for the government under new legislation brought in by Theresa May

BYLINE: By John Shammas
SECTION: NEWS, UK NEWS
LENGTH: 317 words

Everything you do online - from Facebook stalking to watching pornography, and even what you buy - will be stored by the government, if a new legislation is passed.

Home Secretary Theresa May is unveiling the new Investigatory Powers Bill today - commonly known as the Snooper's Charter.

It will demand that popular mobile phone or broadband providers store YOUR data for at least 12 months, with security bosses and police having permission to access that data without a warrant.

The legislation hopes to combine existing powers available to authorities under a single piece of law.

However while Prime Minister David Cameron described it as "one of the most important pieces of legislation" that Parliament will see over the next five years, it has come in for fierce criticism from civil liberties groups.

Shami Chakrabarti, director of Liberty, said: "If the authorities need a judge's warrant before they search my home, why not before the equal or greater intrusion of accessing my private communications?"

"This happens all over the free world including in the United States."
There are also concerns about how the legislation may risk your privacy, with corporations being ordered to store mass amounts of your personal data just weeks after high-profile hacks at websites such as adultery website Ashley Madison, or broadband provider TalkTalk.

Speaking to Sky News, Chris Phillips, the former head of the National Counter Terrorism Security Office, said: "The world has moved on so quickly: people communicate on many different means, whether it's WhatsApp, whether it's Facebook, whether it's email or telephone.

"So it's really important that the laws keep up. [Without new laws] we'd be in a very dangerous place."

The so-called Snooper's Charter was originally floated in 2012, but faced heavy opposition from Liberal Democrat ministers in the Coalition.

Ashley Madison: Why was cheating website hacked?

MI5 and GCHQ secretly bulk collecting British public's phone and email records for years, Theresa May reveals; First formal confirmation that there has been mass collection of phone and email records in the UK as Investigatory Powers Bill is published

BYLINE: By Tom Whitehead Security Editor

SECTION: NEWS

LENGTH: 937 words

MI5 and GCHQ have been secretly scooping up the telephone and email records of the British public for almost 15 years, the Home Secretary has revealed for the first time.

The revelation came as Theresa May unveiled a raft of new snooping measures in the Investigatory Power Bill, which includes forcing communication companies in law to help spy agencies snoop on suspects.

Other proposals will see the collection of the public’s web browsing history for up to a year and judges signing off warrants for intrusive surveillance.

The biggest overhaul of spying laws still face tough opposition but could now make it through parliament and in to law after Labour appeared to back the measures.
In a surprise development, Mrs May confirmed to MPs that she and her predecessors have quietly approved warrants for bulk collection of communication data in the UK since 2001.

The public avowal of the spy agencies’ tactic was described by the terrorism laws watchdog as a "significant and necessary" move.

It is the first formal confirmation that there has been mass collection of phone and email records in the UK, including those of innocent people.

The records are kept for no more than a year and more detailed examination of the content of calls or messages would only be allowed via a separate warrant.

∑ Theresa May: Internet data will be recorded under new spy laws

However, it was previously believed that bulk collection of data only referred to individuals based overseas.

The secret authorisations have been happening since 2001, in the wake of the 9/11 attacks on America and senior Whitehall sources insist the bulk collection is vital in the fight against terrorism and crime.

Publishing the bill, Mrs May said the bill will establish "world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world".

Shadow home secretary Andy Burnham said it was important to stress the proposals are "neither a snoopers’ charter nor a plan for mass surveillance".

"In a world where the threats we face internationally and domestically are growing, Parliament cannot sit on its hands and leave blind spots where the authorities can’t see," he added.

Under the bill internet and communication firms will also be forced in law to help spies hack in to phones and computers under new powers.

There will be a legal requirement on communication providers to assist MI5, GCHQ and the police to break in to suspects phones and computers.

That will include where the agencies want to remotely take control of devices and eavesdrop on suspects.

All police forces will also have the power to hack in to devices of suspects.

It came as police warned one in ten paedophiles are escaping capture because communication companies are not retaining web browsing histories.

A sample of more than 6,000 child abuse alerts revealed that in 14 per cent of the cases officers could not identify a suspect because officers could not access so-called internet connection records.

The proposed bill will require companies to now hold such data for up to a year at a cost to the public of £25 million a year.

The data relates to websites any many of the public connects to but not their full browsing history of each individual pages - meaning investigators could see if they used services such as Twitter or Snapchat but not the content of messages sent.

But a new safeguard where both the Home Secretary and a specially appointed judge will be required to sign off warrants to intercept data was criticised by all sides.

The "double lock" mechanism means any decision by a Secretary of State to allow intrusive surveillance will only be allowed to go ahead once a judge has approved it as well.

Former Northern Ireland secretary Owen Paterson was among a number of MPs who warned the move could delay and complicate important spying operations.

At the same time, Tory backbencher David Davis, who had called for judicial oversight, said the proposal would simply result in judges rubber stamping a politician's decision.

In another move to help ease the bill's passage, any request to spy on the communications of politicians will in future have to signed off personally by the Prime Minister.

A new offence will also be created for public authorities of "knowingly or recklessly obtaining communications data from a telecommunications operator without lawful authority".

It will carry a maximum penalty of two years in prison.
Independent reviewer of terrorism legislation David Anderson QC told the BBC: "This isn't a licence for the police to simply prowl over everything you have been doing but I quite accept that a lot of data is being kept by these service providers and under the Government's proposals it would be kept for a very long time.

"There are obvious risks attached to that. I simply wouldn't vote for this unless I had been very substantially satisfied that those risks had been minimised."

Writing for the Telegraph, Peter Wanless, chief executive of the children's charity, said combating the "vile trade" of child abuse took both time and perseverance.

"It is why despite the clanging furor, as the much debated investigatory powers bill comes into the Commons, the NSPCC will be supporting the retention of metadata for at least a year."

He said without the measures "there is a real danger that we might falter and tie the hands of those that are seeking to deliver essential convictions that visibly deter people from these crimes".

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDTNS

Copyright 2015 Telegraph Media Group Limited
All Rights Reserved

Return to List

48 of 104 DOCUMENTS

telegraph.co.uk

November 4, 2015 Wednesday 7:24 PM GMT

Theresa May, the new spy laws... and a warning for the public;
POLITICAL SKETCH: As spies are offered access to your internet records, a Tory MP says you shouldn't worry... as long as you've got 'nothing to hide'

BYLINE: By Michael Deacon Parliamentary Sketchwriter

SECTION: NEWS

LENGTH: 329 words

Last week saw the release of Spectre, the new James Bond film. It soared to the top of the box office chart, breaking the British record for opening-day ticket sales. By the weekend it had made £41m in the UK alone.

Now, mere days later, the Government has chosen to publish the contentious list of new powers it wants to give its spies. Yes, at exactly the same time as the public is thrilling to the sight of a heroic British spy saving us from cartoonish baddies.

Say what you like about this Government - they know how PR works.

The message today is very clear... If you have nothing to hide, you have nothing to fear! Richard Graham, Conservative MP for Gloucester
When Theresa May tried to secure new spying powers in the last parliament, she was denied by the Lib Dems, who dismissed her plans as a "snoopers' charter". This afternoon in the Commons, the Home Secretary stressed that her latest bill - which proposes to give spies access to the public's internet records - was different.

"A significant departure from the proposals of the past," she promised. "An approach that sets new standards for openness, transparency and oversight... Unparalleled openness and transparency about our investigatory powers..."

She was saying all this in her gentlest, most conciliatory tones. Anyone who has previously heard Mrs May speak will appreciate the effort this must have cost her. Normally she's as placatory as a pickaxe.

The effort seemed to pay off, though, because her statement received glowing praise from her opposite number in Labour, Andy Burnham.

"It's clear to me that both she and the Government have been listening carefully to the concerns expressed about the original legislation," he gushed. "I think it would be helpful if this House sent out a unified message today that this is neither a 'snoopers' charter' nor a plan for mass surveillance."

An intriguing judgment, given that he hadn't yet been able to read the bill he was applauding so heartily.

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDTNS

Copyright 2015 Telegraph Media Group Limited
All Rights Reserved

Return to List

49 of 104 DOCUMENTS

telegraph.co.uk

November 4, 2015 Wednesday 7:22 PM GMT

The politics of surveillance are about politics, not keeping us safe; Is Britain really going to become the first major democracy to log every website its citizens visit?

BYLINE: By Mike Harris

LENGTH: 869 words

Every piece of surveillance legislation proposed by government in the last generation has inevitably been "crucial" to stop terrorists, peadophiles and criminal masterminds who haunt the public consciousness. The new fear is that the internet is giving those with malicious intent a new tool to disrupt - or end - the lives of the law-abiding. So nearly every year we see another piece of draconian legislation aimed at taking control of the internet. In 2012, we had the draft Communications Data Bill (or Snooper's Charter), the most draconian piece of surveillance legislation ever proposed in a democracy. In the summer of 2014, the DRIPA Act was shoved through parliament in 48 hours. It was so illiberal our courts have ruled it breaches the law.

"We cannot rely on technology to solve complex human problems, we need human intelligence to fight crime"
Now, Theresa May strikes a different tone. May now believes in new safeguards to protect our privacy, including judicial authorisation of surveillance requests, a key demand of the "civil liberties lobby" who have gone from being maligned to praised in the House of Commons. Oversight of our intelligence agencies - woefully lacking in the past - will be improved with a strengthened commissioner. Yet, as ever, the devil will be in the detail of this legislation. The government still hasn't weaned itself off collecting our most private data, it's this battle that will determine how we remember this Bill.

The Government wants to enhance the bulk collection and interception of data to keep us safe. The truth is that terrorists have known for some time that the internet is a bad way to communicate. Bin Laden's compound had no internet connection, he wrote his emails in advance and his associates used internet cafes to send them. The killer of Lee Rigby, Michael Adebowale, was highly security-conscious - as a parliamentary report put it "MI5 noted that Adebolajo was a "difficult [suspect] to investigate due to his security-consciousness". He would use pay phones rather than smart phones and barely use electronic communications. The fact is, criminals are already on the Dark Net using highly encrypted communications tools far beyond the reach of our government and police, as brilliantly described by Jamie Bartlett. These tools are also used by dissidents in authoritarian states to hide from the state and protect their free speech and their lives. The Investigatory Powers Bill can't stop this. The technology is too complex, evolving too quickly, and is distributed among a network of internet activists who will do anything to protect human rights activists working in dangerous places.

Politicians don't understand this. They just don't get that legions of coders are building technologies to make private communications easier and cheaper. So the parliamentary debate felt like shadow boxing. MPs all agreed new powers were needed, but none understood that the powers they will be signing into law will not be particularly effective in tracking terrorists, but will be good at capturing the data of law-abiding citizens. So every Briton's internet history will be logged to prevent crime, but crime bosses and terrorists using the Dark Net can't be traced. The real concern is that this data, alongside the bulk retention of data, will not be used to prosecute serious crimes, but petty misdemeanors. Protesters in breach of the peace, whistleblowers breaking the Official Secrets Act or school catchment area cheats. The police will have the data to drag up minor crimes 12 months ago to prosecute people they wish to lock away. Go ahead, you may say, but as we saw with the outrageous use of the previous RIPA Act by local councils to prosecute people for low level nuisance, the potential for abuse is huge.

Campaign groups like Don't Spy On Us called for comprehensive legislation to reform the law, wanted judicial authorisation for surveillance requests, improved oversight, and no return for the "Snooper's Charter". Having won all these concessions, it would be churlish to say the least, to not thank the Home Secretary for listening. There's some good in this Bill - in particular the double-lock to ensure democratically elected politicians and our independent judiciary sign off on all surveillance warrants.

Yet, big questions remain. Is the bulk collection of data lawful, will it be effective and does it offer value for money at a time of police cuts? Is Britain really going to become the first major democracy to log every website its citizens visit? Is this legislation going to enable the mass intercept of all our communications and allow the hacking of our personal devices? Parliament said little on this today, and the response from the Labour frontbench was woeful. We cannot rely on technology to solve complex human problems, we need human intelligence to fight crime. In the choice between police and intelligence officers and the bloated surveillance technology pushed by US corporates, the choice should be clear. The best safeguard of our liberty is eternal vigilance, the same is true for our security.

Mike Harris is CEO of 89up and advises the Don't Spy On Us campaign
Theresa May outlines key measures in Investigatory Powers Bill; The Home Secretary has announced new powers for police and security services in tracking the public’s internet use

BYLINE: By Claire Lomas

LENGTH: 572 words

Communications firms will be legally required to help spies hack into suspects’ smartphones and computers under a new ‘snooping law’ unveiled today.

Home Secretary Theresa May has revealed that domestic providers will be obliged to assist authorities in “giving effect to equipment interference” under the draft Investigatory Powers Bill.

She argued that the bill will establish “world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world”.

The Investigatory Powers Bill allows agencies to interfere with electronic equipment in order to obtain data such as communication from a device.

It can involve remote access to computers to covertly download the contents of a mobile phone during a search.

This is not a new power and a number of firms already assist in the activities voluntarily, officials said, but they will now be legally obliged to provide assistance in future.

Privacy campaigners see the new requirement as a major extension of surveillance powers. However, Mrs May has insisted that security services will not be allowed to access web users' full browsing histories under the new powers.

She said it was "simply wrong" to suggest that new powers in the draft Investigatory Powers Bill to access "internet connection records" would allow the collection of someone’s full web history.

The Home Secretary explained it would allow the likes of the police and GCHQ to know if someone has visited a social media website like Facebook - but not which pages they looked at, who they communicated with, or what they said.

She said the publication of the bill is a "decisive moment":

"Never before has so much information been in the public domain about the activities of our police and security services, as well as the oversight, safeguard and authorisation arrangements which govern them.

"I am clear we need to update our legislation to ensure it is modern, fit for purpose and can respond to emerging threats as technology advances.

Communications firms will be legally required to help spies hack into suspects' smartphones and computers under a new 'snooping law' unveiled today.

Home Secretary Theresa May has revealed that domestic providers will be obliged to assist authorities in "giving effect to equipment interference" under the draft Investigatory Powers Bill.

She argued that the bill will establish "world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world".

The Investigatory Powers Bill allows agencies to interfere with electronic equipment in order to obtain data such as communication from a device.

It can involve remote access to computers to covertly download the contents of a mobile phone during a search.

This is not a new power and a number of firms already assist in the activities voluntarily, officials said, but they will now be legally obliged to provide assistance in future.

Privacy campaigners see the new requirement as a major extension of surveillance powers. However, Mrs May has insisted that security services will not be allowed to access web users' full browsing histories under the new powers.

She said it was "simply wrong" to suggest that new powers in the draft Investigatory Powers Bill to access "internet connection records" would allow the collection of someone’s full web history.

The Home Secretary explained it would allow the likes of the police and GCHQ to know if someone has visited a social media website like Facebook - but not which pages they looked at, who they communicated with, or what they said.

She said the publication of the bill is a "decisive moment":

"Never before has so much information been in the public domain about the activities of our police and security services, as well as the oversight, safeguard and authorisation arrangements which govern them.

"I am clear we need to update our legislation to ensure it is modern, fit for purpose and can respond to emerging threats as technology advances.

"Theresa May outlines key measures in Investigatory Powers Bill; The Home Secretary has announced new powers for police and security services in tracking the public's internet use"
“There should be no area of cyberspace which is a haven for those who seek to harm us to plot, poison minds and peddle hatred under the radar.

“But I am also clear that the exercise and scope of investigatory powers should be clearly set out and subject to stringent safeguards and robust oversight.”

**LOAD-DATE:** November 4, 2015

**LANGUAGE:** ENGLISH

**PUBLICATION-TYPE:** Newspaper; Web Publication

**JOURNAL-CODE:** WEBDTNS

Copyright 2015 Telegraph Media Group Limited
All Rights Reserved

---

**Surveillance laws revamp has faced a rocky road;**
**The Investigatory Powers Bill, to be published on Wednesday, has been seven years in the making**

**BYLINE:** By Tom Whitehead Security Editor

**SECTION:** NEWS

**LENGTH:** 388 words

The revamp of Britain’s spy laws and capabilities has endured a long and rocky road spanning three Governments.

Concerns from the spy agencies and police that their coverage of suspects online was deteriorating first came to the fore under the last Labour Government in 2008.

It was argued that modern communications were across many platforms which outdated regulations did not cover and data was not being retained.

Initial moves to address the gaps first emerged in Whitehall as the Interception Modernisation Programme.

It sparked immediate outrage as it was to involve the storage of every phone call, email and website visit on a huge national database.

It was quickly nicknamed the "snooper’s charter" and by 2009, the then Home Secretary Jacqui Smith indicated there would be no database but instead a compulsion on service providers to store their customer data.

The proposals face fierce opposition and did not make it in to draft legislation under the Gordon Brown Government.

The issue was revived under the Conservative and Liberal Democrat coalition government which took power in 2010 again with the intention that the internet companies themselves would retain the data.

Theresa May, the Home Secretary, had hoped to introduce the measures in a Draft Communications Bill during the 2012/13 parliamentary session, with the powers being enacted by 2014.
However, Lib Dem leader and then deputy prime minister Nick Clegg withdrew his support of the measures and his party blocked all attempts to bring the proposals forward during the 2010/15 parliament.

The revelations of spying techniques by former CIA contractor Edward Snowden in 2013 and claims of mass surveillance intensified that opposition.

Following the Conservative victory in the 2015 General Election, Mrs May vowed to bring the measures forward again but only after a major review of surveillance capabilities and safeguards by the independent reviewer of terrorism legislation, David Anderson QC.

His comprehensive 370-page report heavily influenced Government thinking and the Investigatory Powers Bill to be unveiled on Wednesday is not much broader than just the snooper's charter but an overhaul of all laws and regulations surrounding surveillance.

Whether the measures fare any better in the face of already growing opposition remains to be seen.

RIPA: Protecting children from paedophiles trumps your privacy; Theresa May's new Investigatory Powers bill, condemned by some as a 'Snooper's Charter', is essential to stop vile images being traded online

BYLINE: By Peter Wanless chief executive NSPCC

LENGTH: 540 words

Every year there are hundreds of thousands of sickening images of children uploaded onto the canvas that is the internet and every year there are thousands of people that seek out these crime scenes for a perverse pleasure that few can understand. In 2012 alone, 50,000 members of the British public accessed indecent images of children.

Combating this vile trade takes both time and perseverance, and it is why, despite the clanging furor, as the much debated investigatory powers bill comes into the Commons, the NSPCC will be supporting the retention of metadata for at least a year. Used appropriately and effectively, access to this information helps crucially with the detection, prosecution and conviction of these crimes.

"Let's also hear the voices of thousands of children placed in jeopardy, while the trade in abusive images continues to flourish"

We have heard plenty from groups extolling privacy principles and spies unveiling foiled terrorist threats, but let's also hear the voices of thousands of children placed in jeopardy while the trade in abusive images continues to flourish.
Time and again society has expressed horror at the cases that have to come to light where stashes of images of children, being abused, raped and molested are traded online. Many have spoken of the need to eradicate these crimes. We have placed pressure on search engines and internet service providers to tackle the accessibility and proliferation of these images head on and we have harangued the police when reports are issued that say their response to this crime is inadequate.

We have welcomed the government making child sexual abuse and exploitation a national priority. And yet, there is a real danger that we might falter and tie the hands of those that are seeking to deliver essential convictions that visibly deter people from these crimes. There are difficult choices that have to be made in finalising the detail but what have I have highlighted is a real tangible example of why an investigatory powers bill is a part of enabling the police, and others to combat child abuse.

A precedent which clearly illustrates this can be found in Germany where the inability to store metadata severely hampers their ability to combat paedophile rings. Crimes that only occur online force us to look for new types of evidence, and access to metadata offers us a fingerprint that can help us trace those that perpetrate these crimes.

"Fears that stored data could fall into the hands of those with unscrupulous intent must also be met head on"

Naturally, access to retained data should be controlled. And fears that stored data could fall into the hands of those with unscrupulous intent must also be met head on. There needs to be oversight and that oversight needs to be robust; but exercised with sufficient pace to allow the police to act decisively against child abusers.

Nevertheless, in working through this detail, we should all never lose sight of the fact that there are real crimes that we are attempting to foil, real children that we are trying to protect and real expectations that the nation wants delivered upon. We should not hamper those that serve to protect us by restricting them to an analogue approach in a digital age.

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDTNS

The Daily Telegraph (London)

November 5, 2015 Thursday
Edition 3;
National Edition

MPs with nothing to hide rally round May's new surveillance plan; Sketch

BYLINE: Michael Deacon

SECTION: NEWS; OPINION; COLUMNS; Pg. 10

LENGTH: 446 words
LAST week saw the release of Spectre, the new James Bond film. It shot straight to the top of the box office chart, breaking the British record for opening-day ticket sales. By the weekend it had made £41 million in this country alone.

Now, mere days later, the Government has chosen to publish the contentious list of new powers it wants to give its spies. Yes, at exactly the same time as the public is thrilling to the sight of a heroic British spy saving us from cartoonish baddies. Say what you like about this Government - they know how PR works.

When Theresa May tried to secure new spying powers in the last parliament, she was denied by the Liberal Democrats, who dismissed her plans as a "snoopers' charter". Yesterday in the Commons, the Home Secretary stressed that her latest Bill was different.

"A significant departure from the proposals of the past," she promised. "An approach that sets new standards for openness, transparency and oversight." She was saying all this in her gentlest, most conciliatory tones.

Anyone who has previously heard Mrs May speak will appreciate the effort this must have cost her. Normally she's as placatory as a pickaxe. The effort seemed to pay off, though, because her statement received glowing praise from her opposite number in Labour, Andy Burnham.

"It's clear to me that both she and the Government have been listening carefully to the concerns expressed about the original legislation," he gushed. "I think it would be helpful if this House sent out a unified message that this is neither a 'snoopers' charter' nor a plan for mass surveillance." An intriguing judgment, given that he hadn't yet been able to read the Bill he was applauding so heartily.

Numerous other MPs welcomed Mrs May's statement - she even won cautious praise from Nick Clegg. Many Tories were thumpingly keen. One enthusiast, Richard Graham (Con, Gloucester), said the message was: "If you have nothing to hide, you have nothing to fear!" This was rather a striking line to use, given that it's commonly attributed to Goebbels.

None the less, the press will be delighted that Mr Graham takes such a view. After all, the Government is apparently considering ways to water down the Freedom of Information Act, which gives journalists and the public access to documents that politicians might rather they didn't see.

Only last week, Chris Grayling, the Tory Leader of the House, said it was "not acceptable" for journalists to use the act as a "research tool".

It is excellent news that Mr Graham will be holding his Government to account on this matter. As he will no doubt be happy to tell David Cameron: "If we MPs have nothing to hide, we have nothing to fear!"

LOAD-DATE: November 5, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: DTL

Copyright 2015 Telegraph Media Group Limited
All Rights Reserved

Return to List

54 of 104 DOCUMENTS

The Guardian

November 5, 2015 Thursday 12:32 PM GMT

Theresa May's investigatory powers bill is a step in the right direction;
The introduction of judicial oversight to surveillance laws should help restore the proper balance of privacy and security - and the trust of all communities

BYLINE: Keir Starmer

SECTION: COMMENT IS FREE

LENGTH: 758 words

In a democracy there will always be a tension between security and privacy. Most people want the police and the security services to have the necessary powers to be able to deal effectively with serious crimes including murder, child sexual exploitation, terrorism and locating missing people. But equally, most people are very uncomfortable with the idea that the state should be able to access the records of every website they have ever visited. Getting the balance right matters for security, for privacy and for democracy.

Related: The surveillance bill is as big a threat to state security as to personal liberty | Simon Jenkins

The current surveillance framework is set in legislation passed in 2000. In the intervening 15 years, so much has changed. The landline and basic mobile phones have been replaced with any number of sophisticated devices and apps. Although it hardly seems possible, Facebook was only launched in 2004 and Twitter came two years later in 2006.

As a result, the case for reform is overwhelming. There should be no gaps in the ability of the police and security services when dealing with serious crime; no safe places where those intent on harming others can go about their business undisturbed. But just as the case for reform gets stronger, so does the case for effective safeguards. Extensions of surveillance can only be justified if accompanied by much improved transparency and ever more robust oversight and scrutiny.

Yesterday Theresa May, the home secretary, unveiled the government's plans for reform by publishing a draft investigatory powers bill. Weighing in at 296 pages, the devil will obviously be in the detail.

But we do know that there is a welcome "double lock" in the bill. This means that authorisation of the most intrusive investigatory powers, whereby intercept warrants are issued by the secretary of state, will not come into force until formally approved by a judge.

Judicial oversight adds a level of independent scrutiny previously lacking. Thousands of interception warrants are granted every year: more than 2,700 applications for warrants were considered and signed off last year by the home secretary, foreign secretary and Northern Ireland secretary. The sheer volume means that while the relevant secretary of state will consider each application, in reality a great deal of the preparatory work is routinely done by support staff. Although that arrangement may have worked well in the past, without judicial oversight it is not appropriate for the future.

The proposed involvement of judges will not reduce accountability as some have claimed. As the independent reviewer of terrorism, David Anderson QC, put it in his report to the home secretary, published in June this year: "The secretary of state is in practice rarely, if ever, held politically accountable for the issue of warrants." Legislation prevents unauthorised disclosure of any detail about individual warrants, and intercepted material is not admissible in court. As far as I have been able to research, there has never been an occasion on which any secretary of state has ever been held politically accountable for the issue of individual warrants.

But the case for judicial involvement does not end there. As surveillance powers are extended, the trust of all our communities in their exercise becomes increasingly important. In the aftermath of terrorist atrocities the inevitable calls from politicians for certain communities to take more responsibility for the actions of those assumed to be among their number who may have had an involvement can cause real damage to our social cohesion. Requiring decisions by politicians to be approved by judges in the most sensitive cases should help to restore trust in the system as a whole.

Clearly the draft investigatory powers bill now needs to be closely scrutinised before it begins its journey through both houses of parliament. Hard questions should focus on the test to be applied by judges before formally approving an intercept warrant; real judicial scrutiny is a safeguard, a judicial rubber stamp is not. And the detailed provisions for the retention and use of internet-connection records, which considerably extend the surveillance reach of the state, need careful attention: what
are the limits on retention, and how closely defined and controlled will access to this material really be?

It will be for the government to answer these questions: but the bill is a step in the right direction.

LOAD-DATE: November 5, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

May internet plan is an 'attack on privacy'; SECURITY

BYLINE: Nigel Morris DEPUTY POLITICAL EDITOR

SECTION: NEWS; Pg. 8

LENGTH: 382 words

Theresa May was accused of overseeing a "breathtaking attack" on privacy as she set out plans to give the police and security services the power to access records of every Briton's use of the internet without requiring a warrant.

The Home Secretary won praise from political rivals for abandoning elements of the "snooper's charter", which was blocked during the Coalition government, and for giving judges a key role in approving surveillance exercises.

But she came under fire from civil liberties groups over moves to force communications companies to hold data about internet use for up to 12 months and to require them to help spies to hack into suspects' smartphones and computers.

Critics raised fears that the bulk collection could leave huge tranches of personal information vulnerable to attacks similar to the hacking last week of TalkTalk's database.

The draft Investigatory Powers Bill will overhaul the existing legislation governing surveillance, putting all hacking and bugging by the state on a statutory basis.

The move reflects widespread agreement that current laws are outdated because of technological advances. It is also a response to pressure for the government to be more transparent about surveillance techniques following Edward Snowden's revelations about mass "data-mining" exercises conducted by GCHQ.

Ms May told the Commons the proposed Bill would provide some of the "strongest protections and safeguards anywhere in the democratic world".

She said: "There should be no area of cyberspace which is a haven for those who seek to harm us, to plot, poison minds and peddle hatred under the radar."
The measures were backed by the shadow home secretary Andy Burnham, potentially putting him at odds with Jeremy Corbyn. He agreed that the proposed Bill was not "a plan for mass surveillance".

Nick Clegg, who as Liberal Democrat leader blocked the snooper’s charter, said the revised proposals were much improved, but warned: "I have a feeling that under the bonnet it still retains some of the flaws of its predecessor."

Liberty said the Bill gave extensive new powers to the authorities to track and hack private information with few privacy safeguards. It said the promise of judicial approval of surveillance warrants would in practice amount to a "rubberstamping exercise".

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: III

The Government's Investigatory Powers Bill, outlined yesterday by the Home Secretary, has been dubbed a "snooper's charter" by critics. It may, in fact, offer a licence to security agencies and to criminals that we come to regret.

Existing legislation is less than satisfactory, either because it has been abused by the authorities - as in the case of the Regulation of Investigatory Powers Act - or because it is out of step with modern technology. It is perfectly reasonable that the Government should want to initiate a thorough overhaul.

Yet there is a paradox in the approach taken by Theresa May and her officials. We are told that the authorities need to stay one step ahead of terrorists and criminal minds, and that they cannot do so unless underlying legislation is responsive to the reality of today's internet world. But it is precisely that reality - of hacking and data breaches - which will cause many people to be anxious about the mass retention of their data by communications companies.

The failure by TalkTalk to keep its customer data secure brought home just how vulnerable big corporations are to hackers. While civil liberties campaigners focus on the invidious potential for the state to examine our private internet browsing history, for ordinary people the greater worry may be the ability (or otherwise) of commercial giants to hang on to data securely for the year demanded by the Government.

That's not to say that the fundamental anxiety about state snooping should be underplayed. Nor should we be fooled by the notion that the new proposals amount to a vastly watered-down version of
the plans Ms May sought to bring forward during the last parliament and which were stymied by the Liberal Democrats. This time, the Lib Dems are thwarted themselves by lack of numbers and appear to have acquiesced in the Government's plans. Likewise, Labour has swung behind the measures: the shadow Home Secretary, Andy Burnham, says the Bill is "neither a snooper's charter nor a plan for mass surveillance".

Such a lack of political opposition is surprising, and it may be left to the Lords once again to raise some sage eyebrows. After all, whatever safeguards are in place, the idea that every citizen of the UK will now have their internet browsing history kept on file for a year by their broadband provider, for perusal by security agencies should the need arise, is surely staggering.

As always, there will be those who contend that people who do no wrong have nothing to fear. That is facile, and, in any case, the authorities are hardly infallible.

Ms May urges us not to worry: for the most part, we're told, the police won't be able to access our full browsing history, just the basics about which sites we visit - the "modern equivalent of an itemised phone bill". Except that it isn't. Once again the Government demonstrates that, in endeavouring to bring difficult legislation up to date, it has little real comprehension of how fundamental the internet has become to most people's lives. To proclaim it simply the telephone of the 21st century is either obtuse or a deliberate attempt to mislead.

None of this should be taken as a lack of support for Britain's security services. They do a difficult job and, on occasion, will require controlled access to the communications data of suspects. But let's not pretend that the Government's Bill does not have the potential to impact on our civil liberties in fundamental ways.

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: IA

Copyright 2015 Independent Print Ltd
All Rights Reserved

Return to List

57 of 104 DOCUMENTS

The Independent (London)

November 5, 2015 Thursday
First Edition

May is accused of 'breathtaking attack' on privacy in new surveillance measures

BYLINE: NIGEL MORRIS DEPUTY POLITICAL EDITOR

SECTION: NEWS; Pg. 8

LENGTH: 745 words

Theresa May was accused of overseeing a "breathtaking attack" on privacy as she set out plans to give the police and security services the power to access records of every Briton's use of the internet without requiring a warrant.
The Home Secretary won praise from political rivals for abandoning elements of the "snooper's charter", which was blocked during the Coalition Government, and for giving judges a key role in approving surveillance exercises.

But she came under fire from civil liberties groups over moves to force communications companies to hold data about internet use for up to 12 months and to require them to help spies to hack into suspects' smartphones and computers. Critics raised fears that the bulk collection could leave huge tranches of personal information vulnerable to attacks similar to the hacking last week of TalkTalk's customer database.

The draft Investigatory Powers Bill will overhaul the existing legislation, putting all hacking and bugging by the state on a statutory basis. The move reflects widespread agreement that current laws are outdated because of technological advances. It is also a response to pressure for the Government to be more transparent about surveillance after Edward Snowden's revelations about mass "data-mining" exercises by GCHQ.

Ms May told the Commons the proposed Bill would provide some of the "strongest protections and safeguards anywhere in the democratic world". She said: "There should be no area of cyberspace which is a haven for those who seek to harm us, to plot, poison minds and peddle hatred under the radar."

The measures were backed by the shadow Home Secretary Andy Burnham, potentially putting him at odds with Jeremy Corbyn. He agreed the proposed Bill was not "a plan for mass surveillance".

Nick Clegg, who as Liberal Democrat leader blocked the snooper's charter, said the revised proposals were much improved, but warned: "I have a feeling that under the bonnet it still retains some of the flaws of its predecessor."

Ms May announced a new "double lock" approval system under which agencies are allowed to see the content of communications or bug telephone calls. Initial approval would be given by a Cabinet minister - usually the Home Secretary - but have to be approved by a "judicial commissioner", a security-cleared senior judge. The only exception would be in operations deemed urgent because lives could be put at risk without rapid action. Web and phone companies would retain "internet connection records", listing websites visited but not every page visited, for a year.

The security services, police and other public bodies - but not local councils - would be allowed to examine the information on the authority of a senior officer. There would be no need for ministerial or judicial approval.

The companies would also be legally required to assist the authorities in "giving effect to equipment interference", such as hacking operations to download the contents of a mobile phone's memory. All police forces will be permitted to use the tactic under the new regime, with a code of practice to regulate the "more sensitive and intrusive techniques".

Liberty said the Bill gave extensive new powers to the authorities to track and hack private information with few privacy safeguards. It said the promise of judicial approval of surveillance warrants would in practice amount to a "rubber-stamping exercise". Its director, Shami Chakrabarti, said: "This long-awaited Bill constitutes a breathtaking attack on the internet security of every man, woman and child in our country. We must now look to Parliament to step in where ministers have failed, and strike a better balance between privacy and surveillance."

Anne Jellemma, chief executive officer of the Web Foundation, said: "The Bill seeks to introduce mass surveillance of every Briton's internet connection records without warrants, something which should be unthinkable in a modern democracy."

She said the requirement for firms to store records of every citizen's computer use was "deeply misguided and is neither necessary nor proportionate. It will hurt UK businesses, create new vulnerabilities for criminals to attack, and ride roughshod over the right to privacy."

The Green MP Caroline Lucas said: "The cosy consensus on surveillance that appears to have taken hold in Westminster is troubling. Many of the aspects of this Bill need far more scrutiny."

Number of months companies would hold data about personal internet use

LOAD-DATE: November 4, 2015

LANGUAGE: ENGLISH
Spooks have been harvesting our phone and email data for 14 years: Now MI5 and police get new power to snoop as terror bill leaves no hiding place online

BYLINE: JAMES SLACK POLITICAL EDITOR FOR THE DAILY MAIL

SECTION: NEWS

LENGTH: 2569 words

Home secretary Theresa May's admission came during statement to MPs
She said it had helped MI5 to foil a string of terrorist plots since 2001
The statement came during the unveiling of new Investigatory Powers Bill
It grants the police and security services extensive surveillance powers

Security officials have been secretly harvesting and storing the phone and email records of millions of UK citizens for the past 14 years, it emerged last night.

Theresa May revealed that the bulk collection of communications data had been authorised by every Home Secretary since 2001 and had helped MI5 to foil a string of terrorist plots.

Her admission came in a statement to MPs during the unveiling of the controversial new Investigatory Powers Bill, which will grant the police and security services extensive surveillance powers.

They include a legal requirement on communications firms to help spies hack into suspects' smartphones and computers. Bulk data gathering powers will be extended to include basic internet records. The likes of BT, TalkTalk and Sky will be obliged to assist with warrants designed to unlock an electronic device, or implant software allowing the contents to be read remotely.

The basic power to interfere with computer equipment applies to all 43 police forces in England and Wales.

Security services MI5 and MI6, the GCHQ spy base at Cheltenham and a limited number of police forces will be able to switch on cameras and microphones for more intrusive spying missions once they obtain a warrant.

The Bill, which has been heavily trailed in recent days, will also:

- Force internet firms to store internet records for 12 months
- Allow police and spies to access this data without a judicial warrant
Introduce a new ‘double lock’ system requiring judges to approve the most intrusive surveillance

Set out new protections intended to stop police accessing journalists’ call records in order to identify their sources. Police forces must get the approval of a judicial commissioner before accessing the communications data of a journalist in order to identify a source.

Land the public with a bill of £245million over ten years for implementing the new regime

Q&A: THE QUESTIONS RAISED BY THE DRAFT INVESTIGATORY POWERS BILL

Political Editor JAMES SLACK examines the questions raised by the 182-page draft Investigatory Powers Bill

What can police and security services do at the moment?

With the approval of a senior official or police officer, they can obtain basic communications data - such as who you called, texted or emailed, the time of day and your location. Some 500,000 requests were made last year. If the police, MI5, MI6 or GCHQ want to access the content of an email or listen to the calls, they need a separate warrant from a Secretary of State.

What is changing?

The most significant new power is a requirement for internet firms to store details of every person’s website visits for 12 months. Police and security officials will be able to access this without a judicial warrant. It will include the main address of the website but not the details of the individual pages which were looked at. The Home Office gives the example of the BBC website. Police and spies would know you visited www.bbc.co.uk, but not the specific stories you go on to read. On apps, they would be allowed to see if someone used Snapchat at 9am on their smartphone at home, but not the text typed into it.

What is the point of keeping so much information?

Police and security officials say people increasingly communicate online, using the likes of Skype, Facebook or WhatsApp, rather than by text or email. More than 19 billion online messages were sent in 2012 alone. If the law enforcement agencies are unable to work out who is talking to who online, it creates blind spots which terrorists and criminals can readily exploit.

Should I be worried?

The Government insists not, as safeguards will ensure internet records can only be accessed in relation to serious crimes, such as child abduction and terrorism. Town halls will not be allowed to benefit from the new powers.

However, civil liberties campaigners say the powers amount to a massive and unwarranted extension of state surveillance. The cyber-attack on TalkTalk has also exposed the danger of any data stored by internet firms falling into criminal hands. For instance, a list of a person’s web visits might expose use of pornography, making them a target for blackmail.

Will I still be able to send encrypted phone messages?

Yes. The Bill stops short of outlawing encryption, which is used widely for the likes of online banking. Instead, companies must provide the data when a warrant is issued. The company would decode the message itself before handing it to police or security officials. It is unclear what will happen if companies based overseas - such as Apple (iMessage) and WhatsApp - refuse to cooperate.

What is bulk data collection and how am I affected?

Bulk data collection is when the security services hoover up and store the details of millions of communications records - the who, where and when of a text, phone call or email. Intelligence officials then trawl through looking for patterns which might identify terrorist networks.

Controversially, the data of millions of entirely innocent people is inevitably scooped up. Previously, it was believed British agents had only been targeting communications sent via overseas. However, Theresa May revealed yesterday that, for the past 14 years, the bulk data of British citizens had been stored, too.

She insists this was perfectly legal under the 1984 Telecommunications Act - but most MPs and the public were kept entirely in the dark. The data is stored for 12 months then destroyed. MI5 argues it has played a major role in all recent major operations - saving countless lives. The new law will allow this tactic to continue.
The most surprising revelation, however, was the secret collection of so-called bulk data by the British intelligence agencies.

The details, which were stored for 12 months, were phone and other communications data - such as who a person called or texted, where from and at what time.

It did not include the content but, according to security officials, the programme allowed MI5 to foil at least one major plot by uncovering the links between members of a terrorist network.

Parliament cannot sit on its hands and leave blind spots where the authorities can't see

Mrs May told MPs that the plot was an attempt in 2010 by Islamist fanatics to launch a firearms attack on the London Stock Exchange and other targets.

Whitehall sources insisted the top secret programme was legal under the Telecommunications Act 1984, even though this legislation predates the widespread use of the internet or mobile phones.

They also insisted the programme had been approved by every Home Secretary since 2001 - the year of the 9/11 attacks on the World Trade Centre in New York and the Pentagon. MPs on Parliament's intelligence and security committee were also made aware, though other MPs and the public were kept entirely in the dark.

Previously, it had been disclosed - in the wake of the revelations by the fugitive US whistleblower and ex-spy Edward Snowden - that British involvement in bulk data collection related only to individuals based overseas.

It will now continue under the new legislation. The Government, which has a majority of only 12, faces a fierce battle to get the Bill on the Statute books.

It is opposed by civil liberties groups and some Tory and Liberal Democrat MPs.

But, in a boost to Mrs May, Labour yesterday appeared to back the proposals.

Shadow Home Secretary Andy Burnham said it was important to stress the proposals are 'neither a snoopers' charter nor a plan for mass surveillance'.

Mr Burnham added: 'In a world where the threats we face internationally and domestically are growing, Parliament cannot sit on its hands and leave blind spots where the authorities can't see.'

TAP ON CALLS FOILED BOMB PLOT

Four Muslim fanatics were foiled after MI5 spies snooped on their phone calls as they plotted to launch a Mumbai-style bombing and shooting attack on London.

The Al Qaeda-inspired gang intended to unleash a Christmas campaign of atrocities with high-profile targets that included the Stock Exchange, Big Ben and Westminster Abbey.

But they were arrested four days before they planned to plant their first bomb in December 2010.

Yesterday Home Secretary Theresa May revealed for the first time that analysis of mass communications data by MI5 was crucial to smashing the plot.

When officers searched the homes of the suspects, they found evidence of their violent Islamist beliefs and a handwritten list of targets including London Mayor Boris Johnson, the Dean of St Paul's Cathedral, two rabbis and the US Embassy. The plotters, inspired by terrorist firebrand Anwar Al Awlaki, planned to send bombs in the post to London synagogues.

Police listened to them discussing replicating the carnage of the 2008 Mumbai massacre, which claimed 173 lives, after bugging their homes and cars. In 2012 the four ringleaders and five accomplices were jailed for terms of up to 18 and a half years.

Aides to party leader Jeremy Corbyn will now be anxiously waiting to see if there is a backlash on Twitter from his Left-wing followers, with whom state surveillance powers are deeply unpopular. Some Labour MPs are also unhappy.

Mrs May said: 'There should be no area of cyberspace which is a haven for those who seek to harm us to plot, poison minds and peddle hatred under the radar.'

She argued that the new regime will establish 'world-leading oversight to govern an investigatory powers regime which is more open and transparent than anywhere else in the world'.

But Labour home affairs select committee chairman Keith Vaz said he was worried that the internet records powers may allow more data to be collected than Mrs May was implying.
'I know you said the information is equivalent to an itemised bill but there's a lot of information in an itemised bill,' he said.

'If I were to look at your itemised telephone bill and you were to look at mine we might be surprised at who we were telephoning.'

There are also concerns, in the wake of the massive recent cyber-attack on TalkTalk, that the public's internet records could be stolen by blackmailers.

Liberty director Shami Chakrabarti said: 'After all the talk of climb-downs and safeguards, this long-awaited Bill constitutes a breathtaking attack on the internet security of every man, woman and child in our country.'

Home Office officials said there would be new protections on journalists sources and phone records, which can be accessed only with the approval of a judge.

Conservative MP Richard Graham was criticised on social media yesterday for using a quote attributed to Nazi propaganda minister Joseph Goebbels while defending the Bill. He said that 'if you have nothing to hide, you have nothing to fear'.

Fears over judges' veto on spying

The 'double lock' plan to allow judges a veto on spying missions was under attack from all sides last night.

Under the proposed compromise, a warrant to carry out intrusive surveillance - such as tapping a phone - would continue to require the approval of the Home Secretary.

But, in a new safeguard, separate approval would also be needed from one of eight new judicial commissioners.

The final decision on whether the undercover operation could go ahead would ultimately rest with the judges - who, unlike politicians, are not accountable to the public.

In the most dramatic scenario, a judge could refuse to sanction a spying mission on a suspect who might go on to commit an atrocity, triggering a huge political row.

Downing Street and Theresa May had previously stressed their preference was for the warrant power to remain with ministers alone - Mrs May signed 2,450 warrants last year.

Government insiders believe the compromise is necessary to win approval for the Bill, which - given the Tory Party's slender majority - could face a ferocious battle in the Commons as well as in the Lords.

Tory former Northern Ireland Secretary Owen Paterson, who was responsible for signing hundreds of warrants, warned the double-lock could lead to crucial delays.

He told MPs: 'I believe strongly these decisions should be made by an elected member of this House, accountable to this House. I am concerned that involving another decision maker from the judiciary, who may not have particular skills in this area, will bring delay and will bring complication.

'How many hours after an early morning decision by a secretary of state will there be scrutiny by a judge?'

However, civil liberties campaigners criticised Mrs May for not having gone far enough in diluting the Home Secretary's powers. They pointed out that the independent reviewer of terrorism, David Anderson QC, had suggested judges alone should approve or decline a warrant.

Tory David Davis, a former shadow home secretary, said that, in any event, the 'double lock' was not as it seemed.

He pointed out the Bill says the judicial commissioners will 'have to make decisions based on judicial review principles, not on the basis of the evidence'.

Mr Davis, the likely leader of any Tory backbench revolt against the legislation, added: 'In other words the Home Secretary would have to behave in an extraordinary manner not to get his or her warrant approved.

MORE THAN 850 PAEDOPHILES AT LARGE ON WEB IN THE UK

More than 850 active paedophiles at large in the UK are beyond the reach of the police because officers do not have access to internet records, it was claimed last night.
Government officials said the suspects had been posting vile images of child abuse online.

But child protection experts are unable to identify them because, under existing rules, service providers are not obliged to store details of websites a person visits.

This is preventing police from linking a person's IP address - a code which identifies the user of a computer or smartphone - to the websites where the images are being shared.

Home Office sources said the National Crime Agency had examined a sample of 6,025 referrals to its child abuse command and found that inquiries against 862 potential suspects could not be pursued without access to their internet connection records.

Analysis of the mobile phone use of 600 serious criminal suspects revealed 300 were communicating online and potentially out of reach, officials said.

'This is not the judge checking the evidence, it is the judge checking that the correct procedure has been followed.'

Mrs May said that in 'urgent' circumstances - such as a direct threat to life - a warrant could come into force without prior judicial approval. It would last for a maximum of five days. She also announced the Prime Minister would have to be consulted before MPs' communications could be intercepted by spies.

Mrs May said the move - which will also apply to peers, MEPs and members of the devolved institutions - would write the protection of the so-called Wilson Doctrine into law for the first time.

MPs have been seething since a tribunal ruled last month that, under existing rules, they are not entitled to any special protection from having their phones tapped.

LOAD-DATE: November 5, 2015
LANGUAGE: ENGLISH
PUBLICATION-TYPE: Web Publication
JOURNAL-CODE: WEBDM

Government spooks have been secretly spying on UK phone calls in a bid to root out terrorists, it has emerged.
MI5 is said to have collected vast swathes of data about public communications over the last decade. The programme has been running over a law described as "vague" by a government security adviser. It comes as Theresa May proposed new legislation meaning everything the public does online - from Facebook stalking to watching pornography - will be stored by the government.

In her Commons statement, the home secretary referred to the 1984 Telecommunications Act, which she said had allowed successive governments to access data from communications companies. MI5 didn't record what was said during phone calls, just the fact contact was made, according to the BBC report.

David Anderson QC, the government's independent reviewer of terrorism legislation, said the legislation was "so vague that anything could be done under it". He added: "It wasn't illegal in the sense that it was outside the law, it was just that the law was so broad and the information was so slight that nobody knew it was happening".

The Snooper's Charter was unveiled by Home Secretary Theresa May in the House of Commons yesterday.

It will demand that popular mobile phone or broadband providers store YOUR data for at least 12 months, with security bosses and police having permission to access that data without a warrant.

The legislation hopes to combine existing powers available to authorities under a single piece of law. However while Prime Minister David Cameron described it as "one of the most important pieces of legislation" that Parliament will see over the next five years, it has come in for fierce criticism from civil liberties groups.

Shami Chakrabarti, director of Liberty, said: "If the authorities need a judge's warrant before they search my home, why not before the equal or greater intrusion of accessing my private communications?"

"This happens all over the free world including in the United States."

There are also concerns about how the legislation may risk your privacy, with corporations being ordered to store mass amounts of your personal data just weeks after high-profile hacks at websites such as adultery website Ashley Madison, or broadband provider TalkTalk.

Speaking to Sky News, Chris Phillips, the former head of the National Counter Terrorism Security Office, said: "The world has moved on so quickly: people communicate on many different means, whether it's WhatsApp, whether it's Facebook, whether it's email or telephone.

"So it's really important that the laws keep up. [Without new laws] we'd be in a very dangerous place."

The so-called Snooper's Charter was originally floated in 2012, but faced heavy opposition from Liberal Democrat ministers in the Coalition.

Ashley Madison: Why was cheating website hacked?

LOAD-DATE: November 5, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

Copyright 2015 Trinity Mirror, Plc. All Rights Reserved

Return to List

60 of 104 DOCUMENTS

The Sun (England)
THERESA MAY yesterday revealed for the first time the incredible covert measures taken by British spies.

The Home Secretary admitted that intelligence officers hack computers, use devices' microphones as bugs and harvest vast amounts of bulk data from all over the world.

The revelations came as the Tory minister unveiled the draft Investigatory Powers Bill in Parliament aimed at giving sweeping new powers for security chiefs. Mrs May dubbed it "a licence to operate".

The Bill will force internet providers to store for up to a year records of all the social media messages users send and all the websites they visit.

Police will not need a warrant to access the information.

But they will need special permission to see detailed browsing history or the content of messages. In a bid to reassure the public the new powers will not be abused, Mrs May proposed a "double lock" of judges and Cabinet ministers to approve these requests.

Mrs May also announced a beefed-up regulator and tough new controls on cops to force them to always ask a judge before prying on journalists' calls or emails to their sources.

This move is a victory in a year-long campaign by The Sun and others newspapers.

Below CRAIG WOODHOUSE takes a look at what the new measures mean for you.

Can spies read my emails?

Potentially yes - but only if you are suspected of some pretty serious crimes.

The Bill lets law enforcement agencies, the MI5 domestic security service, foreign intelligence service SIS (formerly MI6), listening post GCHQ and the Ministry of Defence carry out what is called "interception", letting them read emails.

But this is only for protecting national security, tackling serious crime and stopping the economy being harmed. And then only if the Home Secretary signs it off and a judge approves it.

What about my internet browsing history?

Partly, and not just the spies. Public bodies including the taxman and police can also obtain so-called "communications data" - basically a list like an itemised phone bill of what sites you have visited but not what pages.

So it would show that you had visited www.thesun.co.uk, but not what stories you had read.

Web companies will be forced to keep the information for 12 months.

What about councils?

Can they see what I've been searching? No. They have been severely limited in being able to apply for the communications data amid fears of snooping by busybodies.

They can only ask to see info if they can show they are trying to help fight crime.

But what's to stop determined busybodies in these authorities trying it on?

A new two-year jail term can be slapped on anyone who tries to misuse the power.
It will also require a two-stage sign-off, first by someone in the relevant authority and then by a trained checker making sure their application is fair.

OK, that's the internet.

What about phone calls?
The same people who can read your emails - spies and law enforcement agencies - can also listen in to your phone calls.

But again they would need a very good reason to do so and would have to convince the Home Secretary and a judge to agree. What about other spying tricks? The Bill covers those too. It lets spooks and major crime fighters secretly break in to computers and smartphones without the user knowing.

It also lets them download content during searches without the user knowing.

Police Chief Constables can approve this for cops, the Home Secretary is in charge for the spies.

Anything else?
Oh yes. The Bill lets MI5, GCHQ and SIS hoover up vast amounts of data using all the tricks above in what is known as "bulk powers". This is key to monitoring terrorists and working out what they are up to.

It will usually only be used for national security. And warrants will normally only be issued to track bad guys abroad.

Spies will need permission to suck up the data, then need extra permission if they want to look at it. They will also have to say what it will be used for.

But I've done nothing wrong. Is it only terrorists that have anything to fear?
Terrorists and other bad guys such as paedophiles and major criminals. The Government has taken great care to ensure lawabiding Brits will not be spied on as they go about their daily lives.

This follows criticism that previous proposals would be a "snooper's charter".

Even Labour seems happy with the balance, saying the new Bill is "neither a snooper's charter nor a plan for mass surveillance".

Will I know if I'm being spied on?
You might not be able to find out. But MPs might try to change that as the Bill makes its way through Parliament.

Where is the data stored? Won't it leak out?
If the security services told you where it was being held then it would defeat the point of keeping it secret. Government sources say it will be subject to "robust security arrangements" and "strong safeguards".

LOAD-DATE: November 5, 2015

LANGUAGE: ENGLISH

GRAPHIC: BILL ... Theresa MayLISTENING IN ... GCHQ building in Cheltenham

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: SUN

Copyright 2015 NEWS GROUP NEWSPAPERS LTD
All Rights Reserved

Return to List

61 of 104 DOCUMENTS
What spooks know about you; MAY UNVEILS SPY POWERS

BYLINE: TOM NEWTON DUNN

SECTION: NEWS; Pg. 8

LENGTH: 721 words

THERESA MAY yesterday revealed for the first time the incredible covert measures taken by British spies. The Home Secretary admitted that intelligence officers hack computers, use devices’ microphones as bugs and harvest vast amounts of bulk data from all over the world.

The revelations came as the Tory minister unveiled the draft Investigatory Powers Bill in Parliament aimed at giving sweeping new powers for security chiefs. Mrs May dubbed it "a licence to operate".

The Bill will force internet providers to store for up to a year records of all the social media messages users send and all the websites they visit.

Police will not need a warrant to access the information. But they will need special permission to see detailed browsing history or the content of messages. In a bid to reassure Can spies read my emails? Potentially yes - but only if you are suspected of some pretty serious crimes.

The Bill lets law enforcement agencies, the MI5 domestic security service, foreign intelligence service SIS (formerly MI6), listening post GCHQ and the Ministry of Defence carry out what is called "interception", letting them read emails.

But this is only for protecting national security, tackling serious crime and stopping the economy being harmed. And then only if the Home Secretary signs it off and a judge approves it.

What about my internet browsing history? Partly, and not just the spies. Public bodies including the taxman and police can also obtain so-called "communications data" - basically a list like an itemised phone bill of what sites you have visited but not what pages.

So it would show that you had visited www.thesun.co.uk, but not what stories you had read.

Web companies will be forced to keep the information for 12 months.

What about councils? Can they see what I've been searching? No. They have been severely limited in being able to apply for the communications data amid fears of snooping by busybodies. They can only ask to see info if they can show they are trying to help fight crime.

But what's to stop determined busybodies in these authorities trying it on? A new two-year jail term can be slapped on anyone who tries to misuse the power.

It will also require a two-stage sign-off, first by someone in the relevant authority and then by a trained checker making sure their application is fair.

OK, that's the internet. What about phone calls? The same people who can read your emails - spies and law enforcement agencies - can also listen in to your phone calls.

But again they would need a very good reason to do so and would have to convince the Home Secretary and a judge to agree.

What about other spying tricks? The Bill covers those too. It lets spooks and major crime fighters secretly break in to computers and smartphones without the user knowing.

It also lets them download content during searches without the user knowing.

Police Chief Constables can approve this for cops, the Home Secretary is in charge for the spies.
Anything else? Oh yes. The Bill lets MI5, GCHQ and SIS hoover up vast amounts of data using all the tricks above in what is known as "bulk powers". This is key to monitoring terrorists and working out what they are up to.

It will usually only be used for national security. And warrants will normally only be issued to track bad guys abroad.

Spies will need permission to suck up the data, then need extra permission if they want to look at it. They will also have to say what it will be used for.

But I've done nothing wrong. Is it only terrorists that have anything to fear? Terrorists and other bad guys such as paedophiles and major criminals. The Government has taken great care to ensure lawabiding Brits will not be spied on as they go about their daily lives.

This follows criticism that previous proposals would be a "snooper's charter".

Even Labour seems happy with the balance, saying the new Bill is "neither a snooper's charter nor a plan for mass surveillance". Will I know if I'm being spied on? You might not be able to find out. But MPs might try to change that as the Bill makes its way through Parliament.

Where is the data stored? Won't it leak out? If the security services told you where it was being held then it would defeat the point of keeping it secret. Government sources say it will be subject to "robust security arrangements" and "strong safeguards".

LOAD-DATE: November 5, 2015

LANGUAGE: ENGLISH

GRAPHIC: BILL ... Theresa MayLISTENING IN ... GCHQ building in Cheltenham

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: SUN

Copyright 2015 NEWS GROUP NEWSPAPERS LTD
All Rights Reserved

Return to List

62 of 104 DOCUMENTS

Daily Mirror

November 6, 2015 Friday
Edition 1;
National Edition

Spy Bill is threat to our freedom

BYLINE: FIONA PARKER

SECTION: FEATURES; OPINION COLUMN; Pg. 52

LENGTH: 566 words

EVERYONE wants to be safe and to support measures to help discover potential terrorists plotting against us. But how the politicians and legal profession choose to operate any new powers is a matter of contention and could be abused.

If the Investigatory Powers Bill is passed and becomes law, it should only be enforced with solid and substantiated reasons to so do.

We are all fortunate to live in a free and democratic society where civil liberties are respected and it is imperative that we, and our political leaders, never lose sight of this.

215
Diane Silva, Lytham, Lancs

This Bill is just the start. Soon the Government will demand access to all your private information without the need for a warrant. Our freedom and individual privacy are basic rights hard won by previous generations but it seems people are willing to let them be taken away without so much as a murmur. George Orwell's 1984 is very much beginning to look like the reality of life in Tory Britain.

T Lockwood Stockport, Gtr Manchester

These new powers aren't about criminal surveillance; they are about the Government spying on the people. We already have terrorist legislation being used to go through our dustbins and now they want to spy on our emails.

Security is always used as the reason for these draconian laws but the reality is the more intrusive our Government is, the less secure our private lives are - and soon we will realise we have no rights at all.

S T Vaughan, Birmingham

If the authorities can access your online data and browsing habits, then surely any competent online hacker would have the same or even better capabilities?

I fear you could be targeted by all sorts of scams while browsing online if the Government needs reduced security in order for them to access your data. We need more privacy, not less. Anything less than that and terrorism has won the battle, it's as simple as that.

Phillip Smith via Mirror online

Why is there such opposition to the new Investigatory Powers Bill, with MPs demanding judges must sign warrants to permit intrusion into an individual's privacy? Surely, we all know our web activities need monitoring and indeed GCHQ already operates mass surveillance of UK citizens, judge or no judge.

We need protection from extremist plotters and I doubt most Brits would lose much sleep over the authorities having access to their web history when we already accept we are the most watched population in Europe.

Willie McKenna Uckfield, East Sussex

The point is this: whatever you have to hide doesn't compare have to hide with the bigger priority of stopping serious crime. You're going to wish police had read a few of your awkward emails the next time you're getting blown upon a train. There's no such thing as free speech either, that is also controlled by the law. As long as it's clearly related to an investigation, then I have no problem with police checking my browsing history to stop crime.

Elle Hancock Newcastle upon Tyne

I object to the Investigatory Powers Bill. We are not a police state and what I look at on the internet is my business and mine alone. Who do the Tories think they are?

David Bridling David Marsden Bridlington, East Yorks

THE BIG ISSUE

Theresa May's Investigatory Powers Bill lets government agencies see our web browsing history, hack phones and read social media messages. Critics say it hits civil liberties. Many of you agree...

LOAD-DATE: November 6, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: DMR
Investigatory Powers Bill: Labour accused of acting like a 'nodding dog' over support for Theresa May's plans; Exclusive: LibDem leader Tim Farron promises to lead fight against draft bill as he seeks to carve out a niche for his party

BYLINE: Andrew Grice

SECTION: UK POLITICS

LENGTH: 733 words

The Liberal Democrats have accused Labour of acting like a "nodding Conservative dog" for giving qualified support to Theresa May's controversial plans to shake up Britain's surveillance laws.

Tim Farron, the Lib Dem leader, has promised to lead the fight against the Draft Investigatory Powers Bill as he seeks to carve out a niche for his party as a champion of civil liberties.

The Lib Dems will table amendments to the legislation in an attempt to give judges, rather than ministers, the power to authorise warrants to intercept the contents of people's communications and hack computers. Mrs May proposed a "double-lock" under which ministers could approve warrants in urgent cases, with their action reviewed later by judges.

Read more

Five things you need to know about the 'Snooper's Charter'

Mr Farron told The Independent: "The Home Secretary has created a sham of judicial authorisation that doesn't fool me, the public or the experts. It is an utter disgrace."

He added: "The Labour Party is even worse though. It is acting like Conservatives on this Bill and just acquiescing. It is about as useful as a nodding dog. The Liberal Democrats will make sure the public's concerns are heard. You can't rely on Labour or the Tories to stand up for our hard won civil liberties."

Liberal Democrat leader Tim Farron has said that his party will strongly oppose the Draft Investigatory Powers Bill

The Lib Dems will also seek "redress" for individuals who are no longer under suspicion, under which people would be told they had been under surveillance unless there were a specific reason to maintain secrecy. The United States, Germany and Belgium have such a provision, the Lib Dems say. "You can't seek justice if you never know you've been spied on," said a party source.

Mr Farron's tough stance could prove important when the legislation reaches the House of Lords. The party has 108 peers and can defeat the Government by joining forces with Labour. Many of the 149 independent crossbenchers have strong views on civil liberties.

The Lib Dem leader is adopting a harder line than his predecessor Nick Clegg did when he responded to Mrs May's announcement in the Commons on Wednesday. Mr Clegg said the proposals had been "much improved" since his party blocked her original "snooper's charter inside the Coalition Government."

Read more

Snooper's charter calls on firms to store clients' data for a year
Theresa May is 'villain of the year' for Snooper's Charter
Concessions to surveillance bill unlikely to head off peer revolt
MI5 secretly collected Britons' data for 'more than a decade'

Theresa May accused of launching 'major attack on privacy'

Mr Farron’s intervention could raise tensions inside the Labour Party. Jeremy Corbyn has a strong record of attacking the Tories on civil liberties. But Andy Burnham, the shadow Home Secretary, said Mrs May had "listened to legitimate concerns" and broadly got right the difficult balance between national security and the privacy of individuals. He said the draft Bill was "neither a snooper's charter nor a plan for mass surveillance."

A Labour spokesman said: "We will support plans that protect children, keep the public safe and tackle online fraud. Tim Farron must say which of those things he's now opposed to. The safeguards are important and it has been Labour, not the Liberal Democrats, pushing the Home Secretary for more details on the precise role of judges and we'll continue to do that."

Mr Clegg said the "double lock" of judicial oversight "appears to be nothing of the sort, as judges will have very little discretion when making decisions about individual warrants." But the former Deputy Prime Minister argued: "We are now in touching distance of a comprehensive new law covering every single surveillance power at the disposal of the Government."

Liberty, the civil liberties organisation, has launched a campaign against a draft Bill that it claims "will make us less and less free." The group added: "Surveillance powers can play an important part in preventing and detecting serious crime. But the current framework fails to provide sufficient safeguards to ensure it is conducted in a necessary, proportionate and accountable way."

LOAD-DATE: November 6, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI

Copyright 2015 Independent Digital News and Media Limited
All Rights Reserved

Return to List

64 of 104 DOCUMENTS

Sacrifice a little privacy to support our spies, says anti-terror tsar:
LORD CARLILE warns how without UK intelligence MORE planes
might have blown up over Egypt

BYLINE: DAILY MAIL COMMENT

SECTION: RIGHTMINDS

LENGTH: 1178 words

Would Theresa May steal our privacy? When the Home Secretary announced that her Investigatory Powers Bill would increase the security services’ scope to watch the way we use the internet, up rose the predictable screams of protest.

She had, it was said, produced a 'snooper's charter'. The Bill, it was claimed, will undermine fundamental civil liberties at the behest of an overmighty state.
I and many others believe such claims are not only unfair, but malign - they are too often a disreputable attempt to undermine rational debate on a subject which not only concerns us all, but can fairly be described as a matter of life and death.

The Russian airliner from Sharm-el-Sheikh, destroyed with the death of all on board, comes immediately to mind.

We are told that intelligence analysts in the Joint Terrorism Analysis Centre, or JTAC, a rarely mentioned UK Government office, discovered Sharm-el-Sheik airport was so porous that it was penetrated easily by an IS bomber - whilst tourists were being offered to bypass security in return for £20 notes.

It is at the same time shocking, yet all too believable.

Only yesterday we learned the American intelligence services picked up internet 'chatter' between known jihadis before the catastrophic crash - and after, when chilling messages of celebration were intercepted.

Russian protests evaporated within hours into acceptance of the JTAC judgment, founded on the interception of calls and on communications data, and analysis of their patterns. If not for JTAC - which draws together Government security agencies under the supervision of Mi5 - how many more planes at Sharm might have been affected by this carry-on bomb butchery? How many more lives has British intelligence saved?

What exactly is it, then, that Mrs May and her controversial Bill are proposing?

One important provision is that the authorities should continue to have access, over a limited period (set at 12 months), to the metadata - the 'what' and 'when', but not the content, of communications.

Already this is used in courts to establish where murderers, drug dealers, terrorists and other serious criminals were at key times. To undermine this capability would be not less than a disaster for the prevention and detection of crime. The Crown Prosecution Service view is that a high majority of serious contested trials rely to some part on this type of data.

This is clearly no 'snoopers charter'. Parliament should support the Home Secretary, and conclude that it is no more than a necessary modernisation of traditional forms of detection.

The fact is that we are in a new world. Forty years ago, interception of criminals' communications was much simpler. It was largely restricted to a cruder, nationalised telephone system and the Royal Mail.

Today life is terrifyingly more complicated. We are trying to spot and track lone wolves in the secure bubbles of their bedrooms. Armed with multiple and impenetrably encrypted fake identities, they can disrupt huge entities and utilities, even basic necessities like electricity.

For example, last year James Arbuthnot MP, then Defence Select Committee chairman, told a London conference: 'Our National Grid is coming under cyber-attack not just day-by-day but minute-by-minute' after his committee had scrutinised the country's security policy.

As Mrs May says, such challenges mean we must allow the security services the proportionate tools they need to protect us from the ever more complex, technically sophisticated and secret actions of dangerous enemies like IS as well as the criminals and cranks who use the internet to damage and even endanger our lives.

There is another uncomfortable truth: voluntarily we have given away a huge percentage of our privacy to the private sector. The so-called 'privacy policies' of major internet based companies, including the social networks, are no such thing.

They allow the keeping and largely uncontrolled sharing of information. In a few days' time online shops will remind us what we enjoyed in our Christmas orders last year. iTunes knows exactly what new Christmas music will meet our tastes.

By merely giving my date of birth to an online retailer, I give permission to them to sell my details and produce an avalanche of offers tailored to me and other people of pensionable age. Against this voluntary surrender, the use by the State of limited information about suspect individuals, to protect the public as a whole, is a small and reasonable concession.

One serious question is this: does this Bill allow the browser history of any random member of the public to be accessed by the authorities?

The clear answer is No. Your browser history or mine will only be accessed if there is a specific reason requiring it.
But there is a second aspect of the Bill about which I am more worried - for judges to be involved in verifying warrants for the interception of content.

This has been accepted by Mrs May. Is she right? Up to a point.

When a Minister approves an interception warrant, she is accountable to Parliament. If there is a serious error, she will be forced to resign, possibly even her seat.

Judges, brilliant as many are, cannot be held accountable in anything like the same way.

Most have no deep knowledge of national security. Nor can they be allowed to make policy - all they can do is check what has happened for legality. So Parliament will have to consider whether the proposals forget proper role of the courts.

As the destruction of the Egyptian airliner makes clear, our security services are crucial.

Yet - much to Mrs May’s disadvantage - any recognition of the extraordinary contribution to public safety by the police and security services is almost impermissible in some minds.

I would have far more respect if such campaigners offered a cogent alternative to the Bill. If Theresa May is so wrong, where are the proposals with which the critics would replace hers? Criticising without exercising responsibility is no better than the troll who, busy attacking one traveller, leaves the road wide open to whatever passes.

I urge Parliament to consider Mrs May’s Bill bearing this evidence in mind - and not on the basis of prejudiced argument.

The Bill will go to a Scrutiny Committee of Commons and Lords, where visceral party political hostility must be set aside to ensure that we hold the precious balance between security and liberty.

Whatever solution is reached, we must have regard for wider opinions than those of raucous interest groups. Mrs May knows most citizens wish to be protected from bombs, attacks on the electricity system and misuse of their bank accounts. Most see the reason in giving the unsung heroes of the security services the tools they need.

The public recognise the absurdity of the notion of a wicked MI5 agent who is so bored he has the time or curiosity to examine the telephone traffic of those not under suspicion of serious crime.

The reality is the techniques sought by this Bill, with considerable checks, are what is needed to ensure we remain what we are - a reasonably safe country in an unsafe world.
WITHOUT UK INTELLIGENCE, HOW MANY MORE PLANES MIGHT HAVE BEEN BLOWN UP OVER EGYPT? THAT’S WHY I MAKE THIS PLEA: SACRIFICE A LITTLE PRIVACY TO

BY LORD CARLILE FORMER INDEPENDENT REVIEWER OF ANTI-TERROR LEGISLATION

WOULD Theresa May steal our privacy? When the Home Secretary announced that her Investigatory Powers Bill would increase the security services’ scope to watch the way we use the internet, up rose the predictable screams of protest.

She had, it was said, produced a snooper’s charter. The Bill, it was claimed, will undermine fundamental civil liberties at the behest of an overmighty state.

I and many others believe such claims are not only unfair, but malign - they are too often a disreputable attempt to undermine rational debate on a subject which not only concerns us all, but can fairly be described as a matter of life and death.

The Russian airliner from Sharm-el-Sheik, destroyed with the death of all on board, comes immediately to mind.

We are told that intelligence analysts in the Joint Terrorism Analysis Centre, or JTAC, a rarely mentioned UK Government office, discovered Sharm-el-Sheik airport was so porous that it was penetrated easily by an IS bomber - whilst tourists were being offered to bypass security in return for £20 notes.

It is at the same time shocking, yet all too believable.

Only yesterday we learned the American intelligence services picked up internet chatter between known jihadis before the catastrophic crash - and after, when chilling messages of celebration were intercepted.

Russian protests evaporated within hours into acceptance of the JTAC judgment, founded on the interception of calls and on communications data, and analysis of their patterns. If not for JTAC - which draws together Government security agencies under the supervision of Mi5 - how many more planes at Sharm might have been affected by this carry-on bomb butchery? How many more lives has British intelligence saved?

What exactly is it, then, that Mrs May and her controversial Bill are proposing?

One important provision is that the authorities should continue to have access, over a limited period (set at 12 months), to the metadata - the what and when, but not the content, of communications.

Already this is used in courts to establish where murderers, drug dealers, terrorists and other serious criminals were at key times. To undermine this capability would be not less than a disaster for the prevention and detection of crime. The Crown Prosecution Service view is that a high majority of serious contested trials rely to some part on this type of data.

This is clearly no snooper’s charter. Parliament should support the Home Secretary, and conclude that it is no more than a necessary modernisation of traditional forms of detection.

The fact is that we are in a new world. Forty years ago, interception of criminals’ communications was much simpler. It was largely restricted to a cruder, nationalised telephone system and the Royal Mail.

Today life is terrifyingly more complicated. We are trying to spot and track lone wolves in the secure bubbles of their bedrooms. Armed with multiple and impenetrably encrypted fake identities, they can disrupt huge entities and utilities, even basic necessities like electricity.

For example, last year James Arbuthnot MP, then Defence Select Committee chairman, told a London conference: Our National Grid is coming under cyber-attack not just day-by-day but minute-by-minute after his committee had scrutinised the country’s security policy.

As Mrs May says, such challenges mean we must allow the security services the proportionate tools they need to protect us from the ever more complex, technically sophisticated and secret actions of dangerous enemies like IS as well as the criminals and cranks who use the internet to damage and even endanger our lives.

There is another uncomfortable truth: voluntarily we have given away a huge percentage of our privacy to the private sector. The so-called privacy policies of major internet based companies, including the social networks, are no such thing.

They allow the keeping and largely uncontrolled sharing of information. In a few days time online shops will remind us what we enjoyed in our Christmas orders last year. iTunes knows exactly what new Christmas music will meet our tastes.
By merely giving my date of birth to an online retailer, I give permission to them to sell my details and produce an avalanche of offers tailored to me and other people of pensionable age. Against this voluntary surrender, the use by the State of limited information about suspect individuals, to protect the public as a whole, is a small and reasonable concession.

One serious question is this: does this Bill allow the browser history of any random member of the public to be accessed by the authorities?

The clear answer is No. Your browser history or mine will only be accessed if there is a specific reason requiring it.

But there is a second aspect of the Bill about which I am more worried - for judges to be involved in verifying warrants for the interception of content.

This has been accepted by Mrs May. Is she right? Up to a point.

When a Minister approves an interception warrant, she is accountable to Parliament. If there is a serious error, she will be forced to resign, possibly even her seat.

Judges, brilliant as many are, cannot be held accountable in anything like the same way.

Most have no deep knowledge of national security. Nor can they be allowed to make policy - all they can do is check what has happened for legality. So Parliament will have to consider whether the proposals forget proper role of the courts.

As the destruction of the Egyptian airliner makes clear, our security services are crucial.

Yet - much to Mrs May’s disadvantage - any recognition of the extraordinary contribution to public safety by the police and security services is almost impermissible in some minds.

I would have far more respect if such campaigners offered a cogent alternative to the Bill. If Theresa May is so wrong, where are the proposals with which the critics would replace hers? Criticising without exercising responsibility is no better than the troll who, busy attacking one traveller, leaves the road wide open to whatever passes.

I urge Parliament to consider Mrs May’s Bill bearing this evidence in mind - and not on the basis of prejudiced argument.

The Bill will go to a Scrutiny Committee of Commons and Lords, where visceral party political hostility must be set aside to ensure that we hold the precious balance between security and liberty.

Whatever solution is reached, we must have regard for wider opinions than those of raucous interest groups. Mrs May knows most citizens wish to be protected from bombs, attacks on the electricity system and misuse of their bank accounts. Most see the reason in giving the unsung heroes of the security services the tools they need.

The public recognise the absurdity of the notion of a wicked MI5 agent who is so bored he has the time or curiosity to examine the telephone traffic of those not under suspicion of serious crime.

The reality is the techniques sought by this Bill, with considerable checks, are what is needed to ensure we remain what we are - a reasonably safe country in an unsafe world.
Andy Burnham calls for more judicial safeguards in UK surveillance bill;
Shadow home secretary, who had welcomed draft investigatory powers bill, shifts position in letter to Theresa May after consulting Lord Falconer

BYLINE: Patrick Wintour Political editor

SECTION: POLITICS

LENGTH: 588 words

Andy Burnham has reconsidered his initially warm welcome for the draft investigatory powers bill after discussions with the leader's office and the shadow justice secretary, Lord Falconer.

The shadow home secretary had welcomed the bill in the Commons last week, saying it was neither a snooper's charter nor mass surveillance, but it now appears he feels he was misled about the scale of the judicial safeguards in the bill.

In the buildup to the launch of the draft bill, the government gave the impression it was making a major shift away from a system of intrusive warrants issued only by ministers and that in future, judges would be equal partners in the warrant process. But Burnham has now written to the home secretary, Theresa May, to criticise the absence of judicial authorisation for intercept warrants.

The bill gives the state powers to force communications firms to store individuals' internet connection records - the addresses of websites visited - for 12 months.

Related: This snooper's charter makes George Orwell look lacking in vision| Heather Brooke

The Liberal Democrat leader, Tim Farron, accused Labour of behaving like a "nodding dog", and the official reviewer of terrorism legislation, David Anderson, appeared to take a more critical stance on some of the proposals than the party.

Few Labour shadow ministers have criticised the bill, focusing instead on the compromises that have been made since the snooper's charter was first published in 2012.

In a letter to May released to the New Statesman, Burnham said he wanted to work constructively over the bill, but added: "I have now had the opportunity to study your proposals in detail and have taken advice from the shadow justice secretary. This has given rise to concerns that the safeguards you are proposing are not as strong as it appeared when they were presented to the Commons."

Burnham echoed concerns raised by civil liberties campaigners over the so-called "double-lock" for intercept warrants, warning that judicial authorisation would not be required. He wrote: "[You] created the impression that both the home secretary and a senior judge would review the evidence. Indeed, you may recall that I asked you in the House about what would happen if there were a difference of opinion between the two.

"On closer inspection of the wording of the bill, it would seem that it does not deliver the strong safeguard that you appeared to be accepting. The current wording of the draft bill requires the judge to review the 'process' undertaken by the home secretary in the same way applied to a judicial review."

Related: Mass snooping and more - the measures in Theresa May's bill

Burnham added: "Legal advice we have sought confirms that the current wording does not deliver what we believed was being proposed in terms of the home secretary and judicial commissioner double lock for warrant authorisation."

Burnham said that if Labour's understanding was correct, the party would look to amend the bill at committee stage to ensure a genuine double-lock.

The shadow home secretary also argued that the legislation "needs to include clearly defined thresholds for access to internet connection records" and that the records should be limited to "police officers of a specified seniority".
He concluded: "I believe you have produced a framework which has the potential to give the authorities the powers they need whilst also commanding public trust. But that will only be achieved by strengthening the safeguards in the areas I have identified."

LOAD-DATE: November 9, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Apple boss warns Tories' snooper's charter could HELP criminals by weakening data security;
Fears WhatsApp and Apple's iMessage could be hit by the Investigatory Powers Bill making data less secure

BYLINE: By David Hughes

SECTION: NEWS, UK NEWS

LENGTH: 513 words

The boss of Apple has warned against giving spies a "back door" to reading people's emails because weakening data security could help criminals.

Tim Cook said any attempt to weaken encryption could have "very dire consequences", harming consumers by making their data less secure.

Under proposals in Theresa May's Investigatory Powers Bill, communications firms will be legally required to help spies hack into suspects' smartphones and computers.

Read more: New internet snooping law will NOT ban WhatsApp and Snapchat

Domestic providers will be obliged to assist intelligence agencies when they are given warrants to carry out equipment interference.

The technique allows authorities to interfere with electronic devices in order to obtain data and can range from remotely accessing a computer to covertly downloading the contents of a mobile phone.

It is seen as an increasingly crucial tool as advanced encryption makes intercepting targets' communications more difficult.

There are also fears in technology circles that the proposals will hit services offering "end-to-end encryption" such as WhatsApp and Apple's iMessage, despite the Home Secretary's assurances that the legislation "will not ban encryption or do anything to undermine the security of people's data".

The proposed new laws could impose obligations on telecommunications providers requiring them to remove "electronic protection" applied to "communications or data".
In an interview with the Daily Telegraph, Mr Cook said: "To protect people who use any products, you have to encrypt."
"You can just look around and see all the data breaches that are going on.
"These things are becoming more frequent.
"They can not only result in privacy breaches but also security issues.
"We believe very strongly in end-to-end encryption and no back doors."
The technology giant's chief executive warned: "We don't think people want us to read their messages.
"We don't feel we have the right to read their emails.
"Any back door is a back door for everyone.
Read more: Snooper's Charter plans revealed: Government wants your to track your porn viewing, Facebook stalking and online shopping
"Everybody wants to crack down on terrorists.
"Everybody wants to be secure.
"The question is how.
"Opening a back door can have very dire consequences."
He added: "It's not the case that encryption is a rare thing that only two or three rich companies own and you can regulate them in some way.
Read more: 7 reasons you should be worried about the Tory snooper's charter
"Encryption is widely available.
"It may make someone feel good for a moment but it's not really of benefit.
"If you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things.
"It's the good people.
"The other people know where to go."
But he said he was "optimistic" that the Government would change its approach: "When the public gets engaged, the press gets engaged deeply, it will become clear to people what needs to occur.
"You can't weaken cryptography.
"You need to strengthen it.
"You need to stay ahead of the folks that want to break it."

LOAD-DATE: November 9, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

Copyright 2015 Trinity Mirror, Plc.
All Rights Reserved

Return to List

68 of 104 DOCUMENTS

mirror.co.uk
Theresa May's spying Bill stops short of allowing access to your full web browsing history;
THE Home Secretary says providers WON'T pass on all the pages visited, but will give 'the modern equivalent of an itemised phone bill" to security services.

BYLINE: By Arj Singh

SECTION: NEWS,POLITICS

LENGTH: 1218 words

THE security services will not be allowed to access web users’ full browsing histories under new surveillance powers, Theresa May has insisted.

The Home Secretary said it was "simply wrong" to suggest that new powers in the draft Investigatory Powers Bill to access "internet connection records" would allow the collection of someone's full web history.

Mrs May said it would allow the likes of the police and GCHQ to know if someone has visited a social media website like Facebook - but not which pages they looked at, who they communicated with, or what they said.

Mrs May claimed the new powers allow access to "the modern equivalent of an itemised phone bill" and would not allow security services to see whether someone had visited, for example, a medical or news website.

Instead only "communications websites", illegal websites and certain IP addresses would fall under the scope of the plans.

The Home Secretary said there would be stricter safeguards in place for accessing the records over and above what is in place for current powers and that local authorities would be banned from using them.

In a Commons statement, she said: "Some have characterised this power as law enforcement having access to people's full web browsing histories.

"Let me be clear, this is simply wrong - an internet connection record is a record of the communications service that a person has used, not a record of every web page they have accessed.

"So if someone has visited a social media website, an internet connection record will only show that they accessed that site, not the particular pages they looked at or who they communicated with or what they said.

"it is simply the modern equivalent of an itemised phone bill.

"Law enforcement agencies would not be able to make a request for the purpose of determining, for example, whether someone had visited a mental health website, a medical website or even a news website.

"They would only be able to make a request for the purpose of determining whether someone had accessed a communications website, an illegal website or to resolve an IP address where it is necessary and proportionate to do so in the course of a specific investigation.

"Strict limits will apply to when and how that data can be accessed, over and above those safeguards that apply to other forms of communications data and we will ban local authorities from accessing such data."

Mrs May said the new power on record collection would end the "illogical" current position whereby suspects can be tracked on their mobile phones but not on social media or communications apps.

She said: "It cannot be right that today the police could find an abducted child if the suspects were using mobile phones to coordinate their crime, but if they were using social media or communications apps then they would be out of reach."
"Such an approach defies all logic and ignores the realities of today's digital age."

Mrs May said the Bill also includes provisions for "equipment interference", meaning communications companies will be legally required to help spies hack into smartphones and computers.

It will allow bulk surveillance of the kind revealed in leaks by former US security contractor Edward Snowden as well as the ability to intercept the contents of online or telephone communication.

Existing powers allowing collection of so-called "metadata" - the who, what, where and when of a particular communication - are also included in the scope of the Bill.

The Home Secretary said it was a departure from the heavily criticised "snooper's charter" blocked by the Liberal Democrats during the coalition government and represented the security services' "licence to operate".

She said: "Today's Bill represents a significant departure from the proposals of the past. "Today we are setting out a modern legal framework which brings together current powers in a clear and comprehensible way.

"A new Bill that provides some of the strongest protections and safeguards anywhere in the democratic world and an approach that sets new standards for openness, transparency and oversight."

Mrs May said the Government intends to ensure powers available to law enforcement, security and intelligence agencies are "clear for everyone to understand", with a transparency report published.

She said: "There remains some powers that successive governments have considered too sensitive to disclose for fear of revealing capabilities to those who mean us harm.

"I'm clear we must now reconcile this with our ambition to deliver greater openness and transparency. So the Bill makes explicit provision for all of the powers available to the security and intelligence agencies to acquire data in bulk.

"That will include not only bulk interception provided under the Regulation of Investigatory Powers Act, and which is vital to the work of GCHQ, but also the acquisition of bulk communications data both relating to the UK and overseas."

Mrs May said this is not a new power but will replace an existing one.

She confirmed a "double lock" approach to accessing communications information, with a judge required to approve a warrant signed by the Secretary of State.

Mrs May said: "This will be one of the strongest authorisation regimes anywhere in the world and for parliamentarians we will go even further."

She confirmed the Prime Minister would also be consulted when proposals to intercept the communications of MPs, peers, UK MEPs and politicians in the devolved legislatures are put forward.

Shadow home secretary Andy Burnham said it was important to stress the proposals are "neither a snooper's charter nor a plan for mass surveillance".

The Labour frontbencher said the UK's laws are outdated given changes in technology, noting the jobs of the security services and police are harder.

Mr Burnham said: "In a world where the threats we face internationally and domestically are growing, Parliament cannot sit on its hands and leave blind spots where the authorities can't see."

He said strong powers must be balanced by strong protections for the public, adding: "What the Home Secretary has said today, it seems clear to me both she and the Government have been listening carefully to the concerns that were expressed about the original legislation presented in the last Parliament."

Mr Burnham added: "I think it would help the future conduct of this important public debate if this House sent out a unified message today that this is neither a snooper's charter nor a plan for mass surveillance."

He questioned what data will be retained by the authorities, for how long and whether it will be held in anonymised form, noting public concern has risen following the hacking of TalkTalk.

Mr Burnham also asked how the law will apply to journalistic sources and questioned if the judicial oversight of warrants will delay action.
Looking at the wider context, Mr Burnham said: "There will be fears in some communities, particularly the Muslim community, that these powers will be used against them disproportionately."

He noted police powers have been wrongly used against trade unionists in the past.

Mr Burnham said the Opposition will examine the Bill carefully and seek to improve the safeguards, adding he believes Mrs May has "broadly got that difficult balance right".

Challenge your news brain in our quick quiz:

Quick Quiz: News 4/11/15

LOAD-DATE: November 9, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

Why spies want Apple and Google's help;
The Snoopers' Charter isn't an attack on encryption; there is another plan to intercept WhatsApp

BYLINE: By Christopher Williams Technology, Media and Telecoms Editor

SECTION: FINANCE

LENGTH: 900 words

The controversy over the latest version of the Government's so-called Snoopers' Charter has subsided following publication of the draft Investigatory Powers Bill last week. But it is a battle that is sure to return and escalate.

One important aspect of the Bill that was largely overlooked amid the hue and cry was that it did not actually suggest any solution to the key problem of intercepting encrypted messages. What was presented was instead no more than a tidying up of existing legislation meant to get cooperation from communications companies. For instance, clauses that would allow the Government to order communications providers to take "reasonable" steps to allow interception already exist in UK law.

If it goes through, the Bill is therefore likely to have no impact on the limited ability of GCHQ or MI5 to spy on users of Facebook's WhatsApp messaging app, or iMessage, the internet messaging service built into Apple's iOS. They are the leaders of a growing band of services that use end-to-end encryption, a form of digital security that if implemented properly makes interception practically impossible.

Security sources insist they have no intention of weakening this strong encryption; GCHQ partially invented it, after all, and receives a sizeable chunk of its funding for advising other parts of the Government on how to use it.
A cynic might ask why they should believe those in the espionage business, who by definition have made a profession of dishonesty; for all Theresa May's warm words about encryption - "important for people to be able to keep themselves safe when they are dealing with these modern communications in the digital age" - the intelligence agencies are surely plotting to undermine it in secret.

That is possible, but I understand GCHQ has other plans that would make end-to-end encryption no barrier to surveillance efforts. The snag for the spies is that this would involve the close cooperation of two of the world's largest technology companies, Apple and Google, which have shown little interest in acting as state agents.

'When the Home Secretary says she supports encryption, she does so in the belief there will be a way to circumvent it.'

The Government views their smartphone software duopoly of iOS and Android as a way to tackle the encryption problem and any new communications apps that emerge. Apple and Google, the spies believe, could adapt features that are already part of their software to be used for interception.

The features under discussion relate to usage monitoring and suchlike - the sort of things we all sign up for when we ignore those epic terms and conditions documents issued by the tech giants.

So, if MI5 got a warrant to read a suspect's WhatsApp messages, it would turn to Apple or Google rather than Facebook or a mobile operator. The operating system providers would flick a switch somewhere to effectively allow the spies to read messages straight from the screen. The end-to-end encryption applied in transit would not be weakened, just irrelevant.

In some cases, intelligence agencies already achieve something similar when they hack into smartphones. But breaking and entering is time-consuming, expensive and risky; they want standard points of entry that are less likely to alert suspects they are being watched.

Of course this is easier said than done. There are doubtless major technical barriers and I understand GCHQ has had little luck so far in persuading Apple or Google to even start the necessary engineering discussions.

The question raised by the Investigatory Powers Bill for those companies is whether it will be judged "reasonable" to force them around the whiteboard. But when the Home Secretary says she supports encryption, she does so in the belief there will be a way to circumvent it.

Tim Cook, the chief executive of Apple, has made clear his company's opposition to weakening encryption and to "backdoors" for security agencies. Putting the massive ethical questions aside, the corporate logic for his opposition is clear: Apple is increasingly making the security and privacy features of the iPhone a point of differentiation to help justify its premium price. Agreeing to cooperate with intelligence agencies could undermine that and, claims Cook, actually make customers unsafe by creating a new vulnerability.

The iPhone is also a global phenomenon; could Apple deny similar interception capabilities to the Chinese or Russian government? What would happen if democracy activists came to harm as a result of information it served up?

So this is a battle that begins rather than ends if and when the Snooper's Charter becomes law. Given the unprecedented global scale of the smartphone industry, it could become a serious test of the relative power of state and corporate interests in the digital age.

Call for Vodafone to prepare for the future

It has been a weird six months for those who follow Vodafone's fortunes closely. Protracted talks with Liberty Global came to nothing, for now, and cast a shadow over everything.

On Wednesday, chief executive Vittorio Colao will probably want to get back to discussing operational progress as the company reports interim results.

But he should say something about the next step in his patient rebuilding of Vodafone as a quad-play communications provider. Its disparate global mobile assets were assembled for a world that never arrived.
The battle over your secrets is only just beginning

BYLINE: CHRISTOPHER WILLIAMS

SECTION: BUSINESS; BUSINESS; OPINION COLUMNS; Pg. 2

LENGTH: 883 words

The controversy over the latest version of the Government's Snooper's Charter has subsided after publication of the draft Investigatory Powers Bill last week. But it is a battle that is sure to return and escalate. One important aspect of the Bill that was largely overlooked amid the hue and cry was that it did not actually suggest any solution to the key problem of intercepting encrypted messages.

What was presented was instead no more than a tidying up of existing legislation meant to get cooperation from communications companies. For instance, rules to let the Government order communications providers to take "reasonable" steps to allow interception already exist in UK law.

If it goes through, the Bill is therefore likely to have no impact on the limited ability of GCHQ or MI5 to spy on users of Facebook's WhatsApp messaging app, or iMessage, the internet messaging service built into Apple's iOS. They are the leaders of a growing band of services that use end-to-end encryption, a form of digital security that, if implemented properly, makes interception practically impossible.

Security sources insist they have no intention of weakening this strong encryption; GCHQ partially invented it, after all, and gets a sizeable chunk of its funding for advising other parts of the Government on how to use it.

A cynic might ask why they should believe those in the espionage business, who by definition have made a profession of dishonesty; for all Theresa May's warm words about encryption - "important for people to be able to keep themselves safe when they are dealing with these modern communications in the digital age" - the intelligence agencies are surely plotting to undermine it in secret.

That is possible, but I understand GCHQ has other plans that would make end-to-end encryption no barrier to surveillance. The snag for the spies is that this would involve the close cooperation of two of the world's largest technology companies, Apple and Google, which have shown little interest in acting as state agents.

The Government views their smartphone software duopoly of iOS and Android as a way to tackle the encryption problem and any new communications apps. Apple and Google, the spies believe, could adapt features that are already part of their software to be used for interception.

The features relate to usage monitoring and suchlike - the sort of things we all sign up for when we ignore those epic terms and conditions documents issued by the tech giants.

So, if MI5 got a warrant to read a suspect's WhatsApp messages, it would turn to Apple or Google rather than Facebook or a mobile operator. The operating system providers would flick a switch to
effectively allow the spies to read messages straight from the screen. The end-to-end encryption applied in transit would not be weakened, just irrelevant.

In some cases, intelligence agencies already achieve something similar when they hack into smartphones. But breaking and entering is timeconsuming, expensive and risky; they want standard points of entry that are less likely to alert suspects they are being watched.

Of course, this is easier said than done. There are doubtless major technical barriers and I understand GCHQ has had little luck so far in persuading Apple or Google to even start the necessary engineering discussions.

The question raised by the Investigatory Powers Bill for those companies is whether it will be judged "reasonable" to force them around the whiteboard. But when the Home Secretary says she supports encryption, she does so in the belief there will be a way to circumvent it.

Tim Cook, the chief executive of Apple, has made clear his company's opposition to weakening encryption and "backdoors" for security agencies. Putting the massive ethical questions aside, the corporate logic for his opposition is clear: Apple is increasingly making the security and privacy features of the iPhone a point of differentiation to help justify its premium price. Agreeing to cooperate with intelligence agencies could undermine that and, Cook claims, actually make customers unsafe by creating a new vulnerability.

The iPhone is also a global phenomenon; could Apple deny similar interception capabilities to the Chinese or Russian government? What would happen if democracy activists came to harm as a result of information it served up? So this is a battle that begins rather than ends if and when the Snooper's Charter becomes law. Given the unprecedented global scale of the smartphone industry, it could become a serious test of the relative power of state and corporate interests in the digital age.

Tim Cook interview: Main paper page 16 What next for Colao It has been a weird six months for those who follow Vodafone's fortunes closely. Protracted talks with Liberty Global came to nothing, for now, and cast a shadow over everything.

Today chief executive Vittorio Colao will probably want to get back to discussing operational progress as the company reports interim results.

But he should say something about the next step in his patient rebuilding of Vodafone as a quad-play communications provider. Its disparate global mobile assets were assembled for a world that never arrived.

'When Theresa May says she supports encryption, she does so in the belief there will be a way to circumvent it'

LOAD-DATE: November 10, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: DTL

Copyright 2015 Telegraph Media Group Limited
All Rights Reserved

Return to List

71 of 104 DOCUMENTS

The Guardian

November 10, 2015 Tuesday 10:07 AM GMT

Why tech companies are really worried about the snooper's charter;
Slipped into the new investigatory powers bill is a law that could spell the end of encrypted services such as WhatsApp and iMessage.

BYLINE: Alex Hern

SECTION: TECHNOLOGY

LENGTH: 978 words

Technology firms could be forced into a no-win situation if the UK government's investigatory powers bill passes without substantial changes from its current draft form.

The legislation includes a number of clauses which are scaring technology firms. Under the proposals they can be required to provide assistance to the government to hack their own users; they can be mandated to open their networks up to bulk interception of data; and they can be required to modify their technologies to make the interception of data easier, even to the extent of removing "electronic protections" applied to them.

That last requirement is what's most concerning for tech companies, since it seems to imply that the government may start asking them to rewrite their apps to remove encryption - or, at least, to alter the way the cryptosystems work so that the technology firms themselves can snoop on their customers' messages.

It's prompted a rare intervention in British politics from Apple chief executive Tim Cook, who said on Monday that the company "believes very strongly in end to end encryption".

Cook added that "if you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things. It's the good people. The other people know where to go".

But the government was adamant in the lead-up to the bill's introduction that it wouldn't be attacking encryption, so why are the tech companies now concerned? The reason seems to be a couple of sleights-of-hand.

The first is that the requirement that telecommunications operators weaken their own encryption if asked to do so - known as a "technical capability order" - is already in British law in the Regulation of Investigatory Powers Act 2000. The government has thus positioned the clause in the investigatory powers bill as a mere continuation of that power, albeit one written into legislation for the first time.

But that's disingenuous. The RIPA power, crucially, works with a very different definition of "telecommunications operator". Under RIPA you have to provide telecommunications services, meaning that internet service providers, mobile carriers, and the like are covered, but tech companies aren't. RIPA was drafted four years before the launch of Gmail, let alone messaging applications such as iMessage and WhatsApp.

The tech companies warn that the new bill has a wider definition of telecommunications operator which covers companies like Apple and Facebook, as well as the old ISPs. Amongst the carefully redrafted legislation, for instance, the phrase "public telecommunications service" has been replaced with "telecommunications service".

The second issue is how the government has managed its messaging on encryption.

In the House of Lords, Baroness Shields was clear: "The government recognise the essential role that strong encryption plays in enabling the protection of sensitive personal data and securing online communications and transactions. The government do not advocate or require the provision of a back-door key or support arbitrarily weakening the security of internet applications and services in such a way".

But that's not the whole picture. While the government is fine with encryption between an individual and a company, which can be hit with a warrant, it isn't so happy about encryption between two individuals which can't be decrypted by a middleman.

Hence the technical capability orders. If a company is offering this sort of encryption - known as "end-to-end" encryption, because the message is encrypted from one endpoint to the other - the government reserves the right to order that company to rebuild its systems to enable eavesdropping.
Those orders can apply to any company, even one based in a country other than the UK, and can mandate changes to equipment in or out of Britain. Ultimately, if the order isn't carried out, the penalties rise to "fine and imprisonment" if the court sees proper.

So what will happen if the government does decide to mandate a technology company to remove its end-to-end encryption?

Initially, a long and ugly legal battle. Whichever company decides to go to bat first would be arguing on two fronts: firstly, trying to claim that the law doesn't apply to them in the first place, by focusing on the contested definition of telecommunications service provider; secondly by trying to argue that the request doesn't fulfil the terms of the law anyway.

One defence they have is that the law limits requests to those that are "reasonably practicable". Whether a tech company considers the request to remove end-to-end encryption "reasonably practicable" depends on who you speak to: one tech insider told me that it would be an easy victory, because if the users hold the encryption keys, there's no way it can be reasonable to demand the company breaks encryption they can't decrypt; but another insider was less hopeful that such an argument would be victorious.

If the rebuttals fail, then any tech company would be faced with a nasty proposition: either a very public climbdown from previous promises to offer end-to-end encryption, or a partial or total withdrawal of encrypted services in Britain - or the prospect of the company's most senior executives facing fines or imprisonment.

Popular services that use end-to-end encryption include Apple's messaging service, iMessage, and the Facebook-owned WhatsApp. But other tools, from PGP to Tor, offer the same security in a package that is nearly impossible for the government to crack down on. As a result, the services you and I use could be caught in the crossfire by an investigatory powers bill that will do nothing to stop the bad guys - whoever they may be.

Edward Snowden urges professionals to encrypt client communications
Why appeasing governments over encryption will never work

LOAD-DATE: November 10, 2015
LANGUAGE: ENGLISH
PUBLICATION-TYPE: Newspaper
JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc.
All Rights Reserved

Return to List

72 of 104 DOCUMENTS

Independent.co.uk

November 11, 2015 Wednesday 10:06 AM GMT

Theresa May's proposed spying law is 'worse than scary' United Nations says;
Thedraft Investigatory Powers Bill would give the Government sweeping new spying powers

BYLINE: Jon Stone
SECTION: UK POLITICS
Theresa May's proposed surveillance and spying laws are "worse than scary", the United Nations' privacy chief has said.

Joseph Cannataci, the UN's special rapporteur on privacy, said the draft Investigatory Powers Bill heralded a "golden age of surveillance" unlike any that had come before.

The draft law, published by the Home Secretary earlier this month, would require internet companies to hand over any and all of their users' communications as required by authorities.

Wikipedia founder urges Apple to stop selling iPhone in UK over law

Other provisions in the bill require the visited websites of all users to be stored on record for a year.

Technical experts have said that the proposed rules on intercepting communications could lead to some services like WhatsApp and iMessage to be de-facto banned because their secure encryption makes it impossible for their host companies to read users' messages.

The Government says it is not making encryption illegal, only "strong" encryption that actually does its job of making communications uninterceptable.

It also claims judge-led reviews of ministerial decisions to use the powers would provide adequate oversight of the Government's spying.

"The snoopers' charter in the UK is just a bit worse than scary, isn't it," Mr Cannataci told the Internet Governance Forum in Brazil, in comments reported by Wired UK.

Mr Cannataci accused the British Government of an "orchestrated" propaganda campaign through its allies in the media to get the law passed with public consent.

"We're now at the stage where for the first time we have an absolute offensive," he said.

Five things you need to know about the 'Snooper's Charter'
Concessions to surveillance bill unlikely to head off peer revolt
Surveillance plans 'could put citizens, economy and internet at risk'

"Just do a media analysis of the way the British establishment is trotting out news about the law and the need for the law and ask yourselves the question 'If this is not orchestrated then what is?'"

A previous attempt at passing powerful laws to allow authorities to intercept communications data was blocked by the Liberal Democrats in the previous 2010 coalition government.

Labour says the bill should have more safeguards and oversight but has not come out strongly against it.

The intervention from Mr Cannataci is not the first time the Government has provoked the ire of the UK.

The international organisation is reportedly launching an investigation into human rights violations in the disability benefits system, and has previously criticised the UK's 'xenophobic' approach to migration and refugee policy.

LOAD-DATE: November 11, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI

Copyright 2015 Independent Digital News and Media Limited
All Rights Reserved
Theresa May's *Snooper* Tax could make broadband bills skyrocket; The cost of storing everyone's browsing history for a year will be way more than the Government has prepared for

**BYLINE:** By Mikey Smith

**SECTION:** NEWS, UK NEWS

**LENGTH:** 369 words

Broadband bills will go up to pay for the "massive cost" of implementing Theresa May's *snooper's* charter, MPs have been warned.

Internet companies told a committee of MPs storing every person's internet history for a year is likely to cost them far more than the government has budgeted for.

The Government has set aside £175m to subsidise companies who have to store the massive amounts of data required.

But experts say that's a fraction of what the true cost will be.

Matthew Hare, chief executive of internet service provider (ISP) Gigaclear told the Commons science and technology committee the amount of data they would need to store is phenomenal.

He said: "On a typical 1 gigabit connection we see over 15TB of data per year passing over that connection ... If you say that a proportion of that is going to be the communications data, it's going to be the most massive amount of data that you'd be expected to keep in the future."

"The indiscriminate collection of mass data is going to have a massive cost."

The stark warning comes just days after David Cameron announced plans to introduce a "universal service obligation" for broadband, giving the public a legal right to request an "affordable" connection.

Read more: 7 reasons you should be worried about the Tory *snooper's* charter

The new Communications Data Bill, being pushed through by Theresa May and David Cameron, would force every ISP to store a history of the websites and services every person in the UK has used for 12 months.

They say this information is essential to allow police and security services to operate in the digital age.

But Apple CEO Tim Cook this week warned some measures in the bill would actually help criminals by putting restrictions on the types of encryption that can be used.

In an interview with the Daily Telegraph, Mr Cook said: "To protect people who use any products, you have to encrypt."

"You can just look around and see all the data breaches that are going on."

"These things are becoming more frequent."

"They can not only result in privacy breaches but also security issues."

"We believe very strongly in end-to-end encryption and no back doors."

Would you be happy to pay Theresa May's *Snooper* Tax?

Whatsapp Mirror Politics
Paris terror attacks: Calls for snooper's charter to be rushed through to prevent UK atrocities;
Lord Carlile says the Investigatory Powers Bill should be passed within a month, warning "it could have been London"

BYLINE: By Mikey Smith
SECTION: NEWS, UK NEWS
LENGTH: 445 words

Lord Carlile says Theresa May's Snooper's Charter should be rushed through Parliament within the next month, to prevent terrorist attacks in the UK.

Speaking in the wake of the Paris terror attacks, the Lib Dem peer warned: "It could have been London."

The Investigatory Powers Bill, branded a Snooper's Charter by critics, would force internet companies to store and allow police and security services to access the browsing history of everyone in the country.

David Cameron called the powers "absolutely vital", saying the current holes in the government's ability to spy on citizens allows terrorists a "safe space" to communicate.

Lord Carlile, who served as an Independent Reviewer of Terror Legislation, told Sky News: "This is a subject that's been discussed repeatedly and at great length. The home secretary presented a draft bill which would not become law possibly until the 31st of December 2016.

"My view is that we don't have time to wait. That what is in the bill is for the most part perfectly reasonable, it could pass through parliament within the next three to four weeks if the government decided that should happen, and I believe that the necessary powers need to be on the statute book as quickly as that."

Home Secretary Theresa May presented the draft bill to the House of Commons earlier this month.

It was welcomed by Labour Shadow Home Secretary Andy Burnham, who said it was neither "mass surveillance" nor a "snooper's charter."

But last week he raised concerns that the judicial oversight of the bill was not enough to prevent ministers invading the privacy of innocent citizens.
In a letter to the home secretary, he wrote: "I have now had the opportunity to study your proposals in detail and have taken advice from the shadow justice secretary."

"This has given rise to concerns that the safeguards you are proposing are not as strong as it appeared when they were presented to the Commons."

Should the snooper's charter be rushed through in the wake of the Paris attacks?

"[You] created the impression that both the home secretary and a senior judge would review the evidence. Indeed, you may recall that I asked you in the House about what would happen if there were a difference of opinion between the two.

"On closer inspection of the wording of the bill, it would seem that it does not deliver the strong safeguard that you appeared to be accepting" 

Civil liberties campaigners have raised serious concerns about the bill.

Human rights group Liberty said the bill "contains sweeping new powers for public bodies to track and hack British people's communications - while failing to include the most basic privacy safeguards."

Don't fast-track the new surveillance bill: it needs considered scrutiny;
Lord Carlile's call for the investigatory powers bill to be rushed through parliament in the wake of the Paris attacks is a misjudged knee-jerk reaction

BYLINE: Paul Bernal

SECTION: COMMENT IS FREE

LENGTH: 742 words

Lord Carlile’s call for the investigatory powers bill to be "fast-tracked" through parliament in the wake of the tragic events in Paris was as unsurprising as it was disappointing. It would be far from the first time that laws giving additional powers to the security services were rushed through on a wave of emotion, without an opportunity for proper scrutiny and with far-reaching consequences.

Carlile himself has particular form. He was one of those who advised the coalition government on the ill-fated communications data bill - dubbed by many the "snooper's charter" - and after the killing in
Woolwich of Lee Rigby in 2013 he suggested that the murder should “haunt” Nick Clegg, while proposing pushing the rejected bill through parliament once more.

Related: The surveillance bill is as big a threat to state security as to personal liberty | Simon Jenkins

He tried the same again after the Charlie Hebdo shootings in Paris in January 2015, working with three other peers to add most of the communications data bill as a late-stage amendment to another already complex bill that had already made most of its way through parliament. Carlile may not be an entirely disinterested party here: as revealed in the Guardian two weeks ago, he has earned £400,000 from a consultancy business that he formed in 2012 with ex-Mi6 chief Sir John Scarlett that specialises in the field.

And yet there is very little reason to suggest that the kinds of powers envisaged in either the old communications data bill or the new investigatory powers bill would have had any effect on the events concerned. The men convicted of the murder of Lee Rigby, as well as the Charlie Hebdo shooters, the Boston bombers, the man behind the Sydney siege in 2014 - indeed all the major terrorist attacks in the west in recent years - were already known to the authorities. Though there is very little information to go on about the latest Paris atrocities, the first man named as being involved, Omar Ismail Mostefai, had been identified as a "high priority for radicalisation" by the authorities as long ago as 2010.

It is possible, of course, that mass surveillance played a part in the identification of those involved in all these atrocities - but what we know so far suggests that it was through far more "conventional" means. The Charlie Hebdo shooter Chérif Kouachi, for example, had been on the French authorities' radar for 10 years, having been arrested in 2003 trying to reach Syria to fight the US forces in Iraq. Lee Rigby's murderer Michael Adebolajo had been trained by known radical cleric Omar Bakri Mohammad as long ago as 2003, and was arrested in Kenya in 2010, believed to be planning to train with a militant group associated with al-Qaida. There are similar stories for the perpetrators of all the other atrocities - which suggests that targeted rather than mass surveillance could have worked better.

Andrew Parker, the head of MI5, recently argued that he wanted a "mature debate" over surveillance and he was right. We do need a mature debate. The events of Paris should make that debate even more important - the nature of the threat has been made starkly clear - but should mean that we do it sensibly and rationally. Is this really likely to be the best way forward? Technological specialists suggest otherwise - last week's appearance of industry experts before the parliamentary science and technology committee to discuss the technological aspects of the investigatory powers bill should have been a salutary lesson about rushing legislation through. The issues raised by these experts - whose companies would be responsible for much of the implementation of the bill - were wide-ranging and fundamental.

Related: This snooper's charter makes George Orwell look lacking in vision | Heather Brooke

This is all without even mentioning the civil liberties arguments - and those arguments against mass surveillance should not be dismissed in the light of tragedy either. The discussions need to be had at all levels: efficacy, proportionality, appropriate allocation of resources, intended and unintended consequences all need to be considered.

David Anderson QC, the independent reviewer of terrorism legislation, entitled his far-reaching report into surveillance A Question of Trust. Laws made in haste rarely generate that crucial trust - and are very seldom a good idea. This bill needs time and intelligent debate, not an emotionally charged rush.
Terror attack on British soil 'prevented in the last month'; Security services are understood to have stopped a planned attack in the UK in the last 30 days

BYLINE: By Jack Blanchard

SECTION: NEWS, UK NEWS

LENGTH: 469 words

David Cameron: we have stopped seven terror attacks in last six months

David Cameron has warned a Paris-style attack "could happen" in Britain as it emerged a major UK terror plot has been foiled in the past few weeks.

The Prime Minister urged worried Brits to show "resolve" following the murderous attacks in France but admitted: "It could happen here."

Mr Cameron revealed seven terror plots have been thwarted in the UK this year - almost one every six weeks.

It means another has been foiled in the three weeks since spy chief Andrew Parker warned of "six attempts" in a speech on October 29.

"It's very important we carry on with our lives," Mr Cameron said today, speaking at the G20 summit in Turkey.

"Our freedom depends upon showing resolve and carrying on."

The PM said he would happily take his kids to the England-France football match at Wembley tomorrow night despite the terror threat.

David Cameron WOULD take his kids to see England play France at Wembley

But he made clear Britain should be under no illusions about the scale of threat posed by Islamic State.

"We live in a very, very dangerous world," the PM warned.

"Those attacks in Paris could have happened in Belgium, in Sweden, in Denmark - it could happen here."

Mr Cameron said the mass shootings and bombings in Paris were "the sort of thing we were warned about" by security chiefs, but admitted UK planning would now go "right back to the drawing board".

"We spent a lot of time working out how to respond to this sort of attack," the PM said.

"But whenever anything like this happens you have to go right back to the drawing board ... and work out what more steps you need to do to try to keep yourself safe.

"That's exactly what we're doing right now."

Mr Cameron also said he would "look at the timetable" for his proposed Snooper's Charter which would give spy chiefs draconian new powers to monitor people's email and internet use.

Read more: Calls for Theresa May to expedite snooper's charter in wake of Paris attacks

It is currently due to come in in 2017 but the PM is under pressure to bring it forward.

He also confirmed funding for 1,900 new spies and made clear it is the intelligences agencies who are keeping Britain safe from Islamic State.
"We have been aware of these cells operating in Syria that are radicalising people in our own countries," he said.

"Our security services and intelligence agencies have stopped something like seven attacks in the past six months - albeit attacks planned on a smaller scale."

Government officials confirmed the number of attacks in 2015 has increased from six to seven, but refused to give any details of the latest plot.

Police officers patrol as London's National Gallery and the fountains in Trafalgar Square are illuminated in blue, white and red lights

Cameron considering speedy passage for spy laws; Terror in Paris; Investigatory Powers Bill; Pressure on PM to expedite legislation that gives agencies more power to track terrorism suspects

NEW powers for the security services may be introduced more quickly in the wake of the Paris terrorist attacks, David Cameron has suggested.

Mr Cameron, who is attending the meeting of G20 leaders in Antalya, Turkey, said "we will look at the timetable" for introducing the Investigatory Powers Bill amid calls for it to be "expedited" to ensure the agencies have the powers they need.

However Theresa May, the Home Secretary, insisted that the new powers need "proper scrutiny" from MPs as she suggested that she would resist calls to bring it forward.

She told the Commons: "As you will be aware we do, of course, look at all counter-terrorism legislation and consider and review the necessary timetable for it.
"But I think it is important - this is a significant Bill - I think it is important that it does have proper scrutiny.

"As you say we have put important safeguards and enhanced oversight into this Bill and greater transparency in terms of the powers that the security and intelligence agencies and police and law enforcement have available to them and it's right that it gets the proper scrutiny."

Earlier, Lord Carlile, the former reviewer of counter-terrorism legislation, had said that Britain's security services needed the powers "now more than ever".

He called on the Government to get its the draft Investigatory Powers Bill into law "as soon as possible".

In an article for the Mail on Sunday he said: "I am not arguing for blanket powers for the police and other security agencies to do what they like without oversight, but for speedy confirmation of powers that, responsibly, they have asked for and which they have demonstrated they need."

Lord Carlile said the Bill "gives our spies all the powers they need to fight terrorism" in the modern world.

"I and other politicians want this Bill to be expedited, so that rather than becoming law by the end of 2016, which is the plan, it should become law as soon as possible," he wrote.

"These are extraordinary times. The threat from terrorist attacks emanating from Syria is the highest it has ever been, and we cannot wait for another horrific murder like that of Drummer Lee Rigby before we act."

The Investigatory Powers Bill will give police and the security services access to the internet records of everyone in the UK.

It will also give the authorities the power to hack into people's mobile phones and computers.

Under the legislation, officials will face up to two years in prison if they abuse the new powers.

A new offence is to be created to target public authorities who inappropriately access phone and email records. Local authorities will also be banned from accessing the web histories of members of the public when ministers publish the biggest overhaul of spying laws for 15 years. The power of town hall staff to target phone and email records has been a subject of growing concern for many years, amid accusations of abuse. Officials frequently do use laws designed to combat terrorism and serious crime to crack down on offences such as benefit fraud, rogue traders, scams against the elderly and illegal waste dumping.

Meanwhile, Mrs May said Britain should welcome Syrian refugees with "open arms" as they begin to arrive in this country today. Some 20,000 refugees from Syrian humanitarian camps will be resettled in Britain over the next five years, with the first plane carrying successful applicants due to land in Glasgow today.

Theresa May said both the United Nations and officials at her department were checking the backgrounds of those seeking asylum to ensure they are not terrorists.

'I think it is important - this is a significant Bill - I think it is important that it gets the proper scrutiny'
The Daily Telegraph (London)

November 17, 2015 Tuesday
Edition 1;
Scotland

Cameron considering speeding up passage of spying laws;
Investigatory Powers Bill Pressure on PM to expedite legislation that gives agencies more power to track terrorism suspects

BYLINE: Steven Swinford

SECTION: NEWS; Pg. 12,13

LENGTH: 704 words

NEW powers for the security services may be introduced more quickly in the wake of the Paris terrorist attacks, David Cameron has suggested.

Mr Cameron said "we will look at the timetable" for introducing the Investigatory Powers Bill amid calls for it to be "expedited" to ensure the agencies have the powers they need.

However Theresa May, the Home Secretary, insisted that the new powers need "proper scrutiny" from MPs as she suggested that she would resist calls to bring it forward.

She told the Commons: "As you will be aware we do, of course, look at all counter-terrorism legislation and consider and review the necessary timetable for it. But I think it is important - this is a significant Bill - I think it is important that it does have proper scrutiny."

"As you say we have put important safeguards and enhanced oversight into this Bill and greater transparency in terms of the powers that the security and intelligence agencies and police and law enforcement have available to them and it's right that it gets the proper scrutiny."

Earlier, Lord Carlile, the former reviewer of counter-terrorism legislation, had said that Britain's security services needed the powers "now more than ever".

He called on the Government to get its recently published draft Investigatory Powers Bill into law "as soon as possible". In an article for The Mail on Sunday he said: "I am not arguing for blanket powers for the police and other security agencies to do what they like without oversight, but for speedy con-firmation of powers that, responsibly, they have asked for and which they have demonstrated they need."

Lord Carlile said the Bill "gives our spies all the powers they need to fight terrorism" in the modern world.

"I and other politicians want this Bill to be expedited, so that rather than becoming law by the end of 2016, which is the plan, it should become law as soon as possible," he wrote.

"These are extraordinary times. The threat from terrorist attacks emanating from Syria is the highest it has ever been, and we cannot wait for another horrific murder like that of Drummer Lee Rigby before we act."

The Investigatory Powers Bill will give police and the security services access to the internet records of everyone in the UK.

It will also give the authorities the power to hack into people's mobile phones and computers.

Under the legislation, officials will face up to two years in prison if they abuse the new powers.

A new offence is to be created to target public authorities who inappropriately access phone and email records. Local authorities will also be banned from accessing the web histories of members of the public when ministers publish the biggest overhaul of spying MCGOWAN JOHN laws for 15 years.
The power of town hall staff to target phone and email records has been a subject of growing concern for many years, amid accusations of abuse.

Meanwhile, Mrs May said Britain should welcome Syrian refugees with "open arms" as they begin to arrive in the country today.

Some 20,000 refugees from Syrian humanitarian camps will be resettled in Britain over the next five years.

She said that the United Nations and officials at her department were checking the backgrounds of those seeking asylum.

Shoot to kill Corbyn against deadly force to end atrocity

Jeremy Corbyn has said he is opposed to letting Britain's security services adopt a "shoot-to-kill policy" if terrorists are loose in the UK in the wake of the Paris attacks.

The Labour leader said he was "not happy" with the idea of immediate and deadly force being used to bring an atrocity to an end, claiming it would bring "war" to Britain's streets.

His comments drew a backlash from shadow ministers, who said his remarks " and that he is "out of touch" with reality.

At a meeting of the parliamentary Labour Party last night, Mr Corbyn was shouted down by his own MPs over his comments. They banged the desks as they questioned the leader over his comments.

Mr Corbyn, a lifelong anti-war campaigner, also said he would deny his MPs a free vote on military intervention in Syria. The move is likely to lead to a significant rebellion.

'I think it is important - this is a significant Bill - I think it is important that it gets the proper scrutiny'

LOAD-DATE: November 17, 2015
LANGUAGE: ENGLISH

GRAPHIC: David Cameron and Vladimir Putin at the G20 meeting in Turkey

Protesters in Monkton, Ayrshire, who oppose Scotland taking in Syrian refugees

JOHN MCGOWAN

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: DTL

Copyright 2015 Telegraph Media Group Limited
All Rights Reserved

Return to List

79 of 104 DOCUMENTS

telegraph.co.uk

November 17, 2015 Tuesday 9:57 PM GMT

The Paris attackers' savage affront to the Western way of life cries out for vengeance;
This act of butchery in our cafes and nightclubs proves that Europe is facing an enemy from within - Cameron must act drastically like the British people want him to

BYLINE: By Allison Pearson

LENGTH: 1037 words
How cruel that one of the worst images from the past few days is also the happiest. A jubilant crowd of young faces waves and gestures at the camera, some even raise a glass to the unseen photographer.

They appear to be lit from within, glowing with the radiance that comes as a free gift with youth. All of them were out on a Friday night in the capital city of the country that gave the world joie de vivre: a relish for life, an exultation of spirit. Minutes after the picture was taken, its opposite was unleashed by people whose business is joie de mourir. The haters of pleasure, the bringers of death. Enter monsters, stage left.

After they had murdered 89 people at the Bataclan concert hall, Isis issued a statement explaining their choice of target. Bataclan, it said, was where "hundreds of pagans gathered for a concert of prostitution and vice". Where do you begin with idiots who think like that? It's preposterous, crazy, laughable.

Yet, according to one survivor, those same idiots stalked the concert hall shooting every third person lying on the floor. Imagine playing a game of Statues as though your life depended on it, because it does.

If some faces in the photograph look familiar, it's because we have seen them over the past few days in the montage of the dead. A bearded British guy, the one raising the beer, lay very still on top of his French girlfriend, trying to shield her. Others were slaughtered around them, but that couple lived, for some reason. For no reason. Another man reported that the jihadists kicked the bodies to check if they were alive. He survived because they kicked his prosthetic leg.

"I feel desperately sorry for Syrians fleeing the monsters in their own country, only to arrive in a new land where they themselves are regarded as potential monsters"

Laurent Lafont-Battesti is alive because he went upstairs at Bataclan. "Everyone who was older wanted to sit on the balcony and leave the dancing downstairs to the young," he told the BBC. So the more mature people tended to live because they preferred to sit down, and the young who were full of joie de vivre and wanted to dance, generally, they died.

It's worth dwelling on the fear and the suffering of the victims, I think, because the authorities and the media try to shift the focus elsewhere as soon as possible; to solidarity and strength, to singing La Marseillaise. In the backlash, too often we lose the sting of the lash itself. If we could only see the unexpurgated pictures inside Bataclan, that human abbatoir, then we would be enraged. And rage would definitely be the correct reaction.

This butchery of innocents, this savage affront to the Western way of life, to music, to young men and women being equal and holding hands in the street, to celebrating a birthday with friends and a bottle of wine around a café table. It cries out for vengeance, not some plonker who set up a portable piano and tinkled Imagine to credulous reporters. Not votive candles and wishful thinking about the brotherhood of man.

Those who dared to point out that letting hundreds of thousands of unchecked Muslims into the European Union might not be such a clever idea just at the moment were shouted down in the usual way. "Exploiting tragedy for political purposes!" Really? Because you lock the door of your house, it doesn't mean you hate the people outside; it just means you love the people inside more.

I feel desperately sorry for Syrians fleeing the monsters in their own country, only to arrive in a new land where they themselves are regarded as potential monsters. I feel even more sorry for my fellow Britons who find themselves sharing their homeland with an enemy within, whom it's considered impolite to mention.

Every time I have a conversation with Jewish friends about whether it's safe for them to stay in the UK, I curse our political classes for their cowardice in not tackling the failures of Muslim integration. For allowing a parallel value system to flourish alongside our own. For permitting schools to make little girls cover up and be taught separately. For tolerating Abu Hamza and Anjem Choudhary, those preachers of hate, for so long.

"Maybe those civil libertarians who veto greater surveillance powers will think about 129 lives that might have been saved if there had been a Snooper's Charter"

According to the Prime Minister, seven attacks by jihadists have been thwarted here in the past 12 months. Undoubtedly, we owe a huge debt of gratitude to our superb security services, but how can
they realistically be expected to keep tabs on hundreds of jihadists who are at liberty to return from Syria and Iraq to our streets?

Quoting a defiant, wartime Churchill, David Cameron urged the British people to channel the Blitz spirit. Say what you like about Winston Churchill, it's unlikely he would have offered jihadists a chance to learn reflexology on some "rehab programme", as the present government has done. Nor would he have talked bafflingly about "counter-narratives" and promised criminal investigations and prosecutions that never materialised.

Maybe the Paris massacre of Friday the 13th will change all that. Maybe those civil libertarians who veto greater surveillance powers will think about 129 lives that might have been saved if there had been a Snoopers Charter; might, in fact, grasp that "snooping" online is one of the precious few ways we have of thwarting attacks.

Maybe the House of Commons will vote for the RAF to bomb Isil, instead of sitting around admiring its conscience. Maybe the EU, which just voted through a special measure for France in a few minutes, when it normally takes 18 months to agree on the correct size for a tomato, could actually pull together.

Maybe the Government will jail or drastically curtail the movements of returning jihadists in line with the wishes of the majority of the British people.

Or maybe it will take another Bataclan concert hall right here to teach us that there is no appeasing the pleasure killers. Let us pray not. In the meantime, while the Government and security services press ahead with essential measures, what about the rest of us? What can we do to fight the hate? Easy. Let’s face the music and dance.

LOAD-DATE: November 17, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDTNS

The horrific attacks in Paris mean that the people there have now had a personal experience of what has been daily life for those comprising the great tide of humanity on their desperate journey to what they hope will be a safe future.

While there is the danger that refugees will be regarded with fear and hostility, it is to be hoped that the reverse will be true. In all the shock and fear of the past few days, Parisians might pause to give thanks that this is only a brief episode, and consider what it must be like to live in terror every day. They are not being bombed by their own government, they have homes and jobs, with warmth and
food and normal life. Hopefully this will bring a better understanding and a feeling of compassion and solidarity with those who have endured so much and now need respite from suffering.

Now it is up to governments to accept that the refugees need a massive effort involving resources and imagination to help them become a productive, secure new sector of European society, where they can make the most of their potential for the good of all. Many will want to return to their own countries when they are able, and need to form a good foundation for stability when they do. They need our help, and we will reap the rewards if we offer it with kindness and generosity.

Sierra Hutton-Wilson
Evercreech, Somerset

The flow of refugees is anathema to Daesh [Isis], undermining its message that its self-styled caliphate is a refuge. It has repeatedly put out messages to refugees ranging from pleading to warnings to threats. In just four days in September it released a dozen videos aimed at people fleeing Syria.

Roy Isserlis
Ormiston, East Lothian

The award-winning film
The Class
about school life in multi-ethnic Paris, gives clues about how a terrorist can be formed. In the film a Malian boy, Souleymane, gets into a fight with his teacher. Souleymane has to attend a disciplinary hearing with his mother. His mother is very apologetic. However, the school expels him and he returns to Mali. We don't learn what happens to Souleymane. Whether young men turn to violence or not, depends a lot on how they are treated by schools and other institutions.

Shouvik Datta
Bromley, Kent

Austerity measures are cutting our defence, security and police forces to the bone. The emergency services, which would have to deal with the carnage that follows an attack such as that seen in Paris, are overstretched, under-resourced and undervalued.

It should be apparent to all that a low tax, small-government mentality is not going to enhance the defence or security of this nation. A government that really cared would put the safety of the people first and make sure that everybody contributed to the cost according to their means. Wearing a poppy, kneeling to the Queen and sabre-rattling merely give the appearance of patriotism.

Alan Millington
Beverley, East Yorkshire

After 9/11 we reacted by bombing the Middle East and attacking our own liberties. There are calls to repeat this response. Why do we expect a different outcome?

Fainthearts are calling for a snoopers’ charter. France has a snoopers’ charter. Spying on everybody dilutes intelligence and allows criminals and terrorists to sneak through in the crowd. The answer is targeted surveillance not blanket snooping.

Barry Tighe
Woodford Green, Greater London

Tom McTague ("PM warns a strike on UK is highly likely", 15 November) quotes the Stop the War Coalition that “Without decades of intervention by the US and its allies there would have been no ‘war on terror’ and no terrorist attacks in Paris”.

This claim, which has at least partial assent from both Tony Blair and Barack Obama, he finds "inflammatory" - why? Our mourning for Paris is not helped by hiding truth behind a fantasy of our blamelessness.

John Heawood
York

LOAD-DATE: November 22, 2015
The snooper's charter is a danger to us all. A man in the pub told me

BYLINE: Jeremy Clarkson

SECTION: NEWS REVIEW; FEATURES; Pg. 14

LENGTH: 994 words

So you're walking down the street one day when you encounter a young chap with a ready smile and a clipboard. He's conducting a poll, and since you're in no particular hurry, you readily agree to answer his questions.

Of course you do. It's nice to be singled out and asked for your opinion. It makes you feel important. You may even find yourself standing a little taller as the question begins ...

"Does it worry you that deep packet inspection probes could soon be used when communications service providers refuse to submit data, even though it's expected that most would maintain data about users in unencrypted form, from which contact information could readily be separated from content?" At this point Captain Clipboard looks up and, with much gusto, says: "This of course would circumvent SSL encryption during transmission."

So what's your answer? Are you a) very worried about that, b) not worried in the slightest or c) unable to answer because you have absolutely no clue what he's on about? Well, you're in a minority because according to YouGov, which did a poll on this subject, a whopping 71% of people in Britain are very unhappy about the prospect of these deep packet inspection probes snouting about in their ISP's SSL - secure sockets layer - encryption programs.

This is because the actual question was more like: "Are you happy to let policemen rummage about in your emails and your internet browsing history?" Put it like that and everyone who's had a peek at some online sapphic action is going to say: "Whoa there. Just a cotton-picking minute ..."

But now let's translate it another way. "Would you like the police to be able to prevent some kind of terrorist atrocity on the streets of London?" This not only exposes the big problem with opinion polls - you always get the answer you want - but also highlights the dilemma in the current "snooper's charter" debate about individual liberty and freedom and the Big Brother state.

On an individual level none of us wants our thoughts and our dreams and our sexual fantasies to be available to the forces of law and order. But we do want the security services to be able to access the electronic secrets of the weird-beard loner at No 43.
I've been trying to work out where I stand on the issue, and it's not easy because we simply don't know what's possible already. We hear from Tom Clancy and others of his ilk that if you use the word "bomb" or "gun" while on the phone, government-run tape recorders in limestone caves are automatically triggered and will record the rest of your conversation. But is this true? We have no idea.

We're told that shadowy figures can work out exactly where we are on the planet because our mobile phones are trackable even when they're turned off. But are they? Likewise, we have learnt by watching films and television that the security services run a fleet of geo-stationary satellites that can read the sell-by date on a strawberry-flavoured yoghurt. Is this for real? Again, we don't know.

We do know the police can gain access to every text message you've sent - and possibly every email as well - within a certain time frame. But we don't know what kind of permission they need to telephone Vodafone and say: "Hand over the info."

We learnt after the Russian airliner was brought down in Egypt recently that western intelligence agencies were able retrospectively to identify chatter on social media that hinted at an attack. But were they? Or is that just a bit of PR to make us more inclined to support those deep packet inspection probes? This murkiness is of course important. Because if we don't know what our security services can do, then the terrorists don't know either. That's why it's important to keep on filling the internet and the nation's pubs with claims and counterclaims and conspiracy theories.

I sat next to a cybersecurity expert at dinner the other night and he said that if you gave him a laptop and an aerial he could kill any diabetic with a high-tech insulin pump in about 20 minutes. When I asked him about people with pacemakers, he said, "I wouldn't even need the aerial."

Is medical wi-fi security really that lax? I only have his word for it. It is said North Korean agents managed to hack into Sony's emails. And they were using nothing but two beetroot's and some coal. So what can the CIA do with all its cloak-and-dagger hitech wizardry? More? Who knows? Did you know that you can switch someone's phone on without them knowing? Well, you can. Apparently. You send it a text that turns on the microphone. So then you can listen to every word its owner is saying even though the screen is dark and silent.

Certainly it's very easy to hack into an Android phone. Though when I say "certainly", what I mean is "probably". And before iPhone users get all smug, let's not forget what happens when you put your nipples on iCloud. Next thing you know, they're on YouPorn.

Time and again we are told that by far the safest way to hold a conversation in secret is while playing electronic games on a PlayStation. Do you believe that? Or is it a clever scheme dreamt up by Messrs Bond and Bourne to get disaffected Muslim youths to converse openly on a channel that appeals to them and that in actual fact is as secure as a piggy bank? Which brings us back to the so-called snooper's charter. It worries me, if I'm honest, because if the government sets out exactly what's legal and what's not, all the murkiness and subterfuge is gone. This means that Johnny Terrorist can work up a strategy that allows him to remain in the electronic shadows.

Far better, surely, to maintain the mystery. To keep him guessing. To force him to communicate with a pen and paper and a stamp.

Though there is even a danger there, because forcing him to return to the Stone Age is kind of what he wanted in the first place.

This murkiness is of course important. Because if we don't know what our security services can do, then the terrorists don't know either.
Crossword roundup: the all-seeing eye;
A spot more cricket and an old new word for state intrusion in the
best of the cryptic crop

BYLINE: Alan Connor

SECTION: CROSSWORDS

LENGTH: 695 words

The news in clues

Following last week's addition (on the use of cricket lingo) to our Cryptics for Beginners series, here's
a supremely leather-and-willow puzzle from Knut in the Independent.

The surface readings demonstrate some more words that solvers need to remember might have a
sporting sense...

26ac One on board in international trial (4,3) [ an achievement that would be marked on the
scoreboard in a Test match ]

... like the "test" of TEST RUN and...

7d More wide, perhaps (5) [ what a "wide" is an example of ]

... the word EXTRA. The whole puzzle comes highly recommended; even if you're not a cricket buff,
it's witty and it marks an event from September with a supremely personal touch.

Latter patter

Here's a modern phrase, used in a puzzle by Vlad...

25ac Bugged car so there's no privacy from the outset, right - with this (8,7) [ anagram of
CARSOTHERESNO with first letter of "privacy" and abbreviation for "right" ] [ anagram of
CARSOTHERESNOPR ]

... a SNOOPERS' CHARTER. At least I thought it was new. Nowadays, it's used to describe the draft
communications data bill. I became aware of it when it was used to describe its predecessor, the
Regulation of Investigatory Powers Act, back when internet service providers were a little more
robust.

As it turns out though, the phrase goes back at least as far as 1957. Lord Lucas of Chilworth took a
look at the cinematograph films bill, which wanted to levy charges from cinemas to fund British films,
train young people and the like. He spotted a clause which allowed "the Commissioners of Customs
and Excise" to require cinema owners to furnish "returns or other information as may be so specified",
and didn't like what he saw:

I hope the noble lord will do something for me here, because subsection (1) of clause 4 seems to me
to be a 100% snoopers' charter.

And this was merely the prospect of the taxman keeping paper records relating to the business of
 cinema owners. Imagine what Lord Lucas of Chilworth would make of constant surveillance of all our
 communications. This brings us to our next challenge, which is derived from the Greek ?pt????.

If that's not enough to identify the word, it was originally used to describe a wholesome variety of the
peep show that offered views of European capitals; but for Jeremy Bentham, it described his ideal
kind of prison, where all inmates could be seen at all times.

Such a penitentiary was planned for Millbank in 1794; nowadays, there would be no need for a
physical site. Reader, how would you clue PANOPTICON?
The Annotated Alex

Across at Alex Bellos's Monday puzzle, there's a different kind of crossword.

There are no clues. Instead, there's a rule for what form the entries take:

Each of the six vertical and six horizontal entries gives you the number of times a letter is used in the puzzle, and is of the form: [NUMBER][SPACE][LETTER](S)

More details in the puzzle post.

Clueing competition

Thanks for your clues for MANSPLAIN, a new term that doesn't seem to have quite established consensus on what part of speech it is.

I enjoyed a couple of cameos: Peshwari's spooky "Spin Alan around to follow spy chief's talk, specially for women" and DameSweeneyEggblast's lurid "MP in Alan's bizarre male sex lesson".

And for offbeat clueing, there was some misleading spacing from Ojisan with "Tell the little woman about inconsequential stupid plans": just a pair of definitions in jonemm's "Masculine condescension (that means when a man is talking down to you luv)" and Diplotaulobium didn't stray far from the entry in the wordplay of "Ego is evident in man's plan to set her straight".

The runners-up are ID2155366's "Lianna has PMS trouble. Go on - tell her all about it" and TwoDarrinStephens' "A condescending way to describe Sarkozy, perhaps: small and simple"; the winner is Truthl1 (who also offered "The Descent of Man?") with a sneakily forgivable definition-by-example in "Unhelpfully advise Sarah Palin's man to reform".

Clue of the fortnight

Nice concise stuff from Imogen in the Guardian...

22d Ship’s maximum speed, say (6) [ physics symbol for the speed of light + synonym for ‘say’ ] [ C + UTTER ]

... giving CUTTER. Full steam ahead!

Theresa May accused of rushing surveillance bill through back door;
Home secretary gives committee three weeks to study 'snooper's charter', despite having ruled out fast-tracking it after Paris attacks
The home secretary, Theresa May, has been accused of fast-tracking her "snooper's charter" legislation by the back door after giving a scrutiny committee of MPs and peers only three weeks to consider the 299-page bill.

The Commons was asked to approve a timetable requiring the joint committee on the investigatory powers bill to report back by 11 February. The three-week Christmas and new year parliamentary recess means that the committee, which has yet to appoint a chair, will effectively have little more than three weeks to scrutinise the highly complex surveillance legislation and could have as few as three expert witness sessions.

The joint committee that scrutinised the previous "snooper's charter" bill - the draft communications data bill - in 2012 sat for five months and held 13 public witness sessions over a six-week period. It also took evidence in private from the security services.

One member of the committee, Lord Strasburger, tweeted: "Ridiculous. Committee scrutinising massive investigatory powers bill given just 2 weeks to hear witnesses. Govt turning it into rubber stamp."

Alistair Carmichael, the Liberal Democrat home affairs spokesman, said the rushed timetable risked discrediting the committee's work. "This inadequately short timescale makes it clear that despite reassurances from the home secretary in the aftermath of Paris, the government does in fact intend to rush this monumental bill through parliament," he said.

"Proper scrutiny of complex issues requires time and care. The government seems determined to deny the committee both. I hope that members will not allow themselves to be railroaded in this way but will demand the time and resources that they need to produce a report of which they can be proud and in which the rest of us can have confidence."

Privacy campaigners also voiced alarm. Eric King, of the Don't Spy On Us coalition of campaign groups, said: "This timetable is inhospitable to informed consideration of extraordinary powers. It is a fraction of the time previous versions of the snooper's charter received, which had just a fraction of the issues to consider.

"How are the committee to weigh the proportionality of bulk interception powers, the intrusiveness of bulk hacking powers, or scrutinise the evidence base for internet connection records in just a matter of weeks? This is a once-in-a-generation chance to create a world-class legal framework. Rushing to hear evidence before Christmas jeopardises the chance to get it right," he said.

A Home Office spokesperson said: "Yesterday the House of Lords agreed the schedule for the investigatory powers bill joint scrutiny committee with no opposition. The committee has already started work and under the proposals will have two and a half months before reporting on 11 February 2016. It is for the committee to determine how to use the time available."

The home secretary ruled out fast-tracking the bill in the wake of the Paris attacks, telling MPs that it was a significant bill and it was important that it had proper scrutiny.

LOAD-DATE: November 26, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2015 The Guardian, a division of Transcontinental Media Group Inc.
All Rights Reserved

Return to List

84 of 104 DOCUMENTS

251
The home secretary, Theresa May, has been accused of fast-tracking her new "snooper's charter" legislation by the back door, giving a scrutiny committee of MPs and peers only three weeks to consider the 299-page bill.

The Commons was asked to approve a timetable requiring the joint committee on the investigatory powers bill, which will overhaul Britain's surveillance laws in the wake of Edward Snowden's disclosures, to report back by 11 February.

The three-week Christmas and new year parliamentary recess means that the committee, which has yet to appoint a chair, will effectively have little more than three weeks to scrutinise the highly complex surveillance legislation and could have as few as three expert witness sessions.

The joint committee which scrutinised the previous "snooper's charter" bill - the draft communications data bill - in 2012 sat for five months and held 13 public witness sessions over a six-week period and also took evidence in private from the security services.

One member of the committee, Lord Strasburger tweeted: "Ridiculous. Committee scrutinising massive investigatory powers bill given just 2 weeks to hear witnesses. Govt turning it into rubber stamp."

Alistair Carmichael, the Liberal Democrat home affairs spokesman, warned the rushed timetable risked discrediting the committee's work. "This inadequately short timescale makes it clear that despite reassurances from the home secretary in the aftermath of Paris the government do in fact intend to rush this monumental bill through parliament," he said.

"Proper scrutiny of complex issues requires time and care.

"The government seems determined to deny the committee both. I hope that members will not allow themselves to be railroaded in this way but will demand the time and resources that they need to produce a report of which they can be proud and in which the rest of us can have confidence."

Privacy campaigners also voiced alarm. "This timetable is inhospitable to informed consideration of extraordinary powers. It is a fraction of the time previous versions of the snooper's charter received, which had just a fraction of the issues to consider," said Eric King of the Don't Spy on Us coalition of campaign groups.

"How are the committee to weigh the proportionality of bulk interception powers, the intrusiveness of bulk hacking powers, or scrutinise the evidence base for internet connection records in just a matter of weeks? This is a once-in-a-generation chance to create a world-class legal framework. Rushing to hear evidence before Christmas jeopardises the chance to get it right," he said.

The home secretary ruled out fast-tracking the bill in the wake of the Paris attacks telling MPs that it was a significant bill and it was important that it had proper scrutiny.
NEWS that one of the Paris gunmen visited London and Birmingham BEFORE the shootings suggests similar attacks are likely here.

Civil liberty campaigners will protest, but that means GCHQ spooks will need to intercept calls, emails and internet chatter between extremists at home and abroad.

Police have given phone-tapping a shockingly bad name. But I know who I'd choose between Scotland Yard snoopers and the spies who are there to protect us.

NEWS that one of the Paris gunmen visited London and Birmingham BEFORE the shootings suggests similar attacks are likely here. Civil liberty campaigners will protest, but that means GCHQ spooks will need to intercept calls, emails and internet chatter between extremists at home and abroad. Police have given phone-tapping a shockingly bad name. But I know who I'd choose between Scotland Yard snoopers and the spies who are there to protect us. EU we we was But Theresa The only to Cameron
Wi-Fi Barbie doll 'could be used as spy weapon by the government';
Internet-connected toys would be permitted targets under the proposed 'Snooper's Charter', experts told a House of Commons committee

BYLINE: By Jack Blanchard

Spies could use draconian new powers to hack into children's toys and snoop into suspect's homes, MPs have been warned.

Internet-connected toys like 'Hello Barbie' would be permitted targets for the security services under the proposed 'Snooper's Charter', experts told a House of Commons committee.

The draconian set of laws would give online spooks the power to force manufacturers help them hack into internet-connected "equipment".

Ministers say they need the power to hack into the phones and computers of terror suspects.

But Antony Walker, of industry body techUK, said more and more products from cars to kids' toys are now being hooked up to the internet - and would also be covered by the sweeping new law.

"The definition of 'equipment' would seem to apply to a huge range of devices," he said.

Last week hackers claimed to have found 'vulnerabilities' in the new 'Hello Barbie' doll, billed as the world's first interactive 'smart doll'.

The toy connects to the internet to answer kids' questions and has a microphone to record a child's speech on a remote 'cloud' server.

"A range of devices that have been in the news recently, in relation to a hack, are children's toys, that children can interact with," Mr Walker told the Commons science committee.

"These are devices that may sit in a child's bedroom but are accessible.

"In theory, the manufacturer of those products could be the subject of a warrant (from the security services) to enable equipment interference with those devices."

Read more: JD Wetherspoon cyber attack exposes details of 650k punters

Mr Walker said the spooks' new hacking powers could extend to almost any household device, as more and more gadgets - from smart TVs to smart fridges - become hooked up to the internet.

He begged MPs to carefully consider exactly where the line should be drawn before the Snooper's Charter becomes law.

"The potential extent is something that needs to be carefully considered when we start to think about not just the world today, but the world in five or 10 years' time," he said.

His warning follows comments last week by a senior intelligence official who admitted a "variety of equipment" could be covered by the new hacking law.

Would you let your child play with an online Barbie?

Lewis Neal, director of intelligence policy at the Foreign Office, told MPs: "'Equipment interference' is a range of techniques to acquire communication information from a variety of bits of equipment, from computers to mobile phones."

It is just the latest warning about the scope of the new package of snooping laws - officially titled the Investigatory Powers Bill - drawn up by Home Secretary Theresa May.
Cameron warns SNP on snooping vote

BYLINE: Simon Johnson

SECTION: NEWS; Pg. 2

LENGTH: 501 words

THE Prime Minister will today warn Nicola Sturgeon that she will endanger lives if she allows SNP MPs to fight the "snoopers' charter" which gives police and intelligence agencies more powers to monitor terrorists online.

Speaking before talks with the Scottish First Minister at Downing Street, David Cameron said he wanted crossparty support for the Investigatory Powers Bill.

Mr Cameron warned that Islamic State of Iraq and the Levant (Isil), poses a "very direct threat to our country and our way of life" and that terrorists cannot be given "safe spaces" in which to communicate on the internet. He said he wanted to ensure that the Government and the three devolved administrations are cooperating as effectively as possible to tackle terrorism.

But Ms Sturgeon refused to give any hint as to whether her party will support the legislation, merely stating that the meeting was an "important opportunity" for them to discuss how to work together more closely. She instead focused on the financial arrangements that will accompany the new tax powers being devolved to Holyrood. The Investigatory Powers Bill would compel communications companies to help spies hack into suspects' smartphones and computers. Internet and phone companies will also have to retain customer usage data for a year.

It would protect the ability of GCHQ and MI5 to bulk collect communications data and to hack into a suspect's electronic devices. It would also enshrine the power of ministers to sign off warrants for intrusive surveillance.

SNP MPs, who voted against air strikes on Syria, have expressed scepticism about whether the powers are "proportionate" to the threat, but have promised to carefully consider them.
Mr Cameron said: "We know Daesh (Isil) pose a very direct threat to our country and our way of life. That threat applies across the UK and so it is essential that the UK Government and the governments of our devolved nations cooperate in the most effective way.

"We are looking at a number of issues, including the use of intelligence information, and we also need to ensure cooperation at a legislative level." He concluded: "We cannot afford to give terrorists safe spaces in which to communicate and we must give the police and security services the tools they need to keep us safe in the 21st century. I am hopeful that when we debate the Investigatory Powers Bill in the new year, we can achieve cross-party support for these fundamental concepts."

He said Westminster and the Scottish Government were committed to getting a "good deal for Scotland" on the financial framework that will accompany Holyrood's new powers but it must also be "fair to the rest of the UK". The negotiations centre on the mechanism for calculating the change to Scotland's block grant from Westminster to offset Holyrood getting control over income tax and an array of benefits. Ms Sturgeon has previously warned she would rather veto the new powers than accept a deal that could potentially leave Scotland worse off in future.

LOAD-DATE: December 14, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: DTL

SNP 'risks lives on snoopers' law';
David Cameron to tell First Minister that opposition to new interception powers will put the UK in danger

BYLINE: Simon Johnson

SECTION: NEWS; FRONT PAGE; Pg. 1

LENGTH: 598 words

NICOLA STURGEON will today be warned by the Prime Minister that she will endanger lives if she allows her MPs to fight the "snoopers' charter", which gives police and intelligence agencies more powers to monitor terrorists online.

David Cameron, speaking ahead of talks with the First Minister at Downing Street, said he wanted cross-party support for the Investigatory Powers Bill when it is debated in the new year.

Islamic State of Iraq and the Levant (Isil), poses a "very direct threat to our country and our way of life" and terrorists cannot be given "safe spaces" in which to communicate, he said.

Mr Cameron also said he wanted to ensure that the Government and the UK’s three devolved administrations are cooperating as effectively as possible to tackle terrorism.
But Ms Sturgeon refused to give any hint as to whether her party would support the legislation, merely stating that the meeting was an "important opportunity" for them to discuss how to work together more closely. She instead focused on attacking the Trade Union Bill and calling for a "fair deal" for Scotland regarding the financial arrangements that will accompany the swathe of new tax powers being devolved to Holyrood.

Speaking ahead of the meeting, she said: "Today is not about agreeing a final deal but I hope we can make significant progress in agreeing that deal must be a fair one."

She warned it would be an "unacceptable step" to "impose" the Trade Union Bill on Scotland, arguing there was "clear opposition" across Scottish society and the Holyrood chamber to its proposals for curbing the right to strike.

The Investigatory Powers Bill would compel communications companies to help spies hack into suspects' smartphones and computers. Internet and phone firms would also have to retain customer usage data for a year.

It would protect the ability of GCHQ and MI5 to bulk collect communications data and to hack into a suspect's electronic devices and would enshrine the power of ministers to sign off warrants for intrusive surveillance. Nationalist MPs, who voted against air strikes on Syria, have previously expressed scepticism about whether the powers are "proportionate" to the threat faced but have promised to carefully consider them.

Mr Cameron said: "We know that Daesh (Isil) pose a very direct threat to our country and our way of life. That threat applies across the UK and so it is essential that the UK Government and the governments of our devolved nations cooperate in the most effective way.

"We are looking at a number of issues, including the use of intelligence information, and we also need to ensure cooperation at a legislative level." He concluded that: "We cannot afford to give terrorists safe spaces in which to communicate and we must give the police and security services the tools they need to keep us safe in the 21st century.

"I am hopeful that when we debate the Investigatory Powers Bill in the new year we can achieve cross-party support for these fundamental concepts."

He said Westminster and the Scottish Government are committed to getting a "good deal for Scotland" on the financial framework that will accompany Holyrood's new powers but it must be "fair to the rest of the UK, and built to last". The negotiations centre on the mechanism for calculating the change to Scotland's block grant from Westminster to offset Holyrood getting control over income tax and an array of benefits.

Ms Sturgeon has previously warned that she would rather veto the new powers than accept a deal that could potentially leave Scotland hundreds of billions of pounds worse off in future.
Prime Minister welcomes Scottish First Minister for talks at Number 10
Cameron will warn Scotland is not immune from global terror threats
Sturgeon urged to back controversial new spy laws to take on fanatics

Nicola Sturgeon looked delighted to be in Downing Street this evening as she arrived for key talks with David Cameron.

The First Minister posed outside the door of Number 10 before a meeting where the Prime Minister will call on his SNP rival not to be soft on terrorists and back his controversial new spy laws.

The talks on the so-called Snooper's Charter came just weeks after the SNP voted against the aerial bombardment of Syria.

In their first meeting since May the First Minister will demand that the Prime Minister devolve more powers on tax and welfare to Scotland.

Tonight Mr Cameron will warn the First Minister that Scotland is not immune from global threats.

Mr Cameron will make the case for the SNP to back the Investigatory Powers bill, which would give unprecedented access to the security services and police over emails and internet communications.

A meeting between both leaders comes just weeks after the SNP became the only party to whip its MPs to vote against the aerial bombardment of Syria.

Number 10 said the pair would discuss how Westminster and the Scottish Government could cooperate on security and intelligence matters.

Downing Street said it was vital that people in Scotland were 'protected equally from the threat of Daesh-inspired extremism'.

Ahead of the meeting, Mr Cameron said: 'We know that Daesh (ISIS) pose a very direct threat to our country and our way of life.

'That threat applies across the UK and so it is essential that the UK Government and the governments of our devolved nations co-operate in the most effective way.

'We are looking at a number of issues, including the use of intelligence information, and we also need to ensure co-operation at a legislative level as well

In remarks that infuriated the SNP, he added: 'We cannot afford to give terrorists safe spaces in which to communicate and we must give the police and security services the tools they need to keep us safe in the 21st century.

'I am hopeful that when we debate the Investigatory Powers Bill in the New Year, we can achieve cross-party support for these fundamental concepts.'

A senior SNP source said the remarks were 'curious' as the SNP always supported the police and security services.

'It is an odd way to make friends and influence people via megaphone diplomacy. It says more about the Prime Minister being worried about his tiny majority.

'We have always been very supportive of the police and security services but have said it is vital to get the law right.'

Another source said: 'At no point have we given the impression we are weak on security. We have been broadly supportive of the principles behind the Investigatory Powers Bill provided there is proper judicial oversight.'
In contrast to the PM's warning on security, a statement released before the meeting by Miss Sturgeon struck a more conciliatory tone about fighting the threat of terrorism together.

She said today's meeting would be 'an important opportunity for the PM and I to discuss how our governments can work ever more closely together to help combat the threat posed by international terrorism'.

Miss Sturgeon did, however, warn the Scottish Government would oppose the introduction of the Trade Union bill in Scotland, which would impose new thresholds for strike ballots and restrictions on picketing.

She said: 'The number of days lost to strike action have been reduced in Scotland by 84 per cent through partnership working, not by slapping sanctions on workers.

'To impose this bill on Scotland would be an unacceptable step and I will make that clear to the Prime Minister.'

The First Minister will also raise the ongoing row over the cash settlement for the new Scotland Bill. This would require Scotland's block grant from Westminster to be cut by the proportionate amount once tax and welfare powers are devolved.

She will tell the Prime Minister that Scots would not accept losing hundreds of millions of pounds a year.

'It is absolutely crucial that future Scottish Governments can use the new tax and spending powers, to create a fairer society and grow the economy, without losing out,' she said.

Mr Cameron said ahead of the meeting that any new fiscal deal 'must be fair to Scotland, fair to the rest of the UK and built to last'.
David Cameron will today warn Nicola Sturgeon she will endanger Britons' lives if she allows SNP MPs to fight the 'snoopers' charter' giving the police and intelligence agencies more powers to monitor terrorists online.

Speaking ahead of face-to-face talks with the Scottish First Minister at Downing Street, Mr Cameron said he wanted cross-party support for the Investigatory Powers Bill when it is debated in the Commons in the New Year.

The Prime Minister warned that Daesh, otherwise known as Islamic State, poses a "very direct threat to our country and our way of life" and that terrorists cannot be given "safe spaces" in which to communicate on the Internet.

He also said he wanted to ensure the Government and the UK's three devolved administrations are cooperating as effectively as possible to tackle terrorism.

But Ms Sturgeon refused to give any hint as to whether her party will support the legislation, merely stating that the meeting was an "important opportunity" for them to discuss how to work together more closely.

She instead focused on attacking the Trade Union Bill and calling for a "fair deal" for Scotland on the financial arrangements that will accompany the swathe of new tax powers being devolved to Holyrood.

The Investigatory Powers Bill would compel communications companies to help spies hack into suspects' smartphones and computers. Internet and phone firms will also have to retain customer usage data for a year.

It would protect the ability of GCHQ and MI5 to bulk collect communications data and to hack into a suspect's electronic devices, and the power of ministers to sign off warrants for intrusive surveillance.

SNP MPs, who voted against air strikes on Syria, have previously expressed scepticism about whether the powers are "proportionate" to the threat faced but have promised to carefully consider them.

Mr Cameron said: "We know that Daesh pose a very direct threat to our country and our way of life. That threat applies across the UK and so it is essential that the UK Government and the governments of our devolved nations cooperate in the most effective way.

"We are looking at a number of issues, including the use of intelligence information, and we also need to ensure cooperation at a legislative level as well."

The Prime Minister concluded: "We cannot afford to give terrorists safe spaces in which to communicate and we must give the police and security services the tools they need to keep us safe in the 21st century. I am hopeful that when we debate the Investigatory Powers Bill in the new year, we can achieve cross-party support for these fundamental concepts."

He said the UK and Scottish Governments are committed to getting a "good deal for Scotland" on the financial framework that will accompany Holyrood's new powers but it must also be "fair to the rest of the UK, and built to last."

The negotiations centre on the mechanism for calculating the change to Scotland's block grant from Westminster to offset Holyrood getting control over income tax and an array of benefits.

Ms Sturgeon has previously warned that she would rather veto the new powers than accept a deal that could potentially leave Scotland hundreds of billions of pounds worse off in future years.

Speaking ahead of the meeting, she said: "Today is not about agreeing a final deal but I hope we can make significant progress in agreeing that deal must be a fair one."

The First Minister also warned it would be an "unacceptable step" to "impose" the Trade Union Bill on Scotland, arguing there was "clear opposition" across Scottish society and the Holyrood chamber to its proposals for curbing strike rights.
Cameron urges Sturgeon to back 'snoopers' charter'

BYLINE: Hamish Macdonell

SECTION: NEWS; Pg. 5

LENGTH: 519 words

David Cameron will urge Nicola Sturgeon to endorse the UK government's so-called "snoopers' charter" today as he appeals for cross-party unity in the fight against Isis.

The prime minister and the first minister are due to hold one-to-one talks in Downing Street later today and Mr Cameron made it clear last night that security would be top of his agenda.

He has championed legislation which would allow the police to access the internet records of everyone in the UK. It will also give the authorities the power to hack into people's mobile phones and computers.

Labour and the SNP have expressed doubts about the Investigatory Powers Bill - which has been dubbed the "snoopers' charter" - because of its implications for civil liberties.

Mr Cameron said he would bring up the bill with Ms Sturgeon today in the hope that the SNP's 54 MPs could be brought in to support the new powers.

He said: "We know that Daesh pose a very direct threat to our country and our way of life. That threat applies across the UK and so it is essential that the UK government and the governments of our devolved nations co-operate in the most effective way.

"We are looking at a number of issues, including the use of intelligence information, and we also need to ensure co-operation at a legislative level as well."

The prime minister added: "We cannot afford to give terrorists safe spaces in which to communicate and we must give the police and security services the tools they need to keep us safe in the 21st century. I am hopeful that when we debate the Investigatory Powers Bill in the new year, we can achieve cross-party support for these fundamental concepts."

Ms Sturgeon acknowledged that while security would be an important issue for the talks, she would focus both on the UK government's trade union bill, which would restrict the ability of unions to take industrial action, and on the fiscal framework, which underpins the new phase of devolution, due to be introduced next year.

The SNP opposes the trade union crackdown. The first minister said: "To impose this bill on Scotland would be an unacceptable step, and I will make that clear to the prime minister."

The UK and Scottish governments have been trying to reach agreement on a financial formula that will allocate resources to Scotland in the future, after the Scottish parliament gets control of significant tax-raising powers.

So far the talks have not reached a conclusion, with Scottish ministers insisting they will not sign up to any deal that would leave Scotland worse off.
Ms Sturgeon has also stressed that she would make sure the extra devolution powers were defeated in the Scottish parliament if the fiscal framework was not agreed to her satisfaction.

The first minister said: "We need a fair deal for both governments - no more, no less. These considerations are critical - if the financial framework accompanying the new powers is wrong, Scotland could be worse off by hundreds of millions of pounds a year."

And she added: "Today is not about agreeing a final deal but I hope we can make significant progress in agreeing that the deal must be a fair one."

---

Telecoms companies raise questions over cost and feasibility of 'snooper's charter';

BT, Vodafone, 02 Telefonica, EE and 3 tell peers it is not yet possible to determine whether proposals are technically possible

BYLINE: Alan Travis and Owen Bowcott

SECTION: LAW

LENGTH: 762 words

Britain's biggest phone and web companies have raised serious questions over the cost and feasibility of their delivering the government's "snooper's charter" legislation.

Senior figures from BT, Vodafone, 02 Telefonica, EE and 3 have told MPs and peers that the proposals from the home secretary in the draft investigatory powers bill are so technically complex that it is not yet possible to make any meaningful estimate of the costs involved or whether they are technically possible.

Related: Tim Berners-Lee urges Britain to fight 'snooper's charter'

The phone and internet companies' representatives gave evidence on the issues to two parliamentary committees. Their main concerns focus on the Home Office's estimate that new powers requiring the companies to retain internet connection records - simplified versions of everyone's web browsing history - will cost only £174m over the next 10 years.

The government has said it will underwrite all "reasonable" costs involved in introducing, retaining and storing internet connection records for 12 months for access by the police and security services.

But the web companies have voiced strong scepticism of the £174m figure, saying it will prove to be a serious underestimate. They have given a clear warning that it will take at least 18 months - long after
the legislation has reached the statute book - before they know whether it will be technically feasible to retain and store everybody's internet connection records.

Antony Walker of techUK told MPs: "I have met very few people across business who would regard it as a properly robust figure."

Related: The snooper’s charter: one misspelled Google search for 'bong-making' and you'll be in an orange jumpsuit | Frankie Boyle

Mark Hughes, the president of BT Security, said that despite lengthy consultations over the summer, including a round table with Theresa May, there were still many technical complexities to sort out. He told the Commons science and technology committee that it would cost BT alone “many tens of millions of pounds” to implement. BT said in written evidence: “On overall cost we are not yet able to give a meaningful estimate.”

Senior figures from all the phone companies told MPs and peers on the draft bill scrutiny committee that it might be possible to develop the technical capability to collect everyone's internet connection records. "The technology does not exist at the moment ... We are at the feasibility stage and it will take 18 months before we find a solution." They said that until the Home Office could precisely define its requirements it was very difficult to speculate on the feasibility or the costs involved. "You cannot underestimate the complexity,” one senior executive told MPs and peers.

Home Office officials giving evidence said the £174m estimate was the cost over 10 years based on their work with the industry and the historical costs of data collection. They suggested the new powers would be phased in. The officials said: "We would not be able to implement everything in one place, as there is only so much industrial capacity. We would phase it over time."

The Bar Council is to warn that legally privileged conversations between clients and their lawyers will not be protected from eavesdropping and communications surveillance under the new legislation. The organisation, which represents barristers across England and Wales, is due to give evidence in parliament on Wednesday. It will criticise the lack of any statutory provision within the bill covering exchanges between lawyers and their clients, which enjoy a special protected status under the law.

Related: David Cameron, the 'snooper’s charter' will not make us safer

The Bar Council said that providing explicit protection to clients' conversations only in subsidiary codes of practice would be inadequate since codes of practice do not have legal force and can be changed by statutory instrument.

Peter Carter QC, the chair of the Bar Council's surveillance and privacy working group, said: "If the privacy of legally privileged communications is not written into law, then the law will not protect citizens from surveillance when consulting with their legal representatives.

"Under the current draft, security services would be allowed to spy on private communications between clients and their lawyers because protections for legal privilege are not written into the bill. Even when codes of practice come into force, the security services will still be able to listen in, facing only mild sanctions if they fail to follow the right procedures."
Apple calls on UK government to scale back snoopers's charter; Tech company makes rare foray into British politics in a submission to the committee on the investigatory powers bill

BYLINE: Alex Hern

SECTION: TECHNOLOGY

LENGTH: 818 words

Apple has called for changes to the UK government's investigatory powers bill, over fears it would weaken the security of "personal data of millions of law-abiding citizens".

In a submission to the bill committee, released on Monday, the Californian technology firm expressed major concerns and called for wholesale changes before the bill is passed.

"We believe it would be wrong to weaken security for hundreds of millions of law-abiding customers so that it will also be weaker for the very few who pose a threat," Apple said. "In this rapidly evolving cyber-threat environment, companies should remain free to implement strong encryption to protect customers"

The investigatory powers bill was presented to the House of Commons by the home secretary, Theresa May, in November and is currently at the committee stage.

Apple highlighted the main areas of the bill that it wants to see changed. It told the committee that passages in the bill could give the government the power to demand Apple alters the way its messaging service, iMessage, works. The company said this would weaken encryption and enable the security services to eavesdrop on iMessage for the first time.

The government argues that the proposed legislation does no more than incorporate previous powers granted under Ripa, an earlier piece of legislation. However, technology firms fear that key differences in the language used in the legislation widen the scope of the powers considerably when compared to Ripa, which only affected traditional internet service providers.

In its submission, Apple said: "The creation of backdoors and intercept capabilities would weaken the protections built into Apple products and endanger all our customers. A key left under the doormat would not just be there for the good guys. The bad guys would find it too."

Apple also expressed concern over another section of the draft bill, which gives the security services the authority to hack into computers worldwide - enshrining in statute for the first time the government's licence to do so. It contains provisions that require communications firms to provide aid to the security services when they need help to hack into devices, something that Apple is concerned could be read as requiring the company to help hack into its own devices.

"It would place businesses like Apple - whose relationship with customers is in part built on a sense of trust about how data will be handled - in a very difficult position," Apple says.

"For the consumer in, say, Germany, this might represent hacking of their data by an Irish business on behalf of the UK state under a bulk warrant - activity which the provider is not even allowed to confirm or deny. Maintaining trust in such circumstances will be extremely difficult."

Apple said it was worried about the scope of the bill as many of the provisions in the bill apply to companies regardless of where they are based, giving the bill international scope, despite being a purely domestic piece of legislation. It also runs the risk of placing companies in a damned if they do, damned if they don't position

The company said: "Those businesses affected will have to cope with a set of overlapping foreign and domestic laws. When these laws inevitably conflict, the businesses will be left having to arbitrate between them, knowing that in doing so they might risk sanctions. That is an unreasonable position to be placed in."

Others have expressed concern about the precedent such legislation would set - particularly if other countries with worse human rights records than the UK tried to enact similar legislation.
It isn't the first time Apple has spoken out against the IP bill. The week after it was released, the company's chief executive, Tim Cook, told the Daily Telegraph that the law could have "very dire consequences".

He said: "We believe very strongly in end-to-end encryption and no back doors. We don't think people want us to read their messages. We don't feel we have the right to read their emails. "Any back door is a back door for everyone," he added. "Everybody wants to crack down on terrorists. Everybody wants to be secure. The question is how. Opening a back door can have very dire consequences."

Other technology firms have also opposed the bill. In November, the bill committee was told by internet service providers that another aspect of the bill, which requires them to store browsing data for a year, presented a security hazard to the public and could cause broadband bills to rise.

Matthew Hare, the chief executive of ISP Gigaclear, said: "On a typical 1 gigabit connection we see over 15TB of data per year passing over that connection ... If you say that a proportion of that is going to be the communications data, it's going to be the most massive amount of data that you'd be expected to keep in the future.

"The indiscriminate collection of mass data is going to have a massive cost."

Apple criticises Investigatory Powers Bill: Theresa May's spying law could endanger privacy and security, company says; Apple says the powers would make the 'personal data of millions of law abiding citizens [...] less secure'

Apple has launched a scathing attack on the Government's plans to give spies more powers. The company has said in a rare public statement that it believes that Theresa May's Investigatory Powers Bill would make the "personal data of millions of law abiding citizens [...] less secure".

Theresa May's proposed spying law is 'worse than scary' says UN
The Government intends to bring in the Investigatory Powers Bill as soon as possible, to bring new powers to help intelligence agencies and law enforcement to conduct surveillance. But the legislation has been repeatedly criticised for over-reaching, and apparently banning some of the most central parts of modern technology.

Apple argues that the legislation should be re-written to be more clear about how the powers that are contained within it will be used. It made the statement as part of its submission to the joint scrutiny committee for the Investigatory Powers Bill.

"We believe there is a need for much greater clarity as to how the powers in the bill will be applied," Apple's submission reads. "Not least because, once again, the [powers] could endanger the privacy and security of users in the UK and elsewhere."

Apple's criticisms centre around three key parts of the bill.

The first is that it requires that companies can break their own security measures so that messages can be more easily read.

Encryption - which can be found in Apple's iMessage and FaceTime messaging services - uses mathematical techniques to ensure that a message can only be read by the person it was sent to. But parts of the bill seem to suggest that technology should be broken open, so that messages can't be kept from intelligence agencies.

Apple's submission says that the "best minds in the world cannot rewrite the laws of mathematics", and that as a result there is no way of creating methods of encryption that would only give access to the Government or the intelligence agencies.

"The bill threatens to hurt law-abiding citizens in its effort to combat the few bad actors who have a variety of ways to carry out their attacks," Apple's section on encryption argues. "The creation of backdoors and intercept capabilities would weaken the protections built into Apple products and endanger all our customers."

"A key left under the doormat would not just be there for the good guys. The bad guys would find it too."

Apple's second criticism is that the law contains measures that would force companies like Apple to help the government to hack into phones so that information can be taken from them. The company points out that this will "extend responsibility for hacking from Government to the private sector", and that it will undermine trust between technology companies and their users.

Because Apple sends the same version of its software to every user, wherever they are, the company would have to build those hacking and interception capabilities into every phone that it sells. That would mean that the same weaknesses could be used by governments and other bodies across the world, including in areas with much lesser safeguards or less strong human rights records.

Finally, the company objects to the international aspects of the law, which allow it to apply extraterritorially. That means that Apple and other companies will have to abide by the law despite being based elsewhere, potentially putting it into conflict with other local laws.

Apple's Tim Cook has spoken out publicly about safeguards for privacy and security, including comments about the Investigatory Powers Bill made in recent interviews. But the public criticism is an unusual step for the company itself, which has in the past rarely made statements about legislation or policy.

New legislation will have to be passed by the end of 2016, in part because existing laws will run out by the end of next year.

But Apple's primary suggestion is that the bill should be re-written to provide more clarity about the more contested parts of the legislation.
Nearly a quarter of nosy Britons just can't resist looking for their Christmas presents

BYLINE: Geoff Maynard

LENGTH: 499 words

They are meant to be a big surprise - but nearly a quarter of Britons admit to snooping around for their Christmas presents ahead of the big day.

Nearly a quarter of us are determined to spoil our own Christmas surprise

Some 22 per cent of 2,000 people surveyed said they search high and low for their gifts with 87 per cent succeeding in finding them.

The snoopers resort to great lengths to find their festive haul, with 43 per cent going through every cupboard in the house.

They keep their activities undercover with 31 per cent unwrapping and rewrapping a present when they find it. Some even use technology to track down the Christmas treats - 13 per cent check internet browser history, five per cent sneak a look at text, WhatsApp or email messages and five per cent log into the buyer's bank account.

The most common place to hide gifts is in the wardrobe

But with so many spies around, the givers are getting crafty about hiding Christmas presents according to the research from website lastminute.com.

Fifty-three per cent keep the gifts in the wardrobe, 26 per cent hide them under the bed and seven per cent put them in their underwear drawer.

Some opted for less obvious locations, including the dog's bed, the laundry bin, the boot of the car and even inside stuffed toys.

It seems that women are far nosier than men when it comes to hunting down their bounty - 25 per cent compared with 17 per cent - but they are also more likely to get away with it. The number of men getting caught red-handed was 26 per cent.

The North-east has the worst culprits
People in the North-east are the worst culprits with 31 per cent admitting to having a sneaky peek, followed by the Welsh and those in the West Midlands.

All that snooping comes at a cost, with 30 per cent admitting to buying additional gifts because what they were being given was more expensive than what they had bought. And it can be dangerous too.

Six per cent of respondents have got hurt in their hunt for gifts, with East Midlanders causing themselves the most damage.

GETTY

Britons have even injured themselves looking for their Christmas surprises

Britons have bruised themselves, burnt their hair, fallen off a ladder, tripped running towards the tree or needed stitches after a tin fell on their head when spying around in the garage.

But at least the snoopers have a conscience.

The most common feeling after finding presents ahead of the big day was sneaky and naughty, while nine per cent felt disappointed or they had ruined Christmas.

Only eight per cent got a rush of excitement and five per cent felt dishonest.

Related articles Shameless benefits mum of 12 caught with TROLLEY FULL of toys…and YOU'RE paying LAST-MINUTE shopping in busy public places and socialising at parties is a germ HOTBED Buying a teenager a present is hard work says Jennifer Selway

LOAD-DATE: December 22, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDE

UK snooping law won't ban WhatsApp, but could leave your data open to HACKERS

BYLINE: Aaron Brown

LENGTH: 693 words

THE DRAFT Investigatory Powers Bill could help cybercriminals access your data, technology firm Apple has cautioned the UK Government.

GETTY

The Investigatory Powers Bill will not ban WhatsApp, but it could leave customers open to criminals Apple has raised concerns about the Investigatory Powers Bill to a parliamentary committee.

The iPhone manufacturer believes the legislation could weaken the security protecting the personal data of "hundreds of millions of law-abiding citizens."
The Investigatory Powers Bill - currently in its draft stage - could overhaul the rules governing how authorities can snoop on people's communications.

Under proposals outlined by Home Secretary Theresa May, communication firms will be legally required to help spies hack into suspects' smartphones and computers.

One of the biggest and most controversial new powers afforded in the bill will force broadband firms to hold basic details of every service and website you have accessed online.

GETTY

Apple CEO Tim Cook has warned the Investigatory Powers Bill would leave Britons vulnerable

GETTY

The Investigatory Powers Bill is a watered down edit of an earlier draft, dubbed Snoopers' Charter

"It will provide the strongest safeguards and world-leading oversight arrangements," Theresa May told parliament.

"And it will give the men and women of our security and intelligence agencies and our law enforcement agencies ... the powers they need to protect our country."

But Californian technology firm Apple is believed to have passed on its thoughts to the parliamentary committee scrutinising the legislation.

According to the Financial Times, Apple said demands for the ability to access data held in other countries would "immobilise substantial portions of the tech sector and spark serious international conflicts".

Related articles  Latest WhatsApp update makes messaging much faster  WhatsApp BAN: Popular smartphone messenger BLOCKED for 48 hours

The technique allows authorities to interfere with electronic devices in order to obtain data and can range from remotely accessing a computer to covertly downloading the contents of a mobile phone.

It is seen as an increasingly crucial tool as advanced encryption makes intercepting targets' communications more difficult.

There are also fears in technology circles that the proposals will hit services offering "end-to-end encryption" such as WhatsApp and Apple's iMessage.

However the Home Secretary has assured that the legislation "will not ban encryption or do anything to undermine the security of people's data".

But Apple has warned against the proposals.

The US firm - and world's most valuable company - argues that the existence of a backdoor creates a vulnerability that others could exploit, making data stored or sent online less secure.

APPLE ∑ IG

Apple uses end-to-end encryption to secure customers' information

"A key left under the doormat would not just be there for the good guys. The bad guys would find it too," the company writes in an eight-page submission to the committee.

In an interview with the Daily Telegraph last month, Apple boss Tim Cook said any attempt to weaken encryption could have "very dire consequences", harming consumers by making their data less secure.

"To protect people who use any products, you have to encrypt. You can just look around and see all the data breaches that are going on.

"These things are becoming more frequent. They can not only result in privacy breaches but also security issues. We believe very strongly in end-to-end encryption and no back doors," he said.

Mr Cook warned: "We don't think people want us to read their messages. We don't feel we have the right to read their emails.

"Any back door is a back door for everyone. Everybody wants to crack down on terrorists. Everybody wants to be secure. The question is how. Opening a back door can have very dire consequences."

The proposed new laws could impose obligations on telecommunications providers requiring them to remove "electronic protection" applied to "communications or data".

269
Apple claims more snooping powers will let 'bad guys' in

BYLINE: ANDREW GRIFFIN

SECTION: NEWS; Pg. 11

LENGTH: 441 words

Apple has launched a scathing attack on the UK Government's plans to give spies more powers.

In a rare public statement, the technology giant said it believes that Theresa May's Investigatory Powers Bill would make the "personal data of millions of law-abiding citizens less secure" - potentially allowing "bad guys" to access the information.

The Government intends to bring in the Investigatory Powers Bill soon to bring new powers to help intelligence agencies and police to conduct digital surveillance. But civil liberties campaigners argue the measures are intrusive.

In its submission to the joint scrutiny committee for the Investigatory Powers Bill, Apple argues that the legislation should be re-written to be more clear about how the powers that are contained within it will be used.

"We believe there is a need for much greater clarity as to how the powers in the Bill will be applied," Apple's submission reads. "The [powers] could endanger the privacy and security of users in the UK and elsewhere."

Apple opposes a requirement in the Bill that firms are able to break their own security measures so that messages can be more easily read.

Encryption - which can be found in Apple's iMessage and FaceTime messaging services - uses mathematical techniques to ensure that a message can only be read by the person it was sent to. But parts of the Bill seem to suggest technology should be broken open, so that messages can't be kept from intelligence agencies.

Apple says that the "best minds in the world cannot rewrite the laws of mathematics", and that as a result there is no way of creating methods of encryption that would only give access to the Government or the intelligence agencies.

"The Bill threatens to hurt law-abiding citizens in its effort to combat the few bad actors who have a variety of ways to carry out their attacks," Apple argues. "The creation of backdoors and intercept
capabilities would weaken the protections built into Apple products and endanger all our customers. A key left under the doormat would not just be there for the good guys. The bad guys would find it too."

Apple also opposes a part of the Bill that would force companies to help the Government to hack into phones. The company points out that this will "extend responsibility for hacking from Government to the private sector", and that it will undermine trust between tech companies and users.

Apple's Tim Cook has previously spoken out publicly about the importance of privacy safeguards, but the public criticism of Government policy is an unusual step for the company itself, which has in the past rarely made statements about legislation or policy.

Apple attacks snooping laws: Technology giants say plans to allow access could cause 'paralysis for business and cause 'serious international conflicts'

Tech giant Apple has attacked government's proposed Snoopers' Charter. Said it would 'paralyse' business and contribute to 'international conflicts'.

Apple has attacked government proposals to give spies extra powers to access suspects' mobile phone and internet records.

It said the so-called Snoopers' Charter could 'paralyse' businesses and contribute to 'serious international conflicts'.

The US technology giant also said the draft Investigatory Powers Bill could result in repressive regimes seeking to mimic the legislation.

In a rare public statement, Apple told the Parliamentary scrutiny committee examining the draft bill that 'substantial portions' of the worldwide technology sector would be crippled by government demands for access to data.

The technology giant said: 'It would also likely be the catalyst for other countries to enact similar laws, paralysing multinational corporations under the weight of what could be dozens or hundreds of contradictory country-specific laws.'
Unnamed company executives from another technology firm told the Financial Times they also believe the Russian and Chinese governments would not 'sit on their hands' but boost their own internet spying in the wake of the new law.

Apple's rivals Google, Twitter, Facebook, Yahoo and Microsoft are planning to act as one to express their opposition to the legislation, it was reported.

The Investigatory Powers Bill proposes a legal requirement on communications firms to help spies hack into suspects' smartphones and computers.

Existing bulk data gathering powers will be extended to include basic internet records.

Companies including BT, TalkTalk and Sky will be obliged to comply with warrants designed to unlock an electronic device, or implant software allowing the contents to be read remotely.

The Home Secretary maintains the bill will include 'strong oversight and authorisation arrangements' as a concession to protect civil liberties.

The current basic power to interfere with computer equipment applies to all 43 police forces in England and Wales.

Security services MI5 and MI6, the GCHQ spy base at Cheltenham and a limited number of police forces will be able to switch on cameras and microphones for more intrusive spying missions once they obtain a warrant.

Apple boss Tim Cook calls on British government to scale back snooper's charter;
Cook has already warned against giving spies a "back door" to reading people's e-mails because weakening data security could help criminals

BYLINE: By Catherine Wylie

SECTION: NEWS, TECHNOLOGY & SCIENCE, TECHNOLOGY

LENGTH: 618 words

The boss of Apple has called for Britain's so called snooper's charter to be scaled back over fears it could weaken the security of the personal data of "hundreds of millions of law abiding citizens."

Tim Cook has already warned the draft Investigatory Powers Bill could give spies a "back door" to reading people's e-mails because weakening data security could help criminals.
And now the tech giant is said to have passed on its concerns about the proposed legislation to the parliamentary committee scrutinising it.

According to the Guardian, Apple highlighted the main areas of the bill that it wants to see changed, such as passages that threaten the way its messaging service, iMessage, works.

The company said this would weaken encryption and enable the security services to eavesdrop on iMessage for the first time.

In the report, Apple said: "We believe it would be wrong to weaken security for hundreds of millions of law-abiding customers so that it will also be weaker for the very few who pose a threat.

Read more: Apple chief Tim Cook says company is 'more secretive than CIA' and there isn't a trade-off between security and privacy

"In this rapidly evolving cyber-threat environment, companies should remain free to implement strong encryption to protect customers."

According to the Financial Times, Apple said demands for the ability to access data held in other countries would "immobilise substantial portions of the tech sector and spark serious international conflicts".

Under proposals in Theresa May's Investigatory Powers Bill, communications firms will be legally required to help spies hack into suspects' smartphones and computers.

Domestic providers will be obliged to assist intelligence agencies when they are given warrants to carry out equipment interference.

The technique allows authorities to interfere with electronic devices in order to obtain data and can range from remotely accessing a computer to covertly downloading the contents of a mobile phone.

It is seen as an increasingly crucial tool as advanced encryption makes intercepting targets' communications more difficult.

The BBC said Apple's submission to the committee runs to eight pages, and focuses on three issues: encryption, the possibility of having to hack its own products, and the precedent it would set by agreeing to comply with UK-issued warrants.

In an interview with the Daily Telegraph last month, Mr Cook said any attempt to weaken encryption could have "very dire consequences", harming consumers by making their data less secure.

"To protect people who use any products, you have to encrypt. You can just look around and see all the data breaches that are going on.

"These things are becoming more frequent. They can not only result in privacy breaches but also security issues. We believe very strongly in end-to-end encryption and no back doors," he said.

Read more: Theresa May's Snooper Tax could make broadband bills skyrocket

Mr Cook warned: "We don't think people want us to read their messages. We don't feel we have the right to read their emails.

"Any back door is a back door for everyone. Everybody wants to crack down on terrorists. Everybody wants to be secure. The question is how. Opening a back door can have very dire consequences."

There are also fears in technology circles that the proposals will hit services offering "end-to-end encryption" such as WhatsApp and Apple's iMessage, despite the Home Secretary's assurances that the legislation "will not ban encryption or do anything to undermine the security of people's data".

The proposed new laws could impose obligations on telecommunications providers requiring them to remove "electronic protection" applied to "communications or data".

LOAD-DATE: December 22, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

Copyright 2015 Trinity Mirror, Plc.

273
Theresa May says new spying powers will be used to bring cyberbullies and online trolls to justice

BYLINE: SOPHIE JANE EVANS FOR MAILONLINE

NEW: 665 words

May 'wrote in letter to MP that spying laws will help tackle cyberbullying'.
Powers will force Internet firms to retain individuals' connection records.
Records may then be used by officials to identify online bullies and trolls.

Politician's Investigatory Powers Bill is being considered by parliament.
The draft bill has been criticised by many, including the tech giant Apple.

New spying laws will be used to bring online bullies and trolls to justice, the Home Secretary says.
Theresa May reportedly claims the surveillance powers - unveiled under the Investigatory Powers Bill last month - will help police and spooks to track down and identify anonymous cyberbullies.
This is because they will force Internet firms to retain individuals’ connection records - which may then be used by officials to unmask abusive users going by various aliases, The Times reports.

It is the first time the government has said the new laws will be used to deal with what Mrs May describes as the 'pernicious' issue of cyberbullying, which affects millions of young Brits annually.

The Home Secretary made the remarks on the draft bill - which is being considered by parliament and has been criticised by many including the tech giant Apple - in a letter to MP James Cartlidge.

In her letter, she reportedly wrote: 'Internet connection records would update the capability of law enforcement in a criminal investigation to determine the sender and recipient of a communication, for example, a malicious message such as those exchanged in cyberbullying.'

She said the bill would, therefore, support the effort of police to tackle online bullying and trolling.

Mrs May copied the letter - which she wrote as a response to a question about the bill from Mr Cartlidge following its unveiling - to Shadow Home Secretary Andy Burnham, it is reported.

Researchers from Ditch The Label claim that as many as seven in 10 young people have been victimised by cyberbullies - with one in five having suffered extreme bullying on a daily basis.

The online abuse - carried out on a range of social media networks - has led some to withdraw into themselves, grow depressed, lose self-esteem and, in several cases, even commit suicide.

Mr Cartlidge said: 'We're all becoming much more aware that the internet has a dark side. 'But it's not just about terrorism or hacking into bank accounts.

'There are these nasty, psychological attacks that particularly affect young people.'

Speaking to The Times, The South Suffolk MP added that the government does have to be able to 'police the Internet' - but he said that it must be careful with how far it extends the new powers.

Mrs May presented the Investigatory Powers Bill to the House of Commons in early November.
Under proposals in the bill, communications firms would be legally required to help spies hack into suspects' smartphones and computers, while domestic providers would be obliged to assist intelligence agencies if they were given warrants to carry out equipment interference.

The technique allows authorities to interfere with electronic devices to obtain data and can range from remotely accessing a computer to covertly downloading the contents of a mobile phone.

This week, Apple raised concerns about the draft bill in an official submission to a parliamentary committee, while suggesting that the use of encryption in communications should be strengthened.

"We owe it to our customers to protect their personal data to the best of our ability,' the firm said. "Increasingly stronger - not weaker - encryption is the best way to protect against these threats.'

The submission added: 'The Bill threatens to hurt law-abiding citizens in its effort to combat the few bad actors who have a variety of ways to carry out their attacks.

'The creation of back doors and intercept capabilities would weaken the protections built into Apple products and endanger all our customers.

'A key left under the doormat would not just be there for the good guys.

'The bad guys would find it too.'

LOAD-DATE: December 25, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

JOURNAL-CODE: WEBDM

New Chinese spying laws draw international criticism, despite similarity with UK's Investigatory Powers Bill;

China has said that it took inspiration in drafting the powers from the US and elsewhere for a law that bears marked similarities to the UK's 'Snoopers' Charter'

BYLINE: Andrew Griffin

SECTION: NEWS

LENGTH: 574 words

New spying laws in China have drawn wide criticism from the international community, despite being largely similar to those set to be passed in the UK without much condemnation in the UK.

The new Chinese spying powers allow authorities to weaken security so that messages can be read and force companies to co-operate with surveillance. Both of those powers are also part of the
Investigatory Powers Bill, which is expected to be passed into law in early 2016, on a sped-up schedule.

China's controversial new law was passed on Sunday and requires that technology companies hand over encryption keys and other sensitive information. The country says that the powers are needed to fight against a growing threat from militants and separatists.

Read more

China passes controversial new anti-terrorism law

The UK's Investigatory Powers Bill also requires that technology companies store sensitive information - including a requirement that internet providers hold records of browsing for a year - as well as weakening security so that intelligence agencies can gain access to communications.

Both the UK and China have claimed that the law doesn't ban encryption, which ensures that messages can't be read as they pass over networks. But each appears to undercut the technology that powers such security measures.

The international community has condemned the new Chinese powers, and President Obama has raised concerns with Chinese President Xi Jinping.

Though the UK's laws have received scathing reviews from Apple and other companies, they have not been publicly criticised by other governments.

China has already said that it took inspiration for the law from measures in the US and elsewhere.

The deputy head of the parliament's criminal law division told reporters that China was simply doing what other Western countries had already done. "This rule accords with the actual work need of fighting terrorism and is basically the same as what other major countries in the world do," Li Shouwei told reporters.

Li said that the law would not affect the day-to-day operations of tech companies and that it would not force them to install the controversial backdoors that would weaken security so that authorities could read people's messages.

That is the same argument made by Theresa May and other government officials about the UK's Investigatory Powers Bill. Though a range of companies have pointed out that the law seems to allow the government to install such powers, the government maintains that it is not breaking encryption but rather offering ways of catching terrorists and cybercriminals.

As with the laws that are set to be passed in the UK, experts have worried that China's surveillance laws will make their way across the globe.

Computer makers will "respond by building this capability into any equipment that might end up in China, even if it never does", Cory Doctorow, special advisor to the Electronic Frontier Foundation (EFF), told The Independent last week.

"This creates a vulnerability that other entities - national security forces, police, industrial spies, voyeurs, organized crime, griefers, identity thieves - will exploit, even in countries that never passed a backdoor law."

The UK's law also allows for extraterritorial force, meaning that companies that operate in the UK but are based elsewhere will need to comply with the law, potentially bringing two different regimes into conflict.
Social media bosses face two years in jail if they warn users MI5 is watching them after ministers lose patience with tech giants

BYLINE: JAMES SLACK POLITICAL EDITOR FOR THE DAILY MAIL

SECTION: NEWS

LENGTH: 598 words

Some companies were warning users of requests for communications data
Will be explicit criminal offence to notify subject of a surveillance operation
Firms to store details of public’s use of the internet and apps for 12 months
Companies said they’d take greater steps to protect customers’ ‘privacy’

Bosses at Twitter and other social media giants face prison if they tip off their customers about spying operations by police and the security services, under a sweeping new law.

Ministers have lost patience with the tech giants after it emerged that some companies were warning users of requests for communications data by MI5, MI6 and GCHQ.

Bosses of any technology firm which ignores the Home Office edict to keep operations secret will face up to two years in prison.

It will become an explicit criminal offence to notify the subject of a surveillance operation that requests for their data have been made, unless they have permission to do so. This could include tweets, text messages or emails.

The move, included in the controversial draft Investigatory Powers Bill, will further stoke tensions between the authorities and the communications companies, who officials say have become less co-operative in the wake of the Edward Snowden leaks.

Snowden - an ex-security official for the US Government, now a fugitive in Russia - revealed details of mass surveillance operations by British and American agencies.

In response, technology companies said they would take greater steps to protect their customers’ ‘privacy’.

Antony Walker, deputy chief executive officer at techUK, which represents communications and internet firms, said: ‘A right of redress by the citizen depends upon individuals being notified at some appropriate time that requests have been made to access their data.

‘By preventing companies from notifying consumers about requests for access to data the Investigatory Powers Bill risks being out of step with the direction of international law.

‘This will make co-operation between jurisdictions more difficult and could slow down the sharing of information between international agencies. So from that perspective preventing companies from being more transparent about the data requests they receive appears counter-productive.’

Details of the plan emerged in a note to the Investigatory Powers Bill, which will itself require communications firms to store details of the public’s use of the internet and apps for 12 months.

The note says: ‘While in many cases it would be detrimental to the investigation if a communication service provider notified the subject of an investigation that a request for their data had been made, there are cases where this would not be the case.'
The legislation provides for communication service providers to notify the customer in such circumstances where the public authority is content for them to do so.'

In June a report by David Anderson QC, the independent reviewer of terrorism laws, warned that big internet firms were telling customers whom they knew to be under surveillance. Referring to Twitter, he said: 'Some service providers will tip off a customer that they are under surveillance unless persuaded not to do so, typically by a court order.'

One unnamed company told Mr Anderson: 'Our priority is our brand, not UK intelligence.'

Earlier this month, it emerged Apple has voiced concerns that the Bill would mean technology firms will have to provide the contents of communications on production of a warrant.

The company said: 'A key left under the doormat would not just be there for the good guys. The bad guys would find it too.'

SOCIAL MEDIA BOSSES FACE JAIL IF THEY WARN USERS MI5 IS WATCHING THEM

Bossses at Twitter and other social media giants face prison if they tip off their customers about spying operations by police and the security services, under a sweeping new law.

Ministers have lost patience with the tech giants after it emerged that some companies were warning users of requests for communications data by MI5, MI6 and GCHQ.

It will become an explicit criminal offence to notify the subject of a surveillance operation that requests for their data have been made, unless they have permission to do so. This could include tweets, text messages or emails.

The move, included in the controversial draft Investigatory Powers Bill, will further stoke tensions between the authorities and the communications companies, who officials say have become less co-operative in the wake of the Edward Snowden leaks.

Snowden - an ex-security official for the US Government, now a fugitive in Russia -revealed details of mass surveillance operations by British and American agencies.

In response, technology companies said they would take greater steps to protect their customers privacy'.
Antony Walker, deputy chief executive officer at techUK, which represents communications and internet firms, said: A right of redress by the citizen depends upon individuals being notified at some appropriate time that requests have been made to access their data.

By preventing companies from notifying consumers about requests for access to data the Investigatory Powers Bill risks being out of step with the direction of international law.

This will make co-operation between jurisdictions more difficult and could slow down the sharing of information between international agencies. So from that perspective preventing companies from being more transparent about the data requests they receive appears counter-productive.'

Details of the plan emerged in a note to the Investigatory Powers Bill, which will itself require communications firms to store details of the public's use of the internet and apps for 12 months.

The note says: While in many cases it would be detrimental to the investigation if a communication service provider notified the subject of an investigation that a request for their data had been made, there are cases where this would not be the case.

The legislation provides for communication service providers to notify the customer in such circumstances where the public authority is content for them to do so.'

In June a report by David Anderson QC, the independent reviewer of terrorism laws, warned that big internet firms were telling customers who they knew to be under surveillance. Referring to Twitter, he said: Some service providers will tip off a customer that they are under surveillance unless persuaded not to do so, typically by a court order.'

One unnamed company told Mr Anderson: Our priority is our brand, not UK intelligence.'

Earlier this month, it emerged Apple has voiced concerns that the Bill would mean technology firms will have to provide the contents of communications on production of a warrant.

The company said: A key left under the doormat would not just be there for the good guys. The bad guys would find it too.'

© Daily Mail

LOAD-DATE: December 28, 2015

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Papers

Facebook and Twitter staff could face JAIL if they warn users about police surveillance; Snooper's Charter will punish staff at social media companies for warning customers that they are under surveillance

BYLINE: By Gavin Cordon

SECTION: NEWS, TECHNOLOGY & SCIENCE, TECHNOLOGY

LENGTH: 457 words
Staff at social media companies such as Facebook and Twitter could face up to two years in prison if they tip off customers that they are under surveillance by police or the security services.

The government's draft Investigatory Powers Bill (also known as the "Snooper's Charter") will make the unauthorised disclosure of operations carried out under the provisions of the legislation a criminal offence.

An explanatory note published with the Bill says: "The intent of these provisions is to prevent the so-called 'tipping off' of criminal suspects or subjects of interest that their data has been sought, thus informing them that they are under suspicion."

The move reflects concern among ministers that some telecoms companies have warned suspects that details of their communications data have been requested by police or intelligence agencies.

A report earlier this year by David Anderson QC, the independent reviewer of terrorism laws, warned that some technology companies preferred to "protect customers' privacy rather than co-operate with governments".

"Some service providers will tip off a customer that they are under surveillance unless persuaded not to do so, typically by a court order," he said.

The draft Investigatory Powers Bill, which was unveiled by Home Secretary Theresa May in November, requires telecommunications companies to hand over data to security services and gives police, GCHQ, MI5 and MI6 unfettered access to records of Brits' web use.

Tech firms have spoken out against the proposed legislation, which would require tech firms to store users' data for up to twelve months. They say the legislation would not only hurt trust and transparency but also weaken security.

The boss of Apple, Tim Cook, has warned that giving spies a "back door" to reading people's emails could have "very dire consequences", providing an access route for hackers and harming consumers by making their data less secure.

Commenting on the news, Antony Walker, deputy chief executive of techUK, which represents communications and internet firms, said that preventing companies from being more transparent about the data requests they receive could be counter-productive.

"A right of redress by the citizen depends upon individuals being notified at some appropriate time that requests have been made to access their data," he said.

"By preventing companies from notifying consumers about requests for access to data the Investigatory Powers Bill risks being out of step with the direction of international law.

"This will make cooperation between jurisdictions more difficult and could slow down the sharing of information between international agencies."

Should intelligence agencies be able to spy on social media conversations?
2. Articles for 2016

Results
1. Did we really need HMRC’s festive ‘nudge’? *The Times (London)*, December 31, 2016 Saturday, BUSINESS; Pg. 58, (479 words), Carol Lewis

2. Snoopers in Uncle Sam’s backyard *The Times (London)*, December 31, 2016 Saturday, NEWS; Pg. 36, (478 words), Will Pavia

3. HAPPY NEW YEAR HERE COME THE WRAPPING PAPER POLICE *DAILY MAIL (London)*, December 30, 2016 Friday, (1514 words)

4. Counter Extremism Bill could lead to investigations into people ‘miles away’ from terrorism; ‘We didn’t ban communism during the Cold War, and I think we should be strong and robust enough to argue back’ *The Independent (United Kingdom)*, December 30, 2016 Friday 9:19 PM GMT, HOME NEWS, (660 words), Shaun Connolly

5. Warning: UK Government can record EVERYTHING you click on online from today under new ‘Snooper’s Charter’ *MailOnline*, December 30, 2016 Friday 8:28 PM GMT, NEWS, (332 words), CHRIS SUMMERS FOR MAILONLINE

6. Happy New Year - here come the Wrapping Paper Police: RICHARD LITTLEJOHN on how the concept of ‘public services’ is a sick joke *MailOnline*, December 30, 2016 Friday 12:33 AM GMT, RIGHTMINDS, (1504 words), RICHARD LITTLEJOHN FOR THE DAILY MAIL

7. It’s not just voter ID that needs cleaning up in our grubby electoral system; Send your letters to letters@independent.co.uk *The Independent (United Kingdom)*, December 28, 2016 Wednesday 11:59 AM GMT, LETTERS, (1119 words), Letters

8. THE COUNCILS USING TERROR LAW TO SPY ON BARKING DOGS *DAILY MAIL (London)*, December 26, 2016 Monday, (571 words), BY KATE PICKLES

9. Councils use spying powers to check rubbish and noisy dogs *The Times (London)*, December 26, 2016 Monday, NEWS; Pg. 2, (496 words), Michael Savage

10. Revealed: British councils used Ripa to secretly spy on public; Local authorities used Regulation of Investigatory Powers Act to follow people, including dog walkers, over five years *The Guardian*, December 25, 2016 Sunday 7:00 PM GMT, WORLD NEWS, (1231 words), Anushka Asthana Political editor

11. The councils using terror law to spy on barking dogs and people who feed pigeons: Local authorities given permission to carry out 55,000 hours of surveillance over the past five years *MailOnline*, December 25, 2016 Sunday 10:51 PM GMT, NEWS, (608 words), KATE PICKES FOR DAILY MAIL
12. OUR SPY POWERS TO FIGHT TERROR ARE ILLEGAL, EU JUDGES CLAIM  
DAILY MAIL (London), December 22, 2016 Thursday, (603 words), BY IAN DRURY AND JAMES SLACK

13. Palace is put on lockdown  
Daily Mirror, December 22, 2016 Thursday, NEWS, Pg. 7, (151 words)

14. European court rules 'indiscriminate' UK mass surveillance law to be illegal  
Financial Times (London, England), December 22, 2016 Thursday, FRONT PAGE - FIRST SECTION; Pg. 1, (368 words), Madhumita Murgia and George Parker in London and Jim Brunsden in Brussels

15. Privacy ruling leaves business in a quandary: 'Snooper's charter': Court criticism  
Financial Times (London, England), December 22, 2016 Thursday, NATIONAL NEWS; Pg. 3, (515 words), Madhumita Murgia and George Parker in London and Jim Brunsden in Brussels

16. Politics is a rough trade, but Jamie Reed should be hanging in there: The Corbyn critic has every reason to feel less then thrilled about being a Labour MP right now. But he has a duty to his constituents, and to democracy itself  
The Guardian, December 22, 2016 Thursday 12:15 PM GMT, OPINION, (938 words), Polly Toynbee

17. European court rules against 'indiscriminate' snooper's charter; JUSTICE  
i-Independent Print Ltd, December 22, 2016, NEWS; Pg. 9, (383 words), Harriet Agerholm

18. Labour's Diane Abbott slams 'unlawful' Snooping Charter and calls for major rethink; But her comments also risk new Labour divisions over the legislation  
The Independent (United Kingdom), December 22, 2016 Thursday 10:08 AM GMT, UK POLITICS, (535 words), Joe Watts

19. Labour's Diane Abbott slams 'unlawful' Snooping Charter and calls for major rethink; But her comments also risk new Labour divisions over the legislation  
The Independent (United Kingdom), December 22, 2016 Thursday 10:08 AM GMT, UK POLITICS, (535 words), Joe Watts

20. EU's highest court rules snooper's charter illegal  
The Independent - Daily Edition, December 22, 2016 Thursday, NEWS; Pg. 11, (545 words), HARRIET AGERHOLM

21. Did Leave voters know that Brexit will give the state more power to spy on us?  
telegraph.co.uk, December 22, 2016 Thursday 10:34 AM GMT, NEWS, (816 words), By Rupert Myers

22. The European Court of Justice ruling on state surveillance is exactly why we are leaving the European Union  
telegraph.co.uk, December 22, 2016 Thursday 9:31 AM GMT, NEWS, (432 words), By Philip Johnston

23. Terror fight 'is weakened' by EU ruling on snooping  
The Times (London), December 22, 2016 Thursday, NEWS; Pg. 4, (675 words), Sean O'Neill

24. EU's highest court declares UK surveillance powers illegal  
FT.com, December 21, 2016 Wednesday 12:15 PM GMT, (890 words), Madhumita Murgia and George Parker in London, and Jim Brunsden in Brussels

282
25. EU's highest court rules UK surveillance laws illegal  

FT.com, December 21, 2016 Wednesday 11:27 AM GMT, (200 words), Madhumita Murgia

26. EU's highest court delivers blow to UK snooper's charter; Indiscriminate collection of emails is illegal, court rules in response to challenge originally brought by David Davis  

The Guardian, December 21, 2016 Wednesday 1:13 PM GMT, WORLD NEWS, (1231 words), Owen Bowcott Legal affairs correspondent

27. EU ruling means UK snooper's charter may be open to challenge; Ministers can no longer be certain that Investigatory Powers Act can survive privacy actions in UK courts after landmark ruling on blanket state surveillance  

The Guardian, December 21, 2016 Wednesday 12:58 PM GMT, WORLD NEWS, (676 words), Alan Travis Home affairs editor

28. Snooper's charter dealt blow after EU's highest court rules 'indiscriminate' government retention of emails is illegal  

The Independent (United Kingdom), December 21, 2016 Wednesday 9:26 AM GMT, UK POLITICS, (33 words)

29. Snooper's charter dealt blow after EU's highest court rules 'indiscriminate' government retention of emails is illegal  

The Independent (United Kingdom), December 21, 2016 Wednesday 9:26 AM GMT, UK POLITICS, (97 words)

30. Snooper's charter dealt blow after EU's highest court rules 'indiscriminate' government retention of emails is illegal  

The Independent (United Kingdom), December 21, 2016 Wednesday 9:26 AM GMT, UK POLITICS, (299 words), Harriet Agerholm

31. Snooper's charter dealt blow after EU's highest court rules 'indiscriminate' government retention of emails is illegal; 'UK may have voted to leave the EU - but we didn't vote to abandon our rights,' says Liberty  

The Independent (United Kingdom), December 21, 2016 Wednesday 9:26 AM GMT, UK POLITICS, (513 words), Harriet Agerholm

32. Snooper's charter dealt blow after EU's highest court rules 'indiscriminate' government retention of emails is illegal; 'UK may have voted to leave the EU - but we didn't vote to abandon our rights,' says Liberty  

The Independent (United Kingdom), December 21, 2016 Wednesday 9:26 AM GMT, UK POLITICS, (540 words), Harriet Agerholm

33. Snooper's charter dealt blow after EU's highest court rules 'indiscriminate' government retention of emails is illegal; 'UK may have voted to leave the EU - but we didn't vote to abandon our rights,' says Liberty  

The Independent (United Kingdom), December 21, 2016 Wednesday 9:26 AM GMT, UK POLITICS, (567 words), Harriet Agerholm

34. Ministers are set for clash with EU judges over surveillance powers after ruling that internet companies can't be forced to harvest email data  

MailOnline, December 21, 2016 Wednesday 10.04 AM GMT, NEWS, (291 words), JAMES TAPSFIELD, POLITICAL EDITOR FOR MAILONLINE

35. 
Ministers are set for clash with EU judges over surveillance powers after ruling that internet companies can't be forced to harvest email data. MailOnline, December 21, 2016 Wednesday 10:04 AM GMT, NEWS, (469 words), JAMES TAPSFIELD, POLITICAL EDITOR FOR MAILONLINE

36. Ministers are set for clash with EU judges over surveillance powers after ruling that internet companies can't be forced to harvest email data. MailOnline, December 21, 2016 Wednesday 10:04 AM GMT, NEWS, (546 words), JAMES TAPSFIELD, POLITICAL EDITOR FOR MAILONLINE

37. Brexit Secretary David Davis just took Theresa May to the EU Court of Justice and won; In a victory for both privacy campaigners and absurdity, the EU court agreed with David Davis that parts of the Snooper's Charter are unlawful. mirror.co.uk, December 21, 2016 Wednesday 10:42 AM GMT, NEWS, UK NEWS, (541 words), By Mikey Smith

38. Brexit Secretary David Davis just took Theresa May to the EU Court of Justice and won; In a victory for both privacy campaigners and absurdity, the EU court agreed with David Davis that parts of the Snooper's Charter are unlawful. mirror.co.uk, December 21, 2016 Wednesday 10:42 AM GMT, NEWS, UK NEWS, (651 words), By Mikey Smith

39. Theresa May's Snooper's Charter dealt major setback as EU court rules against 'indiscriminate' collection of internet data. telegraph.co.uk, December 21, 2016 Wednesday 10:10 AM GMT, TECHNOLOGY, (600 words), By James Titcomb

40. Spying on Press is the e-version of using a baton; COMMENT. Daily Mirror, December 19, 2016 Monday, NEWS; Pg. 4,5, (216 words), KEVIN MAGUIRE

41. Police unlawfully intercepted Mirror reporter's phone records after disgraced chief's lies were exposed; Force unlawfully snooped on us and others after its £191,000-a-year Chief Constable, later sacked in disgrace, had an affair with a colleague, lied about it, and spent thousands of pounds of taxpayers' money on jollies with her. mirror.co.uk, December 18, 2016 Sunday 10:36 PM GMT, NEWS, UK NEWS, (1008 words), By Jeremy Armstrong

42. 13 ways your online privacy was violated in 2016 - and what you can do about it; Founder of MeWe and privacy expert Mark Weinstein looks back at 2016 - and it hasn't been a great year when it comes to online privacy. mirror.co.uk, December 18, 2016 Sunday 2:32 PM GMT, TECHNOLOGY, (1981 words), By Jo-Anne Rowney

43. Think ethical and make a gift special. i-Independent Print Ltd, December 16, 2016, NEWS; Pg. 22, (333 words), SOCIETY Elaine Ritch

44. UK security "failing" to protect Brits from fraud attacks, fake goods, and cyber criminals - 7 ways you can protect yourself; A new investigation has warned that the UK's security system is not protecting consumers from modern scams, unfair trading, and unsafe goods - leading to billions of successful attacks each year. mirror.co.uk, December 15, 2016 Thursday 12:01 AM GMT, MONEY, (1166 words), By Emma Munbodh

45. UK security "failing" to protect Brits from fraud attacks, fake goods, and cyber criminals - 7 ways you can protect yourself; A new investigation has warned that the UK's security system is not protecting consumers from modern scams, unfair trading, and unsafe goods - leading to billions of successful attacks each year. mirror.co.uk, December 15, 2016 Thursday 12:01 AM GMT, MONEY, (1265 words), By Emma Munbodh

284
46. Cod bless them all: The decline of fish 'n' chips is hard to swallow in Brexitland i-Independent Print Ltd, December 13, 2016, NEWS; Pg. 13, (606 words), My View Grace Dent

47. Squid and chips as the new national dish? This might be the final straw for Brexiteers The Independent - Daily Edition, December 13, 2016 Tuesday, COMMENT; Pg. 34, (590 words), GRACE DENT

48. The Walking Dead, season 7, episode 8, Hearts Still Beating review: Rick finally wakes up and smells the viscera in a bloody mid-season finale telegraph.co.uk, December 12, 2016 Monday 7:27 AM GMT, TV, (1537 words), By Ed Power

49. The CIA snooper who learnt how to whistle FILM Financial Times (London, England), December 9, 2016 Friday, ARTS; Pg. 10, (1275 words), Nigel Andrews

50. A Conservative general election majority dangles like a bauble on the Number Ten Christmas Tree; Please send your letters to letters@independent.co.uk The Independent (United Kingdom), December 9, 2016 Friday 3:36 PM GMT, VOICES, (817 words), Letters

51. A Conservative general election majority dangles like a bauble on the Number 10 Christmas Tree; Please send your letters to letters@independent.co.uk The Independent (United Kingdom), December 9, 2016 Friday 3:36 PM GMT, VOICES, (830 words), Letters

52. The ‘Snooper's Charter’ hysteria is absurd - The IPB sets a new standard for the world telegraph.co.uk, December 9, 2016 Friday 6:39 PM GMT, NEWS, (965 words), By Jonathan Evans

53. Porn website xHamster sends UK visitors to online petition against Snoopers’ Charter telegraph.co.uk, December 9, 2016 Friday 10:56 AM GMT, TECHNOLOGY, (430 words), By Cara McGoogan

54. Hello, Snooper's Charter. Bye bye, privacy; Technology i-Independent Print Ltd, December 3, 2016, NEWS; Pg. 22, (358 words), Rhiannon Williams

55. SPY LAW TO KEEP SAFE The Sun (England), December 3, 2016 Saturday, NEWS; Pg. 2, (116 words)

56. The internet needs to be policed; The Opinion Matrix COMMENT FROM HOME & ABROAD ‘SNOOPER’S CHARTER’ i-Independent Print Ltd, December 2, 2016, NEWS; Pg. 14, (90 words)

57. Snooper's charter: dissent over the […] The Times (London), December 1, 2016 Thursday, NEWS; Pg. 65, (13 words)

58. No, Sir Tim, this act is not a 'snooper's charter' Alex Carlile The Times (London), December 1, 2016 Thursday, EDITORIAL; Pg. 30, (404 words)
59. Civil liberties fears as spies and police gain new powers; SECURITY i-Independent Print Ltd, November 30, 2016, NEWS; Pg. 14, (535 words), Dean Kirby

60. Can you beat the state snoopers?; TECHNOLOGY Encryption and proxies can still protect you, explains Rhiannon Williams i-Independent Print Ltd, November 30, 2016, NEWS; Pg. 27, (644 words)

61. Quote of the day i-Independent Print Ltd, November 30, 2016, NEWS; Pg. 16, (27 words)

62. Snooper's charter undermines our rights, says web inventor The Times (London), November 30, 2016 Wednesday, NEWS; Pg. 2, (479 words), Fiona Hamilton

63. 'Snooper's charter' bill becomes law, extending UK state surveillance; Home secretary hails 'world-leading' laws, which include forcing web and phone companies to collect browsing histories The Guardian, November 29, 2016 Tuesday 1:12 PM GMT, WORLD NEWS, (573 words), Alan Travis Home affairs editor

64. In tomorrow's i-Independent Print Ltd, November 29, 2016, NEWS; Pg. 27, (17 words)

65. Has the age of online privacy come to an end?; SURVEILLANCE Questions remain on how the Snooper's Charter will work, reports Jill Lawless i-Independent Print Ltd, November 29, 2016, NEWS; Pg. 27, (526 words)

66. Investigatory Powers Bill officially passes into law, giving Britain the 'most extreme spying powers ever seen'; The Bill received large opposition from petitions, but not within parliament The Independent (United Kingdom), November 29, 2016 Tuesday 11:05 AM GMT, NEWS, (494 words), Andrew Griffin

67. Investigatory Powers Bill officially passes into law, giving Britain the 'most extreme spying powers ever seen'; The Bill received large opposition from petitions, but not within parliament The Independent (United Kingdom), November 29, 2016 Tuesday 11:05 AM GMT, NEWS, (622 words), Andrew Griffin

68. Britain's spies enter a new era as powers to sweep up vast troves of call, email and text data are signed into law MailOnline, November 29, 2016 Tuesday 4:21 PM GMT, NEWS, (672 words), TIM SCULTHORPE, MAILONLINE DEPUTY POLITICAL EDITOR

69. Snoopers' Charter passes into law giving intelligence services controversial new spying powers; Ministers say it will ensure law enforcement and the security and intelligence agencies have the powers they need to disrupt terrorist attacks mirror.co.uk, November 29, 2016 Tuesday 6:48 PM GMT, TECHNOLOGY, (525 words), By Hayden Smith

70. Snoopers' Charter passes into law giving British intelligence services sweeping internet surveillance powers; Ministers say it will ensure law enforcement and the security and intelligence agencies have the powers they need to disrupt terrorist attacks mirror.co.uk, November 29, 2016 Tuesday 6:48 PM GMT, TECHNOLOGY, (573 words), By Hayden Smith
71. What is the Investigatory Powers Bill and what does it mean for my privacy? telegraph.co.uk, November 29, 2016 Tuesday 6:29 PM GMT, TECHNOLOGY, (813 words), By Cara McGoogan

72. Snooping bill rebounds The Times (London), November 29, 2016 Tuesday, NEWS; Pg. 10, (60 words)

73. We let technology into our lives. And now it's starting to control us; Internet giants are accessing vast amounts of personal data and using it to shape our behaviour. It's reminiscent of East Germany under the Stasi The Guardian, November 28, 2016 Monday 7:30 AM GMT, OPINION, (1418 words), Rachel Holmes

74. Index on Censorship: journalists now under 'unprecedented' attack; Study finds growing hostility toward media around the world has lead to rise in assaults on individuals as well as press freedom The Guardian, November 28, 2016 Monday 7:00 AM GMT, MEDIA, (872 words), Jane Martinson

75. The rise of fake news must not lead to an increase in snooping and censorship i-Independent Print Ltd, November 28, 2016, NEWS; Pg. 41, (791 words), Media IAN BURRELL on Monday

76. Petition to repeal new surveillance powers reaches 100,000 signatures telegraph.co.uk, November 28, 2016 Monday 9:32 AM GMT, TECHNOLOGY, (518 words), By James Titcomb

77. Revealed: The 48 organisations that can see your entire online browsing history, even if you delete it MailOnline, November 25, 2016 Friday 11:47 AM GMT, SCIENCE, (863 words), ABIGAIL BEALL FOR MAILONLINE

78. These are the 48 organisations that can see EVERYTHING you do online - even if you delete it; Since the passing of the Snooper's Charter a whole host of organisations can now freely spy on your internet activity mirror.co.uk, November 25, 2016 Friday 3:59 PM GMT, TECHNOLOGY, (476 words), By Jeff Parsons

79. How can I protect myself from government snoopers?; Now that the Investigatory Powers Act 2016 - or snooper's charter - has become law, Charles wants to protect his privacy The Guardian, November 24, 2016 Thursday 10:14 AM GMT, TECHNOLOGY, (1329 words), Jack Schofield

80. Pornography is just the first victim of this Government's censorship crusade The Independent - Daily Edition, November 24, 2016 Thursday, COMMENT; Pg. 35, (503 words), JERRY BARNETT

81. Snooper's Charter passes into law -- what it means FT.com, November 20, 2016 Sunday 1:23 PM GMT, (1018 words), Madhumita Murgia, European Technology Correspondent

82. The snooper's charter passed into law this week - say goodbye to your privacy The Independent - Daily Edition, November 20, 2016 Sunday, COMMENT; Pg. 32, (597 words), SILKIE CARLO

83. WARM-UP ACTS; Don't let the crisp autumn chill put you off an English mini-break The Sun (England), November 20, 2016 Sunday, FABULOUS;FEATURES; Pg. 68,69, (777 words)
A birth certificate to use the loo?; Agony uncle

Saturday, FT WEEKEND SUPPLEMENT - HOUSE & HOME; Pg. 2, (729 words), David Tang

'Extreme surveillance' becomes UK law with barely a whimper; Investigatory Powers Act legalises range of tools for snooping and hacking by the security services

The Guardian, November 19, 2016 Saturday 7:00 AM GMT, WORLD NEWS, (814 words), Ewen MacAskill

Parliament hands police and Government sweeping spying powers with new bill

The Independent - Daily Edition, November 19, 2016 Saturday, NEWS; Pg. 9, (989 words), ANDREW GRIFFIN

Tang of salt to travel advice; TMS diary@thetimes.co.uk | @timesdiary

The Times (London), November 19, 2016 Saturday, NEWS; Pg. 11, (489 words)

Snoopers' Charter that will let police hack into phones and check anyone's browser history becomes law after peers backed down on amendments

MailOnline, November 18, 2016 Friday 8:14 PM GMT, NEWS, (346 words), PADDY DINHAM FOR MAILONLINE

VICTORY FOR PRESS OVER LEGAL FEES FOR PHONE HACK CASES

DAILY MAIL (London), November 17, 2016 Thursday, (309 words), BY DANIEL MARTIN CHIEF POLITICAL CORRESPONDENT

Investigatory Powers Bill: 'Snoopers Charter 2' to pass into law, giving Government sweeping spying powers; The bill will force internet companies to store their users' browsing data for a year, and will allow the government to force phone makers to hack into people's handsets

The Independent (United Kingdom), November 17, 2016 Thursday 9:10 PM GMT, NEWS, (709 words), Andrew Griffin

Victory for the Press over 'charter' for the venomous' after peers back down in battle with MPs over new laws

MailOnline, November 17, 2016 Thursday 12:19 AM GMT, NEWS, (342 words), DANIEL MARTIN CHIEF POLITICAL CORRESPONDENT FOR THE DAILY MAIL

Amazon's app gives its customers X-Ray vision: Update can tell you exactly what's in a delivery box simply by pointing your phone's camera at it

MailOnline, November 16, 2016 Wednesday 6:04 PM GMT, SCIENCE, (535 words), STACY LIBERATORE FOR DAILYMAIL.COM and ANTHONY JOSEPH FOR MAILONLINE

Iraq war probe 'used Stasi tactics to spy on our troops'; MP's accuse investigators of carrying out surveillance on serving personnel accused

MailOnline, November 16, 2016 Wednesday 12:29 AM GMT, NEWS, (677 words), LARISA BROWN DEFENCE CORRESPONDENT FOR THE DAILY MAIL
96. Insurance company to trawl Facebook to judge if you are a safe driver; Algorithm could judge excessive use of exclamation marks to demonstrate overconfidence, a trait which leads to bad driving  
The Independent (United Kingdom), November 2, 2016 Wednesday 10:43 AM GMT, BUSINESS NEWS, (699 words), Ben Chapman

97. Company will read your Facebook posts to price your car insurance; Algorithm could judge excessive use of exclamation marks to demonstrate overconfidence, a trait which leads to bad driving  
The Independent (United Kingdom), November 2, 2016 Wednesday 10:43 AM GMT, BUSINESS NEWS, (604 words), Ben Chapman

98. Facebook blocks Admiral from reading your posts to judge if you are a safe driver; Algorithm would have judged certain words and punctuation to demonstrate overconfidence, a trait which leads to bad driving  
The Independent (United Kingdom), November 2, 2016 Wednesday 10:43 AM GMT, BUSINESS NEWS, (716 words), Ben Chapman

99. Government to launch new press regulation consultation; Move likely to infuriate campaigners such as Hacked Off but be welcomed by newspaper industry  
The Guardian, November 1, 2016 Tuesday 12:23 PM GMT, MEDIA, (281 words), Jane Martinson Head of Media

100. Kremlin dismisses 'unfounded and baseless' claims by MI5 chief that Russia is taking hostile measures against UK  
MailOnline, November 1, 2016 Tuesday 6:14 PM GMT, NEWS, (601 words), LARISA BROWN DEFENCE CORRESPONDENT FOR THE DAILY MAIL

Did we really need HMRC's festive 'nudge'?  

BYLINE: Carol Lewis  
SECTIONS: BUSINESS; Pg. 58  
LENGTH: 479 words

We all love to hate the taxman, but he doesn't exactly help himself. Sending out a letter suggesting that people might have made an error on last year's tax return only a couple of days before Christmas is far from festive. Supposedly Revenue & Customs (HMRC) could have just slapped those it suspected of underpaying with penalties, so from that point of view the latest letters - which suggest you might want to "reconsider" the figures you filed - are more passive-aggressive than threatening. Yet accountants say that the letters follow the "nudge" formula of suggesting rather than telling to induce change. The tactic is borrowed from the Behavioural Insights Team, or nudge unit, which was set up by David Cameron to find innovative ways to persuade people to do the right thing.

HMRC has had a fair amount of success with this tactic in the past. For instance, it found that replacing the words "nine out of ten people in the UK pay their tax on time", with "the great majority of people in [substitute local area] pay their tax on time" on letters significantly increased the proportion of people who paid before the deadline.
It all sounds harmless enough.

However, the truth is that HMRC almost has enough information, gathered from different data sources, to complete your tax return itself. The Revenue's Connect computer system is a data-matching tool that enables it to cross-check one billion pieces of data from its records and third-party data to identify links between people, organisations, assets and income. The system then throws up a red flag when the figures you file don't match those held by your bank, building society, Land Registry etc.

And the Revenue could, potentially, have access to more information in the future. HMRC is one of the bodies that is given access to internet connection records without a warrant under the Investigatory Powers Act 2016, the so-called Snoopers' Charter. These records show the services you have accessed on the internet over the past year - website names and instant messaging applications. It is not a full internet browsing history and has been described as giving "context not content" to those investigating crimes, including fraud.

The Revenue deserves all the help that it can get to fight tax evasion, but its mealy-mouthed letters suggesting that you might like to reconsider your last return are disingenuous. If it has evidence that you have "under-declared" then why not just say so and demand the money owed? Maybe something along the lines of: "You said you earned £100 interest on your savings last year, your bank said it was £200." More of a shove than a nudge, but at least we would all know where we stand.

And if the cost of sending the letter is more than the tax that will be recouped, then it's not worth chasing.

The pound suffered a year's worth of volatility in one day. This is the new normal.
where ambassadors could go and forget, at least for a weekend, the ideological struggle against the West.

Yet according to the State Department, these compounds also served as extremely comfortable spy nests. "Under the Foreign Missions Act, we have the authority to restrict their access to these properties based on their pattern of behaviour," a US official said, discussing the decision to close both compounds.

One of the alleged spy nests is on Long Island, where the Russian government owns a mansion in Oyster Bay and a sprawling estate in the nearby town of Glen Cove. It was not clear which of the two would be closed. The estate, known as Killenworth, was bought by the Soviet Union in 1951, apparently for staff at the Russian mission to the UN. In 1982 the Reagan administration claimed that the Russians had been using the estate to eavesdrop on defence contractors and technology companies on Long Island.

The council in Glen Cove had long complained that the Russians were not paying property taxes. Councillors decided, by six votes to one, that the Russians would no longer be given free beach passes. Nor would they be allowed to buy seasonal passes to tennis courts and the golf course.

As for the Oyster Bay mansion, according to Comrade J, a book published in 2009 by Pete Earley, this was set aside for intelligence officials. Judith Berkheimer, who rents a cottage opposite the mansion, told BuzzFeed News that the upper floor of the cottage had previously been rented by the FBI, which put cameras and listening devices in the trees. The landlord, Dan Travers, told the website that the FBI had indeed rented their cottage. He and his wife had once received a call from the compound to hear a Russian voice, speaking in broken English, informing them that "they had our dog". The animal had wandered off, Mr Travers said. The Russians returned it. Contacted yesterday, Mr Travers said he was reluctant to speak further on the matter. The other property the Americans are closing down is a Georgian pile on a peninsula in Chesapeake Bay, Maryland. Bought in 1972, it has a football pitch and a tennis court. A reporter who visited in 1987 saw three employees of the Soviet embassy in a rowing boat about 200 yards off the peninsula, smoking cigarettes and drinking beer.

Residents said that the Russians were pleasant neighbours who sometimes invited them to parties.

More recently, Washington Life Magazine in a profile of the Maryland dacha said that the grounds were "lushly planted with magnolias, cypress and boxwood", and the Russian ambassador maintained a collection of porcelain statues there. There was also a sauna, steam room and "hunting lodge".

LOAD-DATE: December 31, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: TIM

Copyright 2016 Times Newspapers Limited
All Rights Reserved

Return to List

3 of 100 DOCUMENTS

DAILY MAIL (London)

December 30, 2016 Friday

HAPPY NEW YEAR HERE COME THE WRAPPING PAPER POLICE

LENGTH: 1514 words

COLUMN
Trust the recycling nazis to find a way of criminalising Christmas. They have belatedly announced that they won’t be collecting millions of tons of the wrong kind of wrapping paper.

Apparently, festive greetings cards and paper made with glitter contaminate refuse and are only fit for landfill.

Some types of cardboard also pose a clear and present danger to the polar bears, especially if they’ve been sealed with sticky tape.

As for tinsel, plastic baubles and paper napkins with traces of mince pie or figgy pudding, forget it. You might just as well fill your dustbin with nuclear waste.

Councils from Hampshire and Exeter to South Tyneside have declared that dustmen will not take away any environmentally unfriendly wrapping paper put out for collection. Presumably, they will be sending crack teams of uniformed inspectors to sift through bins for offending items. Otherwise, how will they know what horrors are lurking beneath layers of Christmas debris?

You may be labouring under the misapprehension that you have diligently sorted your rubbish into anything up to seven different containers. More fool you. What you should also have done is conduct a scrunch test to see if your wrapping paper and boxes could be recycled.

This involves crumpling the stuff in your hand. If it stays screwed up, it's probably safe to recycle. If it springs back, it is likely to contain some kind of metallised plastic film and is therefore verboten.

A rogue sliver of sticky tape, a glimpse of glitter or a tincture of tinsel will be enough to ensure you fall foul of the Wrapping Paper Police.

Naturally, they didn't bother imparting any of this vital information until after the event. That's because their intention is not to help us recycle, but to catch us out.

And once they've found an infringement, you can bet your life a hefty fine will follow. There's nothing these greedy, officious jobsworths enjoy more than boosting their coffers by issuing penalty notices for an exciting and ever-expanding array of environmental crimes.

One of the reasons the so-called Snooper's Charter has encountered so much justified opposition is not because it gives the Funny People and the anti-terror boys the power to monitor the phone records and internet activity of jihadists.

It's because the rules have been extended to enable tinpot tyrants in Town Halls to mount military-style surveillance operations against people suspected of minor offences, however anti-social, such as letting their dogs foul the footpaths.

How many more times? If you give these people any modicum of authority, they will always, always, always abuse it.

Rather than invest this money in making our lives easier for instance, buying modern recycling machines that automatically separate different types of rubbish they use it to expand their empires. As I've told you for years, we live in an advanced punishment culture, designed deliberately to invert the relationship between the paying public and so-called public servants.

I probably get more letters and emails about our deranged rubbish collection and recycling regimes than anything else.

These vary in degrees of insanity from council to council, but are all intended to pick our pockets and cause us the maximum possible inconvenience.

The only other topic which regularly comes close is the war on motorists, whether it's the rip-roaring bonkers reduction in road space to provide deserted cycle lanes; the way in which traffic calming has turned most of our city streets into crazy golf courses; or the zealous enforcement of parking restrictions. Nowhere does frustration boil over more frequently than in NHS car parks, where if you can find a space you are treated as a cash cow at best and a criminal at worst.

Some years ago I wrote about visiting my mum in hospital in Michigan, where she lives. What struck me as I arrived was the valet parking at the front door.

Talk about a brilliant idea. When you are rushing to see a sick relative, or make a pressing appointment, you've got better things to do than search for a parking space or worry about getting out in time to avoid having to pay a hefty fine.

At five dollars a pop it was cheap at half the price.
Here in Britain, you can forget about valet parking. You're more likely to encounter the wheel-clampers.

OK, so we don't have the space to offer valet parking at all our NHS hospitals. But we do have a duty to make a hospital visit as stress-free as humanly possible.

I accept there has to be a system to deter shoppers and commuters from clogging up hospital car parks. But surely it is not beyond the wit of the NHS bureaucracy to come up with a simple system of getting parking tickets validated for genuine patients and visitors.

Palming off parking to private operators has only served to make things ten times worse. In most cases these so-called respectable' companies are no better than backstreet cowboy clammers.

The Daily Mail this week exposed how hospital visitors are being taken for a ride. One woman attending Lichfield hospital for an X-ray was given a £70 ticket for staying just 13 seconds over her allotted time. Patients visiting London's Royal Free Hospital are being charged even before they reach the car park. Their number plates are clocked on camera as they are queuing to get in. This sinister CCTV system is reminiscent of a maximum-security prison, not a hospital.

Often, once inside, there are no parking places available. Despite this, drivers are still charged for the time they spend looking for somewhere to park before leaving.

NHS Trusts raked in a record £120 million in parking fees last year. But the private enforcement firms they employ get to keep all the fines they impose which gives them a clear incentive to resort to entrapment, exorbitant penalties and sleight-of-hand.

And in an echo of the sharp practices at Britain's airports, they're even fining volunteer ambulance drivers for dropping off patients.

Funny how those who shout loudest about the NHS being free at the point of use' don't seem to have a problem with patients and visitors being robbed blind and fined anything up to a week's disposable income by the spivs who run hospital car parks.

Sorry to end the year on a sour note, but I can't be the only one whose stomach churns every time I hear our posturing politicians banging on about world-class' public services.

From the NHS to refuse collection, the concept of public service' is a sick joke a smokescreen to obscure the depressing reality that these organisations are run purely for the benefit of those who work in them, not for the mugs who pay their wages.

And if you still doubt that, just consider the respective seasonal messages of contempt from those who control refuse collection services' and hospital parking.

Maybe they should cut out the middle man and make us recycle everything in special bins in pay-and-display NHS car parks. Then they can fine us twice in the same place.

Happy New Year. You're nicked.

ON THE TWELFTH WEEK OF CHRISTMAS??.?.?.Call me a miserable old git, but how much longer can the Christmas holidays last? This week I got a stock reply to an email which said the recipient wouldn't be back in the office until January 10. Never mind the traditional 12 Days, the festive season seems to drag on from Christmas trees going up in shops and hotels in August to the first sighting of Easter Eggs in February. As Tom Robinson sang in Too Good To Be True: I've given up reading the papers, I've given up watching TV??.?.?.If I see another hackneyed review of 2016 or unfunny look at the year ahead, I'm going to lose the will to live. And if it's New Year's resolutions you're after, then you've come to the wrong place. I have just one sincere wish for 2017. That's the fervent, if forlorn, hope that I never read another news' story that begins: A Twitter storm erupted last night???.??.'AAAAAARRRRRGGGGH!!

The reason this column carries so many daft shaggy dog stories is because I know how much you all enjoy Gary's brilliant animal cartoons. So I couldn't resist bringing you the latest bulletin from the RSPCA. Among the more bizarre operations its officers mounted this year was rescuing a sheep in Hertfordshire with its head trapped inside a traffic cone. It is not known whether the sheep had been out on a stag night with a gang of Oompa Loompas. They were also called upon to free a snake stuck in a vacuum cleaner and a schnauzer called Bruno who managed to get his head jammed between some fence railings. It's what dogs do. My favourite was a seagull that fell into a vat of curry and turned orange. Can we be certain this was an accident? There have been a number of stories this year about seagulls terrorising holidaymakers in seaside resorts, swooping down and stealing their
fish and chips. Maybe this time Jonathan Livingston Seagull bit off more than he could chew and decided to try his luck in a failed smash and grab raid on an Indian restaurant, which ended up with him on the menu as dish of the day. I've heard of duck l'orange, so why not seagull?..?.

© Daily Mail

LOAD-DATE: December 29, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Papers

Counter Extremism Bill could lead to investigations into people 'miles away' from terrorism;
'We didn't ban communism during the Cold War, and I think we should be strong and robust enough to argue back'

BYLINE: Shaun Connolly

SECTION: HOME NEWS

LENGTH: 660 words

New anti-extremism measures planned by the Government could be "very dangerous", the terror law watchdog has warned.

Expressing serious concerns about the Counter Extremism Bill, David Anderson QC, said people who are "miles away" from terrorism could be investigated because of their religion under expected proposals to combat those with vocal or active opposition to fundamental British values.

The difficulty "is that they want to bring in an element of coercion to this process", the independent reviewer of terrorism legislation, told BBC Radio Four's World At One.

Watchdog gives green light to new spying powers

"They say that if you are going to engage in extremist activity, then you could be made subject to some coercive measure whereby you might not be able to use social media, or you might be limited in your associations, or in where you can go, and so on," he said.

"I think silence coerced by law ... is a very dangerous business, particularly when you are looking at something as vague as extremism.

"I've not met anyone who can really define it in a satisfactory way.

"There's talk of British values, people who oppose diversity, democracy, the rule of law, tolerance. We can all think of people, I'm sure, we would love to see silenced in one way or the other, preachers of hate, of whatever kind.
MI6 chief warns of 'unprecedented terror threat in UK'

"I think the trouble with rules like that is that all sorts of people are going, in principle, to be subject to them. People are going to complain about neighbours, they're going to complain about people they work with, the police are going to feel they have to investigate all sorts of people who are miles away from being terrorists, but may just practise religion in a conservative way, or may have eccentric political views.

"That's not really the way we have ever done things in this country. We didn't ban communism during the Cold War, and I think we should be strong and robust enough to argue back.

"To start applying the force of the law to people who oppose certain values, I think, is a really difficult and dangerous line to go down," he said.

Asked if such provisions in the Bill could themselves be opposed to fundamental British values, Mr Anderson, who is to stand down from his review of terror laws role in February, said: "That's of course one way of putting it."

Mr Anderson said he expected changes to the controversial Investigatory Powers Act, which some have branded a "snooper's charter", after the European Court of Justice ruled that measures in it allowing the "general and indiscriminate retention" of emails and other electronic communications were illegal.

Read more

New counter-extremism strategy 'could make fight even harder'

Archbishop intervenes to stop anti-terror laws hitting Sunday schools

Government's counter-extremism plans risk creating 'thought police'

Criminalising people for thinking bad thoughts spreads extremism

He said provisions in the Act making telephone providers retain call logs for 12 months in case police want to look at them made sense.

"It certainly does look as though in some respects the Act is going to have to be amended. My own view is that the power is a particularly useful one to the police, and not only in terrorism cases, and it's actually not very intrusive at all," he said.

Mr Anderson said the UK had learned lessons after an "overreaction" following 9/11.

Asked if Britain had the balance right on anti-terror laws, he said: "I would say we are not in too bad a place. We made some terrible mistakes in the past. I think we really went over the top in Northern Ireland in the 1970s. In ways that I think are still having bad effects, and everyone can see that now.

"Even 10 years ago, we maybe overreacted in ways that we shouldn't have done to the 9/11 bombings. But, I think what we have done is learn from that. The laws I'm reviewing now are actually less onerous, less restrictive than the ones I started to review in 2010/11."
Warning: UK Government can record EVERYTHING you click on online from today under new 'Snooper's Charter'

BYLINE: CHRIS SUMMERS FOR MAILONLINE

SECTION: NEWS

LENGTH: 332 words

In November Investigatory Powers Bill was passed and given Royal Assent
App companies must keep data for a year and police can hack your phone
An attempted amendment to the law from the Lords was rejected by MPs
The Government sees it as essential for tackling organised crime

Police are now officially able to hack into your phones and check your browsing history after the Snooper’s Charter came into force today.

The law - officially called the Investigatory Powers Bill - forces electronic data to be stored by app companies for 12 months, which can be subsequently collected by law enforcement.

While critics have cited it as an attack on privacy, the Government believes the charter is essential for combating terrorism and organised crime.

The legislation replaces the Regulation of Investigatory Powers Act, which several local authorities have been accused of abusing to snoop on people feeding pigeons and failing to clear up dog mess.

The Act was passed by the House of Lords in November, after they backed down on an amendment that would have forced the press to pay court costs for both parties in any case involving allegations of phone or email hacking, even if they were completely spurious.

One peer said it would have 'chilled' journalism and stopped papers writing about figures such as ex-BHS boss Sir Philip Green.

The following day the Lords accepted defeat in what will be seen as a victory for Press freedom.

Aside from the controversy surrounding its morality, the charter's effectiveness has also been questioned, with Virtual Private Network software already being highlighted as a potential way for internet users of getting around it.

Using a VPN means data will be scrambled and protected from the company that provides the connection.

In China VPNs are routinely used by expats to avoid Beijing's rigid control of the internet, which involves blocking news websites like the BBC, anything which might be remotely critical of the Chinese Communist Party, and porn websites.

LOAD-DATE: December 30, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

JOURNAL-CODE: WEBDM

Copyright 2016 Associated Newspapers Ltd.
All Rights Reserved

Return to List

6 of 100 DOCUMENTS
Happy New Year - here come the Wrapping Paper Police: RICHARD LITTLEJOHN on how the concept of 'public services' is a sick joke

BYLINE: RICHARD LITTLEJOHN FOR THE DAILY MAIL

SECTION: RIGHTMINDS

LENGTH: 1504 words

Trust the recycling nazis to find a way of criminalising Christmas. They have belatedly announced that they won’t be collecting millions of tons of the ‘wrong’ kind of wrapping paper.

Apparently, festive greetings cards and paper made with glitter ‘contaminate’ refuse and are only fit for landfill.

Some types of cardboard also pose a clear and present danger to the polar bears, especially if they’ve been sealed with sticky tape.

As for tinsel, plastic baubles and paper napkins with traces of mince pie or figgy pudding, forget it. You might just as well fill your dustbin with nuclear waste.

Councils from Hampshire and Exeter to South Tyneside have declared that dustmen will not take away any environmentally unfriendly wrapping paper put out for collection. Presumably, they will be sending crack teams of uniformed inspectors to sift through bins for offending items. Otherwise, how will they know what horrors are lurking beneath layers of Christmas debris?

You may be labouring under the misapprehension that you have diligently sorted your rubbish into anything up to seven different containers. More fool you. What you should also have done is conduct a ‘scrunch’ test to see if your wrapping paper and boxes could be recycled.

This involves crumpling the stuff in your hand. If it stays screwed up, it’s probably safe to recycle. If it springs back, it is likely to contain some kind of metallised plastic film and is therefore verboten.

A rogue sliver of sticky tape, a glimpse of glitter or a tincture of tinsel will be enough to ensure you fall foul of the Wrapping Paper Police.

Naturally, they didn’t bother imparting any of this vital information until after the event. That’s because their intention is not to help us recycle, but to catch us out.

And once they’ve found an infringement, you can bet your life a hefty fine will follow. There’s nothing these greedy, officious jobsworths enjoy more than boosting their coffers by issuing penalty notices for an exciting and ever-expanding array of ‘environmental crimes’.

One of the reasons the so-called Snoopers’ Charter has encountered so much justified opposition is not because it gives the Funny People and the anti-terror boys the power to monitor the phone records and internet activity of jihadists.

It’s because the rules have been extended to enable tinpot tyrants in Town Halls to mount military-style surveillance operations against people suspected of minor offences, however anti-social, such as letting their dogs foul the footpaths.

How many more times? If you give these people any modicum of authority, they will always, always, always abuse it.

Rather than invest this money in making our lives easier - for instance, buying modern recycling machines that automatically separate different types of rubbish - they use it to expand their empires. As I’ve told you for years, we live in an advanced punishment culture, designed deliberately to invert the relationship between the paying public and so-called public ‘servants’.

I probably get more letters and emails about our deranged rubbish collection and recycling regimes than anything else.
These vary in degrees of insanity from council to council, but are all intended to pick our pockets and cause us the maximum possible inconvenience.

The only other topic which regularly comes close is the war on motorists, whether it's the rip-roaring bonkers reduction in road space to provide deserted cycle lanes; the way in which 'traffic calming' has turned most of our city streets into crazy golf courses; or the zealous enforcement of parking restrictions. Nowhere does frustration boil over more frequently than in NHS car parks, where - if you can find a space - you are treated as a cash cow at best and a criminal at worst.

Some years ago I wrote about visiting my mum in hospital in Michigan, where she lives. What struck me as I arrived was the valet parking at the front door.

Talk about a brilliant idea. When you are rushing to see a sick relative, or make a pressing appointment, you've got better things to do than search for a parking space - or worry about getting out in time to avoid having to pay a hefty fine.

At five dollars a pop it was cheap at half the price.

Here in Britain, you can forget about valet parking. You're more likely to encounter the wheel-clampers.

OK, so we don't have the space to offer valet parking at all our NHS hospitals. But we do have a duty to make a hospital visit as stress-free as humanly possible.

I accept there has to be a system to deter shoppers and commuters from clogging up hospital car parks. But surely it is not beyond the wit of the NHS bureaucracy to come up with a simple system of getting parking tickets validated for genuine patients and visitors.

Palming off parking to private operators has only served to make things ten times worse. In most cases these so-called 'respectable' companies are no better than backstreet cowboy clampers.

The Daily Mail this week exposed how hospital visitors are being taken for a ride. One woman attending Lichfield hospital for an X-ray was given a £70 ticket for staying just 13 seconds over her allotted time. Patients visiting London's Royal Free Hospital are being charged even before they reach the car park. Their number plates are clocked on camera as they are queuing to get in. This sinister CCTV system is reminiscent of a maximum-security prison, not a hospital.

Often, once inside, there are no parking places available. Despite this, drivers are still charged for the time they spend looking for somewhere to park before leaving.

NHS Trusts raked in a record £120 million in parking fees last year. But the private enforcement firms they employ get to keep all the fines they impose - which gives them a clear incentive to resort to entrapment, exorbitant penalties and sleight-of-hand.

And in an echo of the sharp practices at Britain's airports, they're even fining volunteer ambulance drivers for dropping off patients.

Funny how those who shout loudest about the NHS being 'free at the point of use' don't seem to have a problem with patients and visitors being robbed blind and fined anything up to a week's disposable income by the spivs who run hospital car parks.

Sorry to end the year on a sour note, but I can't be the only one whose stomach churns every time I hear our posturing politicians banging on about 'world-class' public services.

From the NHS to refuse collection, the concept of 'public service' is a sick joke - a smokescreen to obscure the depressing reality that these organisations are run purely for the benefit of those who work in them, not for the mugs who pay their wages.

And if you still doubt that, just consider the respective seasonal messages of contempt from those who control refuse collection 'services' and hospital parking.

Maybe they should cut out the middle man and make us recycle everything in special bins in pay-and-display NHS car parks. Then they can fine us twice in the same place.

Happy New Year. You're nicked.

The reason this column carries so many daft shaggy dog stories is because I know how much you all enjoy Gary's brilliant animal cartoons. So I couldn't resist bringing you the latest bulletin from the RSPCA.
Among the more bizarre operations its officers mounted this year was rescuing a sheep in Hertfordshire with its head trapped inside a traffic cone. It is not known whether the sheep had been out on a stag night with a gang of Oompa Loompas.

They were also called upon to free a snake stuck in a vacuum cleaner and a schnauzer called Bruno who managed to get his head jammed between some fence railings. It's what dogs do. My favourite was a seagull that fell into a vat of curry and turned orange. Can we be certain this was an accident?

There have been a number of stories this year about seagulls terrorising holidaymakers in seaside resorts, swooping down and stealing their fish and chips. Maybe this time Jonathan Livingston Seagull bit off more than he could chew and decided to try his luck in a failed smash and grab raid on an Indian restaurant, which ended up with him on the menu as dish of the day. I've heard of duck l'orange, so why not seagull...

Call me a miserable old git, but how much longer can the Christmas holidays last? This week I got a stock reply to an email which said the recipient wouldn't be back in the office until January 10.

Never mind the traditional 12 Days, the festive season seems to drag on from Christmas trees going up in shops and hotels in August to the first sighting of Easter Eggs in February. As Tom Robinson sang in Too Good To Be True: I've given up reading the papers, I've given up watching TV...

If I see another hackneyed review of 2016 or unfunny look at the year ahead, I'm going to lose the will to live. And if it's New Year's resolutions you're after, then you've come to the wrong place.

I have just one sincere wish for 2017. That's the fervent, if forlorn, hope that I never read another 'news' story that begins: 'A Twitter storm erupted last night...' AAAAAARRRRGGGGGHHHH!
that it's worth their bother seems to have been the real challenge of late), isn't it high time that we cleaned up the electoral process as a whole?

For starters, I'd like to see party "donations" being blocked from anyone who isn't registered in this country for tax purposes and a similar ban placed on lobbying by any bodies which aren't based in the UK. Surely it is crucial to the national interest that we can be certain our politicians aren't being bribed - sorry, incentivised - by extra-national entities?

While we're about it, I'd be quite interested to see the House of Lords stripped of members who aren't UK resident for tax purposes, too. If our increasingly outdated notions of nobility and aristocracy are to continue to bear any weight with the population at large then those in the upper chamber ought at the very least to be seen to be making a fair contributions, rather than running private companies feeding off the NHS from tax havens.

None of this ought to be too difficult to organise, just so long as people carry their passports or identity papers around with them - which, it seems, may be what the country voted for in June.

Julian Self
Milton Keynes

It's about time the UK regularised the carrying of some form of ID. A high proportion of the population already carry some form, in my case a driving licence or bus pass, and I have no objection to being asked to produce some form of ID when voting. We need to ask why anyone would object.

Marlene Maguire
Claygate, Surrey

The government's plan to introduce a scheme of requiring identification at polling stations to prevent electoral fraud superficially sounds sensible. As far as I'm aware such fraud is not common in the UK, but small pockets of the country may have problems and eliminating this is no bad thing.

However, many lower income people could potentially be disenfranchised by the requirement to produce a passport, driving licence or even a utility bill (if they are on prepayment meters) if such documentation is required. Driving and foreign travel does not figure largely in the budgets of this group. Unless a very affordable simple photo identification, costing £2 as a ball park figure, was available, what sounds like an excellent idea could be counterproductive to democracy.

Patrick Cleary
Honiton, Devon

This proposal also disenfranchises older people. A few years ago I was trying to renew my mother's Blue Badge. As she lives in a residential home she had no current passport, utility bill or driving licence. And, no - in answer to a subsequent question - she did not hold a gun licence either.

Christine Kenrick
Address withheld

The "Snooper's Charter" crept in, and now there is talk of showing ID to vote. Look out: next will be ID cards for everything and everyone.

Dave Thomas
Bristol

Brexiteers don't oppose immigration but its effects

Assuming a "distaste for immigration" drove voters towards leave the European Union is a dangerous simplification that alienates those whose support is vital if we wish to wrest Brexit away from bigoted ideologues. It is the effects of immigration, not immigration itself, that is the problem. Everything from competition from Europeans willing and able to undercut British workers, through to competition for housing, schools and access to medical care, adds up to make uncontrolled immigration a dangerous proposition for the average British worker. Add a reduction in real wages (5 per cent since 2008) and the reasons for the result come into stark relief.
Solving these challenges requires domestic policies. Blaming the EU for our ills is a convenient cowardice. New consumer protection rules (requiring licensing for all tradesmen operating in the UK, for example), investment in social housing, education and the NHS would deliver the improvements in living standards enjoyed by our EU partners (France 10 per cent increase in real wages, Germany 14 per cent and Poland 24 per cent) and remove the forces of destruction that created Brexit.

Mark Grey
London

Terrorism must be controlled

The sobering reality of the Paris, Nice and Berlin terrorist attacks can no longer be swept under the carpet by the wishful thinking and politically correct platitudes of EU leaders. The once peacetime merits of the Schengen Agreement must now be reconsidered by a Europe that finds itself immersed in a war with Islamist terrorism.

Europe’s open borders may have made for a smoother interlocking of its cogs of commerce, but they have unwittingly provided (much like the internet) a seamless, clandestine conveyor for the contagion of Islamism. Attempting to safeguard a multinational continent like Europe from insurgent, Islamist terrorism is like trying to navigate a merchant ship through uncharted, treacherous seas.

Without secure borders it is as vulnerable as is a vessel without isolating bulkheads. A single breach of the outer hull, or a fire in any one of its internal compartments, cannot be contained, and will ultimately sink the ship. Islamist terrorism cannot be controlled and ultimately defeated if it cannot first be contained.

Therefore, before firing up its boilers and charting a course to a secure and prosperous future, the good ship Europe must now accept the increased rigidity of having to reinstate its national bulkheads.

Mark Dyer
Rockingham

Hope for Syrian ceasefire

When will the West learn? The only possible chance of a ceasefire in Syria is to support Russia against the rebels. We all know what happened in Iraq when the US and Britain removed a dictator. The Russians, Turkey and Iran have to live with their neighbours. Support their ceasefire plans, bring some semblance of order, and thousands may be able to return to their homes.

Rod Hartley
Preston

Go vegan for 2017

Many people resolve to lose weight every new year, only to find themselves no thinner in July than they were in January. This can be very frustrating, but by simply exercising and eating more wholesome vegan foods, you can look better on the outside and feel better on the inside. Not only do vegan foods taste delicious, they’re also cholesterol-free and most are low in saturated fat and calories too.

Studies have shown that vegans are nine times less likely to be obese than meat eaters. They are also known to have lower rates of many life-threatening diseases, including heart disease, diabetes, and certain cancers. And when you choose vegan foods, you also help spare animals a horrifying death at the abattoir, protect the environment and combat climate change.

Jennifer White
PETA

LOAD-DATE: December 28, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI
THE COUNCILS USING TERROR LAW TO SPY ON BARKING DOGS

BYLINE: BY KATE PICKLES

LENGTH: 571 words

COVERT surveillance powers designed to combat terrorism and organised crime have been used by councils to spy on people feeding pigeons and failing to clear up dog mess, an investigation found.

Local authorities were granted permission to carry out more than 55,000 days of covert surveillance over a five-year period using the Government's Regulation of Investigatory Powers Act (Ripa).

A Freedom of Information request has revealed that two-thirds of the 283 councils that responded had used the powers to gather evidence on members of the public.

Lancaster City Council used the Act for targeted dog fouling enforcement in two areas over a period of 11 days. Allerdale Borough Council in Cumbria targeted people feeding pigeons, while Midlothian Council went after owners of noisy dogs.

Wolverhampton went undercover to check on the sale of dangerous toys and car clocking, in which rogue dealers knock many miles off odometers, leaving owners defrauded and facing serious repair bills.

The Liberal Democrats asked for the figures, published by The Guardian, which revealed councils had launched 2,800 separate surveillance operations lasting up to 90 days each. Brian Paddick, a former Metropolitan police chief who represents the party on home affairs, said some use of the powers was absurd.

It is absurd that local authorities are using measures primarily intended for combating terrorism for issues as trivial as a dog barking or the sale of theatre tickets,' he said.

Spying on the public should be a last resort not an everyday tool.'

A Home Office spokesman pointed out that the law had since changed and Ripa could only now be used if criminal activity was suspected.

The Investigatory Powers Bill dubbed the snoopers charter by critics has incorporated Ripa with a raft of new measures including allowing police to check things such as the browsing history on people's phones. It was passed by Parliament last month. While critics have cited it as an attack on privacy, the Government believes the charter is essential for combating terrorism and organised crime.

But Lord Paddick said he was worried authorities could use powers in a way that Parliament did not intend and called for measures to ensure any surveillance was measured and proportionate.

Other councils used Ripa to check on the legitimacy of benefit claimants, while Slough investigated an illegal puppy farm.

Lincolnshire County Council topped the list for the largest number of days requested with nearly 4,000 as part of a sting on underage alcohol sales and counterfeit cigarettes. Mark Keal from Lincolnshire Trading Standards, defended its use, saying it helped successful prosecutions which got products off the streets'.

Bromley used the powers to deploy a covert camera to catch a serial fly-tipper' and as part of a crackdown on antisocial behaviour.
Deputy council leader Colin Smith told The Guardian the powers were too restrictive and that the victims of crime were in favour of filming evidence to aid prosecutions.

Most local authorities said they would typically request more days of surveillance than were used.

The Home Office said there was a rigorous authorisation procedure and independent inspection before powers were granted. Ripa powers are an important tool that local authorities can use to address the issues that affect many people’s lives, like consumer protection, environmental crime and benefit fraud,' a spokesman said.

Councils have been given permission to spy on the public for a total of more than 55,000 days during the past five years to investigate offences as minor as dog barking and feeding pigeons.

Almost 2,800 surveillance operations have been carried out by local authorities since 2011, which included the use of hidden microphones, covert cameras and private detectives.

Two thirds of local authorities revealed that they had used surveillance powers under the Regulation of Investigatory Powers Act (Ripa). Details of the use of covert council operations since 2011 released under the Freedom of Information Act revealed: ? Westminster city council used surveillance powers to examine the "misleading sales of theatre tickets". ? Allerdale borough council in Cumbria launched a covert operation to find out who was feeding pigeons.

? Wiltshire council began an operation after being told that someone was "downloading films, including the latest releases" and selling them in a www.pub. No such activity was discovered. ? Midlothian council undertook a twoweek surveillance operation to examine dog barking.

? Lancaster city council had two surveillance operations during 2012 aimed at identifying instances of dog fouling. ? Bromley borough council set up a camera on the top floor of an empty house to investigate complaints about rubbish in a back garden.

Surveillance was also used to check that benefit claimants were not making fraudulent claims and to investigate "serious incidents of graffiti".
Of the 283 councils that offered a response, 186 said they had used the powers and 97 said they had not done so in the past five years.

The councils involved in the most controversial use of the powers said that their operations were carried out before the law was strengthened at the end of 2012. Local authorities can now use the powers only to investigate a crime that carries at least six months in prison, or the sale of alcohol and tobacco to children. They also have to seek legal permission before beginning a covert operation.

However, councils continue to gain permission for surveillance covering thousands of days, with 6,684 days granted in 2015 and 3,806 this year.

Some critics are warning that the new Investigatory Powers Act will give even more public bodies access to sensitive digital information.

Brian Paddick, home affairs spokesman of the Liberal Democrats, which made the freedom of information request, said: "It is absurd that local authorities are using measures primarily intended for combating terrorism for issues as trivial as a dog barking.

"While the Investigatory Powers Act will now restrict the ability of local authorities to monitor people's communications, it will give mass surveillance powers to a huge number of government bodies."

A Home Office spokeswoman said: "Ripa powers are an important tool that local authorities can use to address the issues that affect many people's lives, like consumer protection, environmental crime and benefit fraud."

LOAD-DATE: December 26, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: TIM

The Guardian

December 25, 2016 Sunday 7:00 PM GMT

Revealed: British councils used Ripa to secretly spy on public; Local authorities used Regulation of Investigatory Powers Act to follow people, including dog walkers, over five years

BYLINE: Anushka Asthana Political editor

SECTION: WORLD NEWS

LENGTH: 1231 words

Councils were given permission to carry out more than 55,000 days of covert surveillance over five years, including spying on people walking dogs, feeding pigeons and fly-tipping, the Guardian can reveal.
A mass freedom of information request has found 186 local authorities - two-thirds of the 283 that responded - used the government's Regulation of Investigatory Powers Act (Ripa) to gather evidence via secret listening devices, cameras and private detectives.

Among the detailed examples provided were Midlothian council using the powers to monitor dog barking and Allerdale borough council gathering evidence about who was guilty of feeding pigeons. Wolverhampton used covert surveillance to check on the sale of dangerous toys and car clocking; Slough to aid an investigation into an illegal puppy farm; and Westminster to crack down on the selling of fireworks to children.

Related: Surveillance has gone too far. The jig is up | Martha Spurrier

Meanwhile, Lancaster city council used the act, in 2012, for "targeted dog fouling enforcement" in two hotspots over 11 days.

A spokeswoman pointed out that the law had since changed and Ripa could only now be used if criminal activity was suspected. The permissions for tens of thousands of days were revealed in a huge freedom of information exercise, carried out by the Liberal Democrats. It found that councils then launched 2,800 separate surveillance operations lasting up to 90 days each.

Critics of the spying legislation say the government said it would only be used when absolutely necessary to protect British people from extreme threats.

Brian Paddick, the Lib Dem peer who represents the party on home affairs, said: "It is absurd that local authorities are using measures primarily intended for combating terrorism for issues as trivial as a dog barking or the sale of theatre tickets. Spying on the public should be a last resort not an everyday tool."

He argued that the new Investigatory Powers Act, which will take in Ripa powers alongside a raft of new measures, would restrict the ability of local authorities to monitor people's communications.

But he also said it would give "mass surveillance powers to a huge number of government bodies".

"As with any legislation, there is a significant risk that authorities will use powers in a way that parliament never intended," added Lord Paddick, calling for proper oversight to ensure any surveillance is targeted and proportionate.

The freedom of information request also revealed a number of examples of councils using Ripa as a way of checking up on benefit claimants. One example was checking up on those claiming to be single parents.

Other local authorities drew on the powers to crack down on the distress caused by anti-social behaviour.

The London borough of Bromley gave one example in which they considered using a CCTV mobile unit to target three households that were causing "harassment, alarm and distress" by holding parties on a communal green with loud music blaring out through amplifiers, shouting screaming, smashing windows and riding motorbikes around in circles.

The local authority also detailed the use of Ripa following complaint about the accumulation of rubbish in a rear garden, claiming the perpetrator was a "serial fly tipper". The council deployed a "covert camera" in the upstairs, bedroom window of another property, which gathered evidence of what was happening.

More recently it has used the law to monitor the sale of alcohol, tobacco and fireworks to people underage, and capture those illegally dumping waste in recycling centres.

The deputy leader of the London borough of Bromley said he believed the legislation was far too restrictive, arguing that the victims of crime understood that filming evidence that could aid prosecutions was a "minor infringement of the perpetrators so called civil liberties".

Councillor Colin Smith said: "Council officers deal with complaints day in and day out about thoroughly disgusting socially inadequate individuals fly-tipping waste and preying on the weaker, more vulnerable members of our society, normally the elderly, and this technology is key to bringing their worst excesses to heel."

He said the council kept to the letter of the law to prevent any "so called 'spying' taking place on law-abiding individuals"
"I'm frankly far more concerned about the rights and civil liberties of the victims and wider council tax paying public who are currently having to pick up the tab, than the small minority criminal element who continue to treat the rest of us with open contempt."

Lincolnshire County Council had requested permission the largest number of days - close to 4,000, with a major 2012 operation to prevent cigarettes and alcohol being sold to underage teenagers, and attempts to stop counterfeiting at car boot sales and markets.

Mark Keal from Lincolnshire Trading Standards, said: "Without this evidence it is incredibly difficult to get successful prosecutions and get these products off the street."

The council - alongside a number of others - stressed that while they had sought permission for a large number of days, the operations usually spanned over a much shorter period.

The next highest number of days requested was Birmingham where acting strategic director, Jacqui Kennedy, said the powers had been used to crack down on "serious fly-tipping, rogue trader operations and trading standards investigations looking at scams and counterfeiting".

"We only use Ripa when it is proportionate and reasonable and each application is agreed and signed off by a judge," she added, insisting that it had helped catch out criminals. "And as the largest local authority in the country we frequently top statistics lists that are based solely on raw numbers."

The Home Office insisted that permissions were only ever granted for such covert surveillance after a rigorous authorisation procedure and independent inspection.

A spokesman said: "Ripa powers are an important tool that local authorities can use to address the issues that affect many people's lives, like consumer protection, environmental crime and benefit fraud.

"The legislation makes clear that public authorities may use these techniques only when it is both necessary and proportionate to do so.

Related: 'Extreme surveillance' becomes UK law with barely a whimper

"Any local authority use of these powers must be independently authorised by a magistrate, who is an independent judicial figure.

"The Investigatory Powers Act goes further by ensuring that in future the use of these powers will be overseen by the Investigatory Powers Commissioner, who will be a serving or former senior judge."

The new act, which has been branded a snooper's charter by critics, faced difficulties after the EU's highest court ruled that "general and indiscriminate retention" of emails and electronic communications was illegal.

Only targeted interception of traffic and location data in order to combat serious crime - including terrorism - is justified, according to a long-awaited decision by the European court of justice (ECJ) in Luxembourg.

Ironically, the finding came in response to a legal challenge initially brought by the Brexit secretary, David Davis, when he was a backbench MP, and Tom Watson, Labour's deputy leader, over the legality of GCHQ's bulk interception of call records and online messages.
The councils using terror law to spy on barking dogs and people who feed pigeons: Local authorities given permission to carry out 55,000 hours of surveillance over the past five years

BYLINE: KATE PICKES FOR DAILY MAIL
SECTION: NEWS
LENGTH: 608 words

An investigation uncovered that some councils have been spying on the public. Councils launched 2,800 separate surveillance operations lasting up to 90 days. Former Metropolitan police chief Brian Paddick called it ‘absurd.’

Covert surveillance powers designed to combat terrorism and organised crime have been used by councils to spy on people feeding pigeons and failing to clear up dog mess, an investigation found.

Local authorities were granted permission to carry out more than 55,000 days of covert surveillance over a five-year period using the Government's Regulation of Investigatory Powers Act (Ripa).

A Freedom of Information request has revealed that two-thirds of the 283 councils that responded had used the powers to gather evidence on members of the public.

Lancaster City Council used the Act for 'targeted dog fouling enforcement' in two areas over a period of 11 days.

Allerdale Borough Council in Cumbria targeted people feeding pigeons, while Midlothian Council went after owners of noisy dogs.

Wolverhampton went undercover to check on the sale of dangerous toys and car clocking, in which rogue dealers knock many miles off odometers, leaving owners defrauded and facing serious repair bills.

The Liberal Democrats asked for the figures, published by The Guardian, which revealed councils had launched 2,800 separate surveillance operations lasting up to 90 days each.

Brian Paddick, a former Metropolitan police chief who represents the party on home affairs, said some use of the powers was absurd.

'It is absurd that local authorities are using measures primarily intended for combating terrorism for issues as trivial as a dog barking or the sale of theatre tickets,' he said.

'Spying on the public should be a last resort not an everyday tool.’

A Home Office spokesman pointed out that the law had since changed and Ripa could only now be used if criminal activity was suspected.

The Investigatory Powers Bill - dubbed the snoppers’ charter by critics - has incorporated Ripa with a raft of new measures including allowing police to check things such as the browsing history on people's phones.

It was passed by Parliament last month. While critics have cited it as an attack on privacy, the Government believes the charter is essential for combating terrorism and organised crime.

But Lord Paddick said he was worried authorities could use powers in a way that Parliament did not intend and called for measures to ensure any surveillance was measured and proportionate.

Other councils used Ripa to check on the legitimacy of benefit claimants, while Slough investigated an illegal puppy farm.

Lincolnshire County Council topped the list for the largest number of days requested with nearly 4,000 as part of a sting on underage alcohol sales and counterfeit cigarettes.
Mark Keal from Lincolnshire Trading Standards, defended its use, saying it helped successful prosecutions which got ‘products off the streets’.

Bromley used the powers to deploy a covert camera to catch a ‘serial fly-tipper’ and as part of a crackdown on antisocial behaviour.

Deputy council leader Colin Smith told The Guardian the powers were too restrictive and that the victims of crime were in favour of filming evidence to aid prosecutions.

Most local authorities said they would typically request more days of surveillance than were used.

The Home Office said there was a rigorous authorisation procedure and independent inspection before powers were granted.

‘Ripa powers are an important tool that local authorities can use to address the issues that affect many people’s lives, like consumer protection, environmental crime and benefit fraud,’ a spokesman said.
The British people will be more under threat as a result of this judgment by EU judges sat in their ivory towers.'

In a ruling released yesterday, while the Berlin terror suspect was still on the run, the ECJ condemned rules that force communications companies to store huge amounts of personal information routinely.

It said the general and indiscriminate retention' of phone and email records was unlawful - potentially wrecking Downing Street's plans to bolster surveillance to fight terrorism.

It came as Europe reeled from the terror strike at a market in Berlin, which left 12 dead.

The case relates to the Data Retention and Investigatory Powers Act (DRIPA) that requires telecommunications firms to collect metadata' - including who a person called, emailed or texted, where from and when, but not the contents of a message - for up to a year.

This expires on December 31 and will be replaced by the expanded Investigatory Powers Act - described by critics as a turbo-charged snooper's charter'. That would also make service providers such as BT, Sky or TalkTalk store details of internet visits for a year.

The existing powers under DRIPA were ruled illegal by the High Court after a challenge, and the ECJ was asked to make a ruling by the Court of Appeal in London.

Yesterday, the ECJ found that only targeted retention to fight serious crime could justify such interference by the state.

It said the indiscriminate' storing of communications data exceeds the limits of what is strictly necessary and cannot be considered justified'.

The ECJ also said the legislation was illegal because it allowed the police and other public bodies, including the NHS, to authorise their own requests for data instead of having to ask a court.

The case will now return to the Court of Appeal. It will embarrass Theresa May - especially as Brexit Secretary David Davis had been among those who took the case to the ECJ.

Assistant Chief Constable Richard Berry, of the National Police Chiefs' Council, said: Changes that impede our ability to access data quickly with safeguards will undermine our ability to keep people safe.'

Martha Spurrier, of the campaign group Liberty, said the Government would have to amend IPA.

Lib Dem peer Lord Paddick said the Act would create an Orwellian nightmare'.

The Home Office said the Government would put forward a robust' appeal.

David Anderson QC, the outgoing terror laws watchdog, said this year that harvesting communications data had been key to stopping jihadists bringing bloodshed to Britain.

© Daily Mail
Palace is put on lockdown

SECTION: NEWS; Pg. 7

LENGTH: 151 words

COUNTER-terrorism police heightened security measures around Buckingham Palace yesterday in the wake of the Berlin attacks.

Extra road closures and traffic restrictions were imposed ahead of the Changing of the Guard. Armed police stood at barriers blocking the main routes to the Victoria Memorial outside the palace’s main gates. Constitution Hill and Spur Road were shut and The Mall was partially closed for nearly two hours. At 11.30am, the guard marched from Wellington Barracks to the palace.

Mounted officers, police cars and bicycles were stationed at various points in the cordoned-off area. The move did not dissuade tourists, with many gathering to watch. Ministers are under pressure to redraw the "snoopers' charter" after judges ruled the "general and indiscriminate" retention of communications data is illegal. The Government claims it needs new spying powers to tackle terrorism and other crime.

LOAD-DATE: December 22, 2016

LANGUAGE: ENGLISH

GRAPHIC: patrol Cop at palace yesterday

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: DMR

European court rules 'indiscriminate' UK mass surveillance law to be illegal

BYLINE: Madhumita Murgia and George Parker in London and Jim Brunsden in Brussels

SECTION: FRONT PAGE - FIRST SECTION; Pg. 1

LENGTH: 368 words

Britain’s surveillance laws have been deemed illegal by the European Court of Justice in a case that throws into question the fate of the UK’s new Investigatory Powers Act.

The ECJ ruled the legislation was illegal because it allowed "general and indiscriminate" retention of electronic communications. The judgment said member states could perform "targeted retention of
that data solely for the purpose of fighting serious crime" but not the mass and indiscriminate data collection of everyone in Britain allowed by a new UK spying regime.

This type of legislation "cannot be considered to be justified within a democratic society, as required by the directive, read in the light of the Charter", the ECJ said, referring to the charter of European human rights.

The Home Office said it was "disappointed" with the judgment and would consider its implications.

One of the politicians who brought the case was David Davis, now the Brexit minister. He withdrew from the action after becoming Brexit secretary in July.

Mr Davis brought the case under the Data Retention and Investigatory Powers Act 2014, together with Tom Watson, deputy leader of the Labour party. Although Dripa is due to be repealed by the end of this year, the Investigatory Powers Act will be adopted in 2017. The latter significantly expands the mass data-gathering powers challenged in this case.

The new law compels internet and phone companies to keep records of every phone call made and every website visited by users for 12 months. Not only would telecoms companies have a list of every site visited or call made, they would also record the date, time and duration of these actions.

Dozens of public organisations and departments ranging from the police, HM Revenue & Customs and intelligence agencies, to the NHS, the Department of Health, the Food Standards Agency and the Gambling Commission, will be able to access the communications of people in Britain, in some cases without a warrant.

Even though the UK is set to leave the EU and the ECJ's jurisdiction, the decision poses a problem for London as EU rules do not allow exchange of personal data with countries that do not comply with its privacy regime.

Business in a quandary page 3
The ruling by the European Court of Justice that Britain's surveillance laws are illegal creates another large source of post-Brexit uncertainty for UK businesses as they grapple with the prospect of life outside the bloc.

EU rules forbid the sharing of personal data with countries that do not meet its strict data privacy standards, as the US has repeatedly discovered. This year, officials on both sides of the Atlantic had to cobble together a new deal on data transfers after a previous one - itself a result of laborious negotiation - was struck down by the European courts. The new deal, known as Privacy Shield, was essential to provide a legal means for businesses to transfer personal data online - whether payslips, pictures or healthcare data - to the US from the EU without falling foul of Europe's privacy regulations.

Yesterday's ruling means Britain could struggle to convince the EU that its data protection standards are up to scratch. This could create headaches not only for companies but also for law enforcement authorities.

"The government is breaking the law by indiscriminately collecting the nation's internet activity and phone records and letting hundreds of public bodies grant themselves access to these personal details with no suspicion of serious crime and no independent sign-off, meaning significant parts of its new 'snooper's charter' are effectively unlawful," said Liberty, the human rights organisation.

Lawyers believe the ECJ's ruling will force the hand of the government to amend the legislation and limit its remit. "The provisions in the two laws are extremely similar so it is perfectly logical that the rationale will apply equally to the new [act], and it will have to be amended," said Richard Cumbley, partner at Linklaters, the law firm.

"There is no doubt the government, if it takes on board the decision, will have to apply more restrictive rules both to the types of data stored and the conditions under which it can be accessed."

Large swaths of the Investigatory Powers Act will remain unaffected by the ECJ ruling, however, including the ability to "bulk hack" citizens' communications and force technology companies to create a backdoor into their products.

Tom Watson, Labour deputy leader, one of the politicians who brought the original challenge to the surveillance legislation, said the ECJ's ruling showed that it was "counterproductive to rush new laws through parliament without a proper scrutiny".

He added: "At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past. Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe, but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit. It's for judges, not ministers, to oversee these powers."
Politics is a rough trade, but Jamie Reed should be hanging in there;
The Corbyn critic has every reason to feel less then thrilled about being a Labour MP right now. But he has a duty to his constituents, and to democracy itself

BYLINE: Polly Toynbee
SECTION: OPINION
LENGTH: 938 words

To be elected as a member of parliament is as near as we get in these humanistic days to a sacramental role - ordained not by God but by us, the people. Each MP may be just another twig of Kant's "crooked timber of humanity", out of which "no straight thing was ever made", but they each stand as the living representative of our right to choose who governs over us. For that reason, when they resign they undermine the sense of heavy obligation to their voters that they willingly undertook when they stood for election.

Jamie Reed has announced he is standing down from his Copeland seat to return to a job he prefers, back at Sellafield, his old employer. He has given the Guardian his reasons, among them that representing his large, scattered, mainly rural constituency, far from Westminster, means it's "very difficult being a long-distance dad" to his four children.

Well, yes, it is. And he may have his personal reasons. But it always was a gruelling sacrifice, and this son of Whitehaven signed up for it, reconfirming himself in the role only last year in the general election. It is decadent and contemptuous of the democratic process to walk away, as you might from any ordinary job.

To be elected by the people is no ordinary calling, for which reason I have always emphasised that a certain measure of respect is due to MPs, even the ones I detest, against the dangerous tide of contempt for their calling.

How odd, it seems to me, is the reverence we have for "democracy", willing to impose it on other countries at the point of a gun, and yet the office-holders of democracy are held in even lower esteem than journalists.

Whatever cynical old Westminster hands may say, I am still struck with awe each time I enter the cathedral-like Houses of Parliament: the stones of Westminster hall have a very particular smell of history. The statue of Cromwell outside stands guard, along with Simon de Montfort on horseback. Yes, it's an absurdly kitsch pastiche of a building, and the history of the long march to an infuriatingly inadequate form of democracy can be over-romanticised. But nonetheless, don't take it for granted. Pause for a moment to consider the fate of the billions who are without the freedom to throw the bastards out.

There have been several frivolous or vainly self-publicising byelections, expensive and irritatingly pointless. It was good to see Zac Goldsmith get his comeuppance for a silly gesture. David Davis deserved, but didn't get, the same for his quixotic resignation and re-election over civil liberties - though he now seems perfectly happy to sit in a cabinet trying to force through the snooper's charter.

The resignation of the little-known Tory MP Stephen Phillips was an utter mystery, since he had just stood last year on a manifesto he now purports to find repugnant, as he returns to his lucrative lawyering.

Jamie Reed has every reason to feel miserable about his fate as a Labour MP right now. Politics is a rough trade that eats many or most of its practitioners. Clever people who could achieve much more in the world outside give up all else to sit on the backbenches for most of their career, large slabs of it with their party out of office. Even if they make it, briefly, to become minister-for-obeying-your-senior minister, even if they make it briefly to the cabinet, the chances are that they will end their careers unable to point to any one thing they did that wouldn't have happened without them.

Some do. Barbara Castle's lifesaving 70mph speed limit; Patricia Hewitt's smoking ban; Harriet Harman's childcare and nurseries; Roy Jenkins's great 1960s "permissive society is a civilised society" reforms; or David Steel's Abortion Act. But personal achievements are few.
And Reed's fate is faced by many Labour MPs. He's a remainer in a 62% Brexit constituency. He has been a vitriolic opponent of his leader, resigning a minute after Corbyn's re-election this year. He is pro-nuclear, the vital industry for his constituents, who are looking angrily at a Labour party led by an anti-nuclear campaigner. His seat boundaries will be redrawn, obliging him to fight with next door Sue Hayman, MP for Workington.

That's a nasty nexus of wicked issues. But maybe he resigned to embarrass Corbyn, hoping finally to persuade the leader's deluded followers that Labour is destined for a defeat so devastating it might be terminal. This marginal seat may easily be lost to the Tories or even Ukip. But think what harm that does, either giving Theresa May a much needed extra seat to bolster her narrow Commons majority - or, even worse, giving Ukip immense new credibility that will do great damage.

Labour MPs are being tested as never before. Reading the abuse directed at Reed from the left - "I always thought he was a Tory," "He'll be happier destroying the planet," and much worse - it's fair to say his own venting against Corbynism has also been pretty savage. But who would want to spend their life in that toxic zone of hatred and rage?

The answer is, those who chose to stand have a duty to stay and fight - for their party's future, for their constituents against the worsening cuts, and for the country in its Brexit hour of extreme peril.

There are rumours others may follow Reed out of the door, but they must each find their own path to navigate through the thickets. To be true to their constituents, this means finding the bravery to be honest with them about the Brexit dangers ahead and the need for compromise. Many elected in Labour's easy years are having to learn late in life what it takes to stand up and fight, not cut and run, when the going gets tough.

**European court rules against 'indiscriminate' snooper's charter; JUSTICE**

**BYLINE:** Harriet Agerholm

**SECTION:** NEWS; Pg. 9

**LENGTH:** 383 words

The so-called snooper's charter is set to face a series of new legal challenges after the EU's highest court ruled the Government's "general and indiscriminate retention" of emails is illegal.

Only targeted information-gathering is justified, the European Court of Justice (ECJ) ruled, boosting the case against the sweeping collection of emails, text messages and internet data. The
Investigatory Powers Act passed into law in November, granting the Government far-reaching new abilities that allow it to indiscriminately hack and store data relating to internet use.

The case was brought to the ECJ by the now Brexit Secretary David Davis when he was a backbencher. He was joined by Labour's deputy leader, Tom Watson, in bringing the case, and the pair had already gained a High Court victory on the issue in 2015. But after the Government appealed the decision, the case was taken to the ECJ. Mr Davis (inset) withdrew from the legal challenge when he became Brexit Secretary in July this year.

Mr Watson said: "This ruling shows it's counter-productive to rush new laws through Parliament without a proper scrutiny. At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past."

Martha Spurrier, director of Liberty, which supported the MPs in bringing the case, said: "Today's judgment upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant. The Government must now make urgent changes to the Investigatory Powers Act to comply with this. The UK may have voted to leave the EU - but we didn't vote to abandon our rights and freedoms."

The Government has vowed to appeal against the decision. A Home Office spokesperson said: "We are disappointed with the judgment from the European Court of Justice and will be considering its potential implications." THE INDEPENDENT The decision could prove inconsequential after-Brexit, when the ECJ will not have jurisdiction over the Government. Yet the ruling is an embarrassment for Theresa May, who has faced opposition to the law.

Labour's Diane Abbott has called for a major rethink on Theresa May's snooping laws which the European Court have indicated are unlawful.
Ms Abbott slammed the Conservative legislation as a "serious erosion of our rights and liberties" and called for new exemptions.

But she also risked opening divisions in her own party after telling how she tried to warn MPs about dangers before the law was passed, despite concessions having been won by her Labour predecessor Andy Burnham and Sir Keir Starmer, then in the shadow justice brief.

Read more

Labour to abstain on Investigatory Powers Bill, Andy Burnham says

The European Court of Justice has now ruled that bulk email and call data retention by governments is unlawful, even though it was a watered-down version of Ms May's Investigatory Powers Act that reached the UK's statute book last month.

Ms May first brought the legislation forward as Home Secretary, but a legal case against it was brought by Labour's deputy leader Tom Watson and David Davis, who would later end up in Ms May's Cabinet.

Writing for Politics Home, Ms Abbott said that "from time to time" intelligence powers are needed to gather data on terror suspects or criminals.

But she added: "The legislation that was struck down in the European Court went far wider than that. In fact, there was no provision limiting the gathering of data to terrorism or organised crime at all.

"Even the suspicion of the most minor offences was enough to trigger a data trawl by the most junior officials, and in all cases the target had no right to be informed that an investigation had begun, or even that it had taken place in the past with no evidence of wrong doing found.

May on Snoopers' Charter

"This is a serious erosion of our rights and liberties."

The bulk of the legislative process was carried out while Mr Burnham was shadow home secretary and Sir Keir was in the shadow justice brief.

During the summer both fought for concessions to Ms May's earlier versions of the law, with Sir Keir claiming to have won a "really significant step forward".

But Ms Abbott said: "I became involved in this legislation almost at the end of its passage through Parliament as a new shadow home secretary.

"I tried to raise these points in the course of the final debates. I even suggested that the courts might strike down the provision of the Act as being sweeping draconian."

She went on: "Ordinary people are the main victims of both terrorism and organised crime. We need to wage a relentless fight against both.

"But government legislation in this mistakes draconian powers for effective ones. I will be happy to work with government on a major legislative rethink."

Ms Abbott has also clashed with Mr Burnham and Sir Keir more recently over immigration, after giving an interview in which she signalled the economic consequences of stronger controls.

Meanwhile, Mr Burnham, Labour's candidate to be mayor of Manchester, used an interview to say it was "time to confront a hard truth" and implied that immigration could be "undermining the cohesion of our communities and the safety of our streets".

Sir Keir backed tougher controls and said the UK's future relationship with the EU needed to go "beyond" economic considerations.

LOAD-DATE: December 22, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI
Labour's Diane Abbott slams 'unlawful' Snooping Charter and calls for major rethink; But her comments also risk new Labour divisions over the legislation

BYLINE: Joe Watts

SECTION: UK POLITICS

LENGTH: 535 words

Labour's Diane Abbott has called for a major rethink on Theresa May's snooping laws, which the European Court have indicated are unlawful.

Ms Abbott slammed the Conservative legislation as a "serious erosion of our rights and liberties" and called for new exemptions.

But she also risked opening divisions in her own party after telling how she tried to warn MPs about dangers before the law was passed, despite concessions having been won by her Labour predecessor Andy Burnham and Sir Keir Starmer, then in the shadow justice brief.

Read more

Labour to abstain on Investigatory Powers Bill, Andy Burnham says

The European Court of Justice has now ruled that bulk email and call data retention by governments is unlawful, even though it was a watered-down version of Ms May's Investigatory Powers Act that reached the UK's statute book last month.

Ms May first brought the legislation forward as Home Secretary, but a legal case against it was brought by Labour's deputy leader Tom Watson and David Davis, who would later end up in Ms May's Cabinet.

Writing for Politics Home, Ms Abbott said that "from time to time" intelligence powers are needed to gather data on terror suspects or criminals.

But she added: "The legislation that was struck down in the European Court went far wider than that. In fact, there was no provision limiting the gathering of data to terrorism or organised crime at all.

"Even the suspicion of the most minor offences was enough to trigger a data trawl by the most junior officials, and in all cases the target had no right to be informed that an investigation had begun, or even that it had taken place in the past with no evidence of wrongdoing found.

May on Snoopers' Charter

"This is a serious erosion of our rights and liberties."

The bulk of the legislative process was carried out while Mr Burnham was shadow Home Secretary and Sir Keir was in the shadow justice brief.

During the summer both fought for concessions to Ms May's earlier versions of the law, with Sir Keir claiming to have won a "really significant step forward".

But Ms Abbott said: "I became involved in this legislation almost at the end of its passage through Parliament as a new shadow Home Secretary."
"I tried to raisethese points in the course of the final debates. I even suggested that the courts might strike down the provision of the Act as being sweeping and draconian."

She went on: "Ordinary people are the main victims of both terrorism and organised crime. We need to wage a relentless fight against both.

"But government legislation in this mistakes draconian powers for effective ones. I will be happy to work with government on a major legislative rethink."

Ms Abbott has also clashed with Mr Burnham and Sir Keir more recently over immigration, after giving an interview in which she signalled the economic consequences of stronger controls.

Meanwhile, Mr Burnham, Labour's candidate to be mayor of Manchester, used an interview to say it was "time to confront a hard truth" and implied that immigration could be "undermining the cohesion of our communities and the safety of our streets".

Sir Keir backed tougher controls and said the UK's future relationship with the EU needed to go "beyond" economic considerations.

EU's highest court rules *snooper's charter illegal*

The so-called *snooper's charter* is set to face a series of new legal challenges after the European Court of Justice ruled government's "general and indiscriminate retention" of emails is illegal.

Only targeted information gathering is justified, the EU's highest court said, boosting the case against the sweeping collection of emails, text messages and internet data.

The Investigatory Powers Act passed into law in November, granting the Government far-reaching new abilities that allow it to indiscriminately hack and store data relating to internet use.

The case was brought to the European Court by Brexit Secretary David Davis, despite his role in seeking to leave the bloc. He was joined by Deputy Labour Leader Tom Watson in bringing the case, and the pair had already gained a high court victory on the issue. But the case was taken to the European Court after the Government appealed the decision.
The decision could prove inconsequential after the UK withdraws from the EU, when the European Court of Justice will no longer have jurisdiction over the Government. Yet it is an embarrassment for Theresa May, who has faced stiff opposition to the controversial law.

Mr Watson said: "This ruling shows it's counter-productive to rush new laws through Parliament without a proper scrutiny.

"At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

"Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe, but no one would consent to giving the police or the Government the power to arbitrarily seize our phone records or emails to use as they see fit. It's for judges, not ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts."

Martha Spurrier, director of Liberty, which supported the MPs in bringing the case, said: "Today's judgement upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant. The Government must now make urgent changes to the Investigatory Powers Act to comply with this.

"This is the first serious post-referendum test for our Government's commitment to protecting human rights and the rule of law. The UK may have voted to leave the EU - but we didn't vote to abandon our rights and freedoms."

The Government has vowed to appeal against the decision. A Home Office spokesperson said: "We are disappointed with the judgement from the European Court of Justice and will be considering its potential implications.

"It will now be for the Court of Appeal to determine the case. The Government will be putting forward robust arguments to the Court of Appeal about the strength of our existing regime for communications data retention and access.

"Given the importance of communications data in preventing and detecting crime, we will ensure plans are in place so that the police and other public authorities can continue to acquire such data in a way that is consistent with EU law and our obligation to protect the public."
As has been remarked, it is a brilliant irony that David Davis, the Secretary of State for Exiting the European Union, has just beaten his boss the Prime Minister, using the European Court of Justice (ECJ) as the stick.

In good news for anyone who values their privacy, the Snooper’s Charter has been attacked by the ECJ which has sided with Davis. Europe’s highest Court has ruled that data can’t be held as broadly and indiscriminately as the government sought to do in the Investigatory Powers Bill.

It’s sad that it took the ECJ’s intervention to protect our basic rights, and worrying that this judgment may only provide a temporary respite from ever-growing state surveillance.

Rather optimistically, the director of the rights advocacy group Liberty has claimed that “the UK may have voted to leave the EU - but we didn’t vote to abandon our rights and freedoms.”

I’d love to pretend that this was true, but we did vote to abandon rights and freedoms, actually. Recourse to the European Court of Justice is just the sort of legal right enjoyed by David Davis and his colleagues which will be lost when we leave.

When the Court’s advocate general advised the Judges, he articulated an enlightened and proportionate view of surveillance, cautioning that only serious crime “is an objective in the general interest that is capable of justifying a general obligation to retain data, whereas combating ordinary offences and the smooth conduct of proceedings other than criminal proceedings ... are not.”

The ECJ has acted as a bulwark against over-intrusive meddling in citizens’ lives, but we have voted to give up this line of protection from the big-state ideology that underpins the arguments for a Snoopers’ Charter.

Freedom of expression requires privacy - the right to express thoughts freely includes the right to limit the audience to our expression. Our thoughts and our words are altered when we know that they are observed.

We used to live in a society in which, behind locked doors, we could truly experience privacy and freedom. That is no longer the case.

Thanks to leaks, even our own horrified politicians have discovered the extent to which the world’s intelligence services were weakening our online security and collecting our communications.

With the easily-inflated fear of terrorism as their tool, those who would collect and store our secrets can obtain public support with simple arguments. We should be grateful that there are still those, like the ECJ, who stand up for proportionality.

FAQ | Investigatory Powers Act

In any peaceful nation, there are tiny groups and rare individuals who may commit murder and terrorism. It is out of fear of this that our communications are subjected to levels of scrutiny by the government beyond our knowledge and appreciation.

On the other side, there are those like Chelsea Manning who can take the massive intelligence infrastructure and with a USB stick commit acts of espionage which turn the surveillance project on itself. Freedom of expression and our private lives are exposed to the world just by constructing the
apparatus to monitor us all; creating such sweeping systems all but guarantees the breach of our privacy.

The Pentagon

Credit: Charles Dharapak/AP Photo

There are solid arguments against mass surveillance, from the risks it poses to the proper boundary of state actions. A healthy mistrust of governments should be enough to curtail their appetite for expansionist and intrusive policies.

A well-founded concern for the types of leader that the democratic process can sometimes favour should be enough to persuade anyone that the democratic state should only go so far. It's worrying that it is the European Court of Justice which has had to remind us of this.

It is a sign that our future outside the EU, without recourse to the right enjoyed in this case, may be a less liberal one. It is hard to conclude that many would have known that such an illiberal future was the outcome for which they voted.

LOAD-DATE: December 22, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDTNS

Copyright 2016 Telegraph Media Group Limited
All Rights Reserved

Return to List

22 of 100 DOCUMENTS

telegraph.co.uk

December 22, 2016 Thursday 9:31 AM GMT

The European Court of Justice ruling on state surveillance is exactly why we are leaving the European Union

BYLINE: By Philip Johnston

SECTION: NEWS

LENGTH: 432 words

Few pieces of legislation in recent years have been so painstakingly scrutinised as the Investigatory Powers Act, which became law a few weeks ago and takes effect at the end of the year. This is the latest iteration of the so-called Snooper's Charter and as such has attracted a good deal of proper attention from groups alarmed at the extent of state intrusiveness.

But while in normal times, any efforts by the agencies of government to pry into our lives should rightly be resisted, these are not normal times. The security threat posed by terrorists who use new
mass communication methods to plot their attacks makes some snooping inevitable. The challenge is to strike the right balance between security and privacy; and that is a job for parliament.

GCHQ - Britain's spies have been seeking powers fit for the 21st century for years

After lengthy debate, MPs and peers have approved the Act. Yet there is now a possibility it may need to be revisited. The European Court of Justice has ruled that the "general and indiscriminate retention" of data that could be allowed under the Act data is prohibited.

Instead, service providers can only be required to retain data if it is strictly necessary for the purpose of fighting serious crime. Moreover, notice must be given to people affected by the retention, as soon as this would no longer jeopardise an investigation.

Privacy campaigners have hailed the ruling as a landmark in the fight to stop government's keeping information on their citizens. They have a good argument and many of their points were taken on board in the drafting of the legislation. But in the end the security of the realm and its people is a matter for the Government and parliament, not the European Court.

Now that we are leaving the EU here is one area of sovereignty that can be reasserted.

<table>
Are you comfortable with the Investigatory Powers Act (a.k.a. the Snoopers' Charter)? https://t.co/rhJkKkDCcs
- Telegraph Opinion (@TeleComment) December 22, 2016

LOAD-DATE: December 22, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDTNS

Copyright 2016 Telegraph Media Group Limited
All Rights Reserved

Return to List

23 of 100 DOCUMENTS

The Times (London)

December 22, 2016 Thursday
Edition 1;
Scotland

Terror fight 'is weakened' by EU ruling on snooping

BYLINE: Sean O'Neill

SECTION: NEWS; Pg. 4

LENGTH: 675 words

Weakening surveillance laws in response to a European court ruling that they are excessive would leave Britain at greater risk of a terrorist attack, former spy chiefs have warned.

The Court of Justice of the European Union said yesterday that Britain's retention of bulk data on calls, emails and text messages for a year "exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society".
The case concerned emergency legislation from 2014 but the ruling opens the door to further challenges to the powers, and others contained in the new Investigatory Powers Act.

The Home Office said that it was disappointed by the ruling and would argue against it in the British courts. It is studying the implications but former intelligence chiefs and police leaders cautioned against any dilution of their ability to track and thwart terrorists and serious criminals.

Lord Evans of Weardale, the former head of MI5, said that the impact of the ruling on intelligence agencies may be limited because the EU has no remit over national security issues.

The ruling could, however, damage the police's ability to access communications data and hamper the work they do alongside MI5.

"Anything that impacts on their operational effectiveness would be a concern and could leave us more vulnerable to attacks such as those we have seen only too frequently in recent months elsewhere in Europe, including that in Berlin," Lord Evans said.

Sir David Omand, the former head of GCHQ, said that British data-retention powers were stronger than those available to our European allies. "My expectation is that we have a better picture of what is going on in the UK and the links between suspects and jihadists in Syria than the German authorities," he told BBC Radio 4.

David Davis, the secretary for exiting the European Union, was a party to the action against the so-called snooper's charter before withdrawing when he joined the cabinet.

The court ruled that mass retention of every citizen's communications data for access by the authorities was "likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance". It added that the only justification for retaining data was "the objective of fighting serious crime" and that could not be made out when every electronic communication was logged and retained.

Security agencies said that communications data had been used in every MI5 anti-terrorism operation for the past decade and in 95 per cent of serious crime prosecutions.

Tom Watson, Labour's deputy leader and a party in the case, said the judgment showed it was "counterproductive to rush new laws through parliament without proper scrutiny". Liberty, the human rights group, said the ruling "upholds the rights of ordinary British people". The case will return to the Court of Appeal.

Leading article, page 31

Q&A

What exactly is communications data?
The who, what, where, when, how - but not the content - of calls and electronic messages. Logs of when suspects were in contact with each other and for how long are core evidence in many criminal cases.

What are the rules?
The government requires the data to be retained for 12 months so it can be accessed by police or spy agencies. In Germany data is retained for ten weeks.

Is everyone's data held?
Yes. Opponents of the power say it means everyone is treated like a suspect. They want tighter rules on who can access the data and the reasons for accessing it.

If you haven't done anything wrong, why worry?
Because the police have a habit of abusing these powers - eg, hoovering up information from journalists' phones after leaks to the press.

What law was challenged?
The arguments pertain to the Investigatory Powers Act, which recently received royal assent

Brexit is coming, why do we care what Europe thinks?
The government is anxious not to antagonise the EU before negotiations

What happens now?
The Court of Appeal has asked the EU for clarification and the matter will return to the British courts for further arguments.

EU's highest court declares UK surveillance powers illegal

BYLINE: Madhumita Murgia and George Parker in London, and Jim Brunsden in Brussels

LENGTH: 890 words

Britain's surveillance laws have been deemed illegal by the European Court of Justice in a case that throws into question the fate of the UK's new Investigatory Powers Act.

On Wednesday, the ECJ ruled the legislation was illegal because it allowed "general and indiscriminate" retention of electronic communications. The judgment said member states could perform "targeted retention of that data solely for the purpose of fighting serious crime" but not the mass and indiscriminate data collection of everyone in Britain allowed by a new UK spying regime.

This type of legislation "cannot be considered to be justified within a democratic society, as required by the directive, read in the light of the Charter", the ECJ said, referring to the charter of European human rights.

One of the politicians who originally brought the case was David Davis, now the Brexit minister, who has the task of taking Britain out of the jurisdiction of the Luxembourg court. As a backbencher, however, earlier this year Mr Davis turned to the ECJ in an effort to defend British civil liberties. Mr Davis withdrew from the case after becoming Brexit secretary in July.

The Home Office said it was "disappointed" with the judgment and would consider its implications.

Mr Davis brought the case challenging the UK's rules on data retention, under the Data Retention and Investigatory Powers Act 2014 (Dripa), together with Tom Watson, deputy leader of the opposition Labour party.

Although Dripa is due to be repealed by the end of this year, the Investigatory Powers Act (IPA) will be adopted in 2017. The latter significantly expands the mass data-gathering powers challenged in this case.

Specifically, the new law compels internet and phone companies to keep the records of every phone call made and every website visited by any of their users for 12 months. Not only would telecoms companies have a list of every site visited or call made, they would also record the date, time and duration of these actions.

Dozens of public organisations and departments ranging from the police, HM Revenue & Customs, customs officials and intelligence agencies, to the NHS, the Department of Health, the Food
Standards Agency and the Gambling Commission, will be able to access the communications of people in Britain, in some cases without a warrant.

However, the ECJ's ruling creates another major source of post-Brexit uncertainty for UK businesses because EU rules forbid the sharing of personal data with countries that do not meet its strict data privacy standards.

British officials will be looking at the precedent of the US, which has repeatedly come up against such rules. This year, officials on both sides of the Atlantic had to cobble together a new deal on data transfers after a previous one -- itself a result of laborious negotiation -- was struck down by the European courts.

The new deal, known as Privacy Shield, was essential to provide a legal means for businesses to transfer personal data online -- whether payslips, pictures or healthcare data -- to the US from the EU without falling foul of Europe's privacy regulations.

Wednesday's ruling means Britain could now struggle to convince the EU that its data protection standards are up to scratch, a headache not only for companies but also for law enforcement authorities.

"The government is breaking the law by indiscriminately collecting the nation's internet activity and phone records and letting hundreds of public bodies grant themselves access to these personal details with no suspicion of serious crime and no independent sign-off -- meaning significant parts of its new 'snoopers charter' are effectively unlawful," said Liberty, the human rights organisation supporting Mr Watson.

Lawyers believe the ECJ's ruling will force the hand of the UK government to amend the law and limit its remit.

"The provisions in the two laws are extremely similar so it is perfectly logical that the rationale will apply equally to the new [act], and it will have to be amended," said Richard Cumbley, partner at law firm Linklaters. "There is no doubt the government, if it takes on board the decision, will have to apply more restrictive rules both to the types of data stored and the conditions under which it can be accessed."

Large swaths of the Investigatory Powers Act will remain unaffected by the ECJ ruling, however, including the ability to "bulk hack" citizens' communications and force technology companies to create a backdoor into their products so that communications can be accessed.

Mr Watson said: "This ruling shows it's counter-productive to rush new laws through parliament without a proper scrutiny.

"At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

"Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe, but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit. It's for judges, not ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts."
EU's highest court rules UK surveillance laws illegal

BYLINE: Madhumita Murgia

LENGTH: 200 words

Britain's surveillance laws have been deemed illegal by the European Court of Justice, throwing into question the new Investigatory Powers Act under a case originally brought by David Davis, now the Brexit minister.

The judgment said member states could perform "targeted retention of that data solely for the purpose of fighting serious crime" but not the mass and indiscriminate data collection of everyone in the UK allowed by new UK spying regime.

This type of legislation "cannot be considered to be justified within a democratic society, as required by the directive, read in the light of the Charter," the European Court of Justice ruling said, rendering the laws incompatible with European human rights.

The ruling was made in response to a case brought by Mr Davis when he was a backbench MP, along with Labour's deputy leader Tom Watson challenging the UK's rules on data retention, under the Data Retention and Investigatory Powers Act 2014. Mr Davis later dropped his name from the challenge, known as the "Snoopers' Charter" after being appointed in prime minister Theresa May's cabinet in July.

The Home Office said it was "disappointed" with the judgment and would consider its implications.

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

The Guardian

EU's highest court delivers blow to UK snoopers' charter; Indiscriminate collection of emails is illegal, court rules in response to challenge originally brought by David Davis

BYLINE: Owen Bowcott Legal affairs correspondent

SECTION: WORLD NEWS

LENGTH: 1231 words
"General and indiscriminate retention" of emails and electronic communications by governments is illegal, the EU's highest court has ruled, in a judgment that could trigger challenges against the UK's new Investigatory Powers Act - the so-called snooper's charter.

Only targeted interception of traffic and location data in order to combat serious crime - including terrorism - is justified, according to a long-awaited decision by the European court of justice (ECJ) in Luxembourg.

The finding came in response to a legal challenge initially brought by the Brexit secretary, David Davis, when he was a backbench MP, and Tom Watson, Labour's deputy leader, over the legality of GCHQ's bulk interception of call records and online messages.

Related: How can I protect myself from government snoopers?

Davis and Watson, who were supported by Liberty, the Law Society, the Open Rights Group and Privacy International, had already won a high court victory on the issue, but the government appealed and the case was referred by appeal judges to the ECJ. The case will now return to the court of appeal to be resolved in terms of UK legislation.

The aim of going to Luxembourg was to clarify EU law on surveillance. The two MPs had argued successfully in the domestic courts that the Data Retention and Investigatory Powers Act (Dripa) 2014 was illegal. Dripa has since been replaced by the Investigatory Powers Act, which comes into force at the end of this month.

At issue was whether there are EU standards on data retention that need to be respected by member states in domestic legislation. The result, though immediately significant, could prove academic once the UK has withdrawn from the EU and the ECJ no longer has jurisdiction over the UK.

In a summary of the ruling, the court said electronic communications allow "very precise conclusions to be drawn concerning the private lives of persons whose data has been retained".

It added: "The interference by national legislation that provides for the retention of traffic data and location data with that right must therefore be considered to be particularly serious. The fact that the data is retained without the users of electronic communications services being informed of the fact is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance. Consequently, only the objective of fighting serious crime is capable of justifying such interference. Legislation prescribing a general and indiscriminate retention of data ... exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society." Prior authorisation by a court or independent body to access retained data is required for each official request, the ECJ said.

Before becoming Brexit minister, Davis travelled to Luxembourg to hear the case. He argued that the British government was "treating the entire nation as suspects" by ignoring safeguards on retaining and accessing personal communications data.

Davis, one of the most vociferous critics of the state's powers to collect data on its citizens, withdrew from the case following his ministerial appointment.

The Dripa case was heard by 15 ECJ judges. It coincided with successive atrocities in Paris, Brussels and Nice that reinforced political demands for expansion of powers to intercept emails and phone calls to help catch Islamic State militants operating on the continent.

Lawyers for the UK government maintained that intercepted communications have been at the heart of every terrorist case investigated by police and the security services in recent years.

Responding to the ruling, Watson said: "At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

"Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe, but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit. It's for judges, not ministers, to oversee these powers."
Martha Spurrier, director of the human rights group Liberty, said: "Today's judgment upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant. The government must now make urgent changes to the Investigatory Powers Act [IPA] to comply with this.

"This is the first serious post-referendum test for our government's commitment to protecting human rights and the rule of law. The UK may have voted to leave the EU - but we didn't vote to abandon our rights and freedoms." Liberty is preparing to challenge the IPA in court.

Jim Killock, executive director of the Open Rights Group, said: "Blanket surveillance of our communications is intrusive and unacceptable in a democracy.

"The government must act quickly to rewrite the IPA or be prepared to go to court again."

A Home Office spokesperson said: "We are disappointed with the judgment from the European court of justice and will be considering its potential implications.

"The government will be putting forward robust arguments to the court of appeal about the strength of our existing regime for communications data retention and access."

The shadow home secretary, Diane Abbott, said: "Many of us warned that these powers were far too widely drawn. Effectively, they allow for fishing expeditions where data is collected on a vast number of individuals. They also allow for data gathering against anyone suspected of the most minor crimes, not just terrorism and organised crime, and there is insufficient judicial oversight. Targets were not informed."

The Liberal Democrat home affairs spokesman Brian Paddick said: "Collecting and storing everyone's internet web browsing histories and phone records so government agencies can look at them is an Orwellian nightmare that intrudes into our privacy and erodes our civil liberties."

Daniel Carey, the solicitor from Deighton Pierce Glynn who represented the Open Rights Group and Privacy International, said: "The court is very clear that indiscriminately retaining everyone's metadata is unlawful, which is a point my clients placed particular emphasis on. This prohibition arises out of longstanding EU legislation, which the UK played an important role in creating."

Camilla Graham Wood, of Privacy International, said: "Today's judgment is a major blow against mass surveillance and an important day for privacy. It makes clear that blanket and indiscriminate retention of our digital histories can be a very intrusive form of surveillance that needs strict safeguards against abuse and mission creep."

The National Police Chiefs' Council lead for communications data, assistant chief constable Richard Berry said: "We will work within any authorisation and oversight regime deemed appropriate by parliament and courts of law. But it is important for us to have a regime that is practical and dynamic enough to be able to respond to the volume and urgency of our cases. Any changes that impede our ability to access data quickly with appropriate safeguards will undermine our ability to keep people safe."

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

Copyright 2016 The Guardian, a division of Transcontinental Media Group Inc. All Rights Reserved

Return to List

27 of 100 DOCUMENTS
EU ruling means UK snooper’s charter may be open to challenge; Ministers can no longer be certain that Investigatory Powers Act can survive privacy actions in UK courts after landmark ruling on blanket state surveillance

BYLINE: Alan Travis Home affairs editor

SECTION: WORLD NEWS

LENGTH: 676 words

The European court of justice ruling that blanket state surveillance without proper privacy safeguards is unlawful may be packed with post-Brexit irony - not least in that it involves Britain losing a case in Europe initially brought by its Brexit minister, David Davis. But it is important because it means the battle over digital rights in Britain is not over yet.

Theresa May's new turbo-charged state surveillance law - the Investigatory Powers Act 2016, with its extensive powers to track the entire population's web browsing history for two years and allowing industrial scale state hacking of phones and computers - will come into effect from the end of this month.

But the ruling from the European court - particularly if, as is likely, it is upheld by British court of appeal judges - will mean that the new law will now face a succession of legal challenges from privacy campaigners fortified by the ruling in their back pockets.

The ruling itself relates to a much more limited British law - the Data Retention and Investigatory Powers Act 2014, known as Dripa - which expires under a sunset clause at the end of this month.

That law required the telecom companies to hold all their customers’ communications data - the who, when and where they contacted by phone, text or email - for 12 months so it could be accessed by the police, security services and other public bodies.

The ECJ ruling clarified at the request of British court of appeal judges that EU data retention laws say that such blanket retention of everyone's personal confidential data is unlawful under the EU’s fundamental charter of rights and its directive on privacy and electronic communications.

The landmark ruling says that the state can carry out such mass surveillance programmes as long as it is done on a targeted and not a blanket or "general and indiscriminate" basis. Targeting should be done by reference to time, geographical area or named persons. The ruling also lays down that the communications data can only be used for the purposes of fighting serious crime and access should be authorised by a court except in the most urgent cases.

It is a ruling that is enough to strike down Dripa should the British court of appeal accept this "clarification" from the EU's highest court. By the time the UK court gets to it, it will be academic as Dripa will be repealed in 10 days’ time.

But it does have serious implications for the new snooper’s charter, the Investigatory Powers Act 2016 that includes the data retention powers that the EU court has declared to be unlawful without the proper safeguards and which comes into force from the end of this month.

The new state surveillance law includes a major extension of powers, including vast databases recording every website visited by the entire population. These databases can be accessed not just by the police and security services but by dozens of other public authorities, and in the case of communications data, without the need for suspicion of criminality or prior sign-off from a judge or other independent official. They include the NHS, Department for Work and Pensions and the Gambling Commission.

The ruling means that ministers can no longer be certain that the new snooper's charter will survive any privacy legal challenges in the British courts. The ruling is unlikely to mean that the Investigatory Powers Act is struck down by British judges as unlawful, but it may well require further amendment.

Brexit campaigners may claim the ruling is evidence that staying in the EU undermines the fight against terrorism. But the judgment clearly says that the state is within its rights to conduct targeted digital surveillance to fight terrorism and serious crime as long as there are proper judicial safeguards.
Those who say that ministers should just ignore the Luxembourg court ruling because Britain will soon be out of the EU will also be disappointed. Whether Britain is in or out of Europe, British judges will still be using this privacy benchmark to hold British ministers and their laws to account.

LOAD-DATE: December 21, 2016
LANGUAGE: ENGLISH
PUBLICATION-TYPE: Newspaper
JOURNAL-CODE: WEBGNS

The so-called snooper’s charter is set to face a series of new legal challenges after the EU's highest court ruled governments' "general and indiscriminate retention" of emails is illegal.

Snooper’s charter dealt blow after EU's highest court rules 'indiscriminate' government retention of emails is illegal

SECTION: UK POLITICS
LENGTH: 33 words

More follows...
The so-called snooper's charter is set to face a series of new legal challenges after the EU's highest court ruled governments' "general and indiscriminate retention" of emails is illegal. Only targeted information gathering is justified, according to the European Court of Justice, helping the case against the sweeping collection of emails, text messages and internet data.

The Investigatory Powers Act passed into law in November, granting the government a raft of new powers, including the ability to indiscriminately hack and collect the internet use of the population.

More follows...

Copyright 2016 Independent Digital News and Media Limited
All Rights Reserved

Return to List

30 of 100 DOCUMENTS
The case was brought to the European Court by Brexit Secretary David Davis, despite his role in seeking to leave the bloc.

The ruling is an embarrassment for Theresa May, who has faced stiff opposition to the controversial law.

Deputy Labour Leader Tom Watson, who brought the case alongside Mr Davis, said: "This ruling shows it's counter-productive to rush new laws through Parliament without a proper scrutiny.

"At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over.

"That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

"Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit.

"It's for judges, not Ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts."

This is a breaking news story. More follows...

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI

The so-called snooper's charter is set to face a series of new legal challenges after the EU's highest court ruled government's "general and indiscriminate retention" of emails is illegal.

"UK may have voted to leave the EU - but we didn't vote to abandon our rights,' says Liberty

BYLINE: Harriet Agerholm

SECTION: UK POLITICS

LENGTH: 513 words

The Investigatory Powers Act passed into law in November, granting the government far-reaching new abilities meaning they can now indiscriminately hack and store data relating to internet use.
The Snooper’s Charter is now law - say goodbye to your privacy

The case was brought to the European Court by Brexit Secretary David Davis, despite his role in seeking to leave the bloc.

The ruling is an embarrassment for Theresa May, who has faced stiff opposition to the controversial law.

Deputy Labour Leader Tom Watson, who brought the case alongside Mr Davis, said: "This ruling shows it's counter-productive to rush new laws through Parliament without a proper scrutiny.

"At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over.

"That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

The snooper’s charter will infringe our right to privacy

"Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit.

"It's for judges, not ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts."

Martha Spurrier, director of Liberty, which supported the MPs in bringing the casesaid: "Today’s judgment upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant.

"The Government must now make urgent changes to the Investigatory Powers Act to comply with this.

"This is the first serious post-referendum test for our Government's commitment to protecting human rights and the rule of law.

"The UK may have voted to leave the EU - but we didn't vote to abandon our rights and freedoms."

The Government has vowed to appeal against the decision.

A Home Office spokesperson said: "We are disappointed with the judgment from the European Court of Justice and will be considering its potential implications.

"It will now be for the Court of Appeal to determine the case. The Government will be putting forward robust arguments to the Court of Appeal about the strength of our existing regime for communications data retention and access.

"Given the importance of communications data to preventing and detecting crime, we will ensure plans are in place so that the police and other public authorities can continue to acquire such data in a way that is consistent with EU law and our obligation to protect the public."

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI
Snooper's charter dealt blow after EU's highest court rules 'indiscriminate' government retention of emails is illegal; 'UK may have voted to leave the EU - but we didn't vote to abandon our rights,' says Liberty

BYLINE: Harriet Agerholm

SECTION: UK POLITICS

LENGTH: 540 words

The so-called snooper's charter is set to face a series of new legal challenges after the EU's highest court ruled government's "general and indiscriminate retention" of emails is illegal.

Only targeted information gathering is justified, the European Court of Justice said, boosting the case against the sweeping collection of emails, text messages and internet data.

The Investigatory Powers Act passed into law in November, granting the government far-reaching new abilities meaning they can now indiscriminately hack and store data relating to internet use.

The case was brought to the European Court by Brexit Secretary David Davis, despite his role in seeking to leave the bloc.

He was joined by Deputy Labour Leader Tom Watson in bringing the case and the pair had already had a high court victory on the issue.

But after the Government appealed the decision, the case was taken to the European court.

The ruling is an embarrassment for Theresa May, who has faced stiff opposition to the controversial law.

Mr Watson: "This ruling shows it's counter-productive to rush new laws through Parliament without a proper scrutiny.

"At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over.

"That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past."

Martha Spurrier, director of Liberty, which supported the MPs in bringing the case said: "Today's judgment upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant.

"The Government must now make urgent changes to the Investigatory Powers Act to comply with this.

"This is the first serious post-referendum test for our Government's commitment to protecting human rights and the rule of law."
"The UK may have voted to leave the EU - but we didn't vote to abandon our rights and freedoms."

The Government has vowed to appeal against the decision.

A Home Office spokesperson said: "We are disappointed with the judgment from the European Court of Justice and will be considering its potential implications.

"It will now be for the Court of Appeal to determine the case. The Government will be putting forward robust arguments to the Court of Appeal about the strength of our existing regime for communications data retention and access.

"Given the importance of communications data to preventing and detecting crime, we will ensure plans are in place so that the police and other public authorities can continue to acquire such data in a way that is consistent with EU law and our obligation to protect the public."

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI

The so-called snooper's charter is set to face a series of new legal challenges after the EU's highest court ruled governments' "general and indiscriminate retention" of emails is illegal.

Only targeted information gathering is justified, the European Court of Justice said, boosting the case against the sweeping collection of emails, text messages and internet data.

The Investigatory Powers Act passed into law in November, granting the Government far-reaching new abilities that allow it to indiscriminately hack and store data relating to internet use.

Read more

The Snooper's Charter is now law - say goodbye to your privacy

The case was brought to the European Court by Brexit Secretary David Davis, despite his role in seeking to leave the bloc.
He was joined by Deputy Labour Leader Tom Watson in bringing the case, and the pair had already gained a high court victory on the issue.

But after the Government appealed the decision, the case was taken to the European court.

The decision could prove inconsequential after the UK withdraws from the EU, when the European Court of Justice will no longer have jurisdiction over the Government.

Yet the ruling is an embarrassment for Theresa May, who has faced stiff opposition to the controversial law.

Mr Watson said: "This ruling shows it's counter-productive to rush new laws through Parliament without a proper scrutiny.

"At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over.

"That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

Read more

The snooper's charter will infringe our right to privacy

"Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe, but no one would consent to giving the police or the Government the power to arbitrarily seize our phone records or emails to use as they see fit.

It's for judges, not ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts."

Martha Spurrier, director of Liberty, which supported the MPs in bringing the case, said: "Today's judgement upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant.

"The Government must now make urgent changes to the Investigatory Powers Act to comply with this.

"This is the first serious post-referendum test for our Government's commitment to protecting human rights and the rule of law.

"The UK may have voted to leave the EU - but we didn't vote to abandon our rights and freedoms."

The Government has vowed to appeal against the decision.

A Home Office spokesperson said: "We are disappointed with the judgement from the European Court of Justice and will be considering its potential implications.

"It will now be for the Court of Appeal to determine the case. The Government will be putting forward robust arguments to the Court of Appeal about the strength of our existing regime for communications data retention and access.

"Given the importance of communications data in preventing and detecting crime, we will ensure plans are in place so that the police and other public authorities can continue to acquire such data in a way that is consistent with EU law and our obligation to protect the public."

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI

Copyright 2016 Independent Digital News and Media Limited
All Rights Reserved

Return to List

34 of 100 DOCUMENTS
Ministers are set for clash with EU judges over surveillance powers after ruling that internet companies can’t be forced to harvest email data

BYLINE: JAMES TAPSFIELD, POLITICAL EDITOR FOR MAILONLINE

Ministers are heading for a furious clash with EU judges after a ruling that could undermine the so-called ‘snoopers’ charter’.

The European Court of Justice has backed a challenge to the ‘general and indiscriminate retention’ of emails - potentially wrecking the government's plans to step up surveillance to counter terrorists.

The case is an embarrassing setback for Theresa May - especially as her Brexit Secretary David Davis was originally one of those involved in taking on the UK authorities.

He withdrew from the challenge - also supported by Labour’s Tom Watson and campaign group Liberty - after being appointed to Mrs May’s top team.

The High Court had already found against the government but ministers appealed to the ECJ.

The case concerns the powers to force internet companies to harvest and retain large amounts of communications information, contained in the Data Retention and Investigatory Powers Act (Dripa) 2014.

The legislation has since been replaced by the Investigatory Powers Act, which came into force this autumn.

Supporters say the powers are crucial for intelligence services to monitor potential terror suspects.

The judges were asked to consider whether EU standards on data retention had to be respected by member states in domestic law.

The court said today: “With respect to retention, the retained data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.’

The decision on the principle could open the door to legal challenges against the Investigatory Powers Act.

The result, though significant, could eventually prove academic once the UK has withdrawn from the EU and the ECJ no longer has judicial authority over the UK.

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

JOURNAL-CODE: WEBDM

Copyright 2016 Associated Newspapers Ltd.
All Rights Reserved

Return to List
Ministers are set for clash with EU judges over surveillance powers after ruling that internet companies can't be forced to harvest email data

BYLINE: JAMES TAPSFIELD, POLITICAL EDITOR FOR MAILONLINE

SECTION: NEWS

LENGTH: 469 words

European Court of Justice has ruled against 'general and indiscriminate' retention of emails
The decision could open the door to challenges against 'snoopers' charter'
David Davis supported challenge before being appointed to Cabinet

Ministers are heading for a furious clash with EU judges after a ruling that could undermine the so-called 'snoopers' charter'.

The European Court of Justice has backed a challenge to the 'general and indiscriminate retention' of emails - potentially wrecking the government's plans to step up surveillance to counter terrorists.

The case is an embarrassing setback for Theresa May - especially as her Brexit Secretary David Davis was originally one of those involved in taking on the UK authorities.

He withdrew from the challenge - also supported by Labour's Tom Watson and campaign group Liberty - after being appointed to Mrs May's top team.

The High Court had already found against the government but ministers appealed to the ECJ.

The case concerns the powers to force internet companies to harvest and retain large amounts of communications information, contained in the Data Retention and Investigatory Powers Act (Dripa) 2014.

The legislation has since been replaced by the Investigatory Powers Act, which came into force this autumn.

Supporters say the powers are crucial for intelligence services to monitor potential terror suspects.

The judges were asked to consider whether EU standards on data retention had to be respected by member states in domestic law.

The court said today: 'With respect to retention, the retained data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.'

The decision on the principle could open the door to legal challenges against the Investigatory Powers Act.

The result, though significant, could eventually prove academic once the UK has withdrawn from the EU and the ECJ no longer has judicial authority over the UK.

Mr Watson, Labour's Deputy Leader, said: 'This ruling shows it's counter-productive to rush new laws through Parliament without proper scrutiny.

‘At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That’s why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.'
'Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit. It's for judges, not Ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts.'

Ministers are set for clash with EU judges over surveillance powers after ruling that internet companies can't be forced to harvest email data

BYLINE: JAMES TAPSFIELD, POLITICAL EDITOR FOR MAILONLINE

MINISTERS ARE SET FOR CLASH WITH EU JUDGES OVER SURVEILLANCE POWERS AFTER RULING THAT INTERNET COMPANIES CAN'T BE FORCED TO HARVEST EMAIL DATA

Ministers are heading for a furious clash with EU judges after a ruling that could undermine the so-called 'snoopers' charter'.

European Court of Justice has ruled against 'general and indiscriminate' retention of emails

The decision could open the door to challenges against 'snoopers' charter' David Davis supported challenge before being appointed to Cabinet

Ministers are heading for a furious clash with EU judges after a ruling that could undermine the so-called 'snoopers' charter'.

The European Court of Justice has backed a challenge to the 'general and indiscriminate retention' of emails - potentially wrecking the government's plans to step up surveillance to counter terrorists.

The case is an embarrassing setback for Theresa May - especially as her Brexit Secretary David Davis was originally one of those involved in taking on the UK authorities.

He withdrew from the challenge - also supported by Labour's Tom Watson and campaign group Liberty - after being appointed to Mrs May's top team.

The High Court had already found against the government but ministers appealed to the ECJ.

The case concerns the powers to force internet companies to harvest and retain large amounts of communications information, contained in the Data Retention and Investigatory Powers Act (Dripa) 2014.

The legislation has since been replaced by the Investigatory Powers Act, which came into force this autumn.
Supporters say the powers are crucial for intelligence services to monitor potential terror suspects. The former head of MI5, Lord Evans of Weardale, said even if the UK was not directly affected the ruling could leave us more vulnerable to attacks.

'The intelligence agencies work very closely with colleagues in the police and anything that impacts on their operational effectiveness would be a concern and could leave us more vulnerable to attacks such as those we have seen only too frequently in recent months elsewhere in Europe, including that in Berlin.'

The judges were asked to consider whether EU standards on data retention had to be respected by member states in domestic law.

The court said today: 'With respect to retention, the retained data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.'

The decision on the principle could open the door to legal challenges against the Investigatory Powers Act.

The result, though significant, could eventually prove academic once the UK has withdrawn from the EU and the ECJ no longer has judicial authority over the UK.

Mr Watson, Labour's Deputy Leader, said: 'This ruling shows it's counter-productive to rush new laws through Parliament without proper scrutiny.

'At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

'Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit. It's for judges, not Ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts.'
The Brexit Secretary has taken the Prime Minister to an EU court and won, in a victory for anti-surveillance campaigners.

A group successfully brought a case against parts of Theresa May's *Snooper's Charter*.

But in an embarrassing moment for the Prime Minister's Brexit team, one of the leading figures in the group was David Davis, the minister responsible for taking Britain out of the EU - and the court's jurisdiction.

The group, which also included Deputy Labour leader Tom Watson, challenged Mrs May's *Investigatory Powers Act*, which covers state surveillance.

The court ruled parts of the law, which allows the government to collect and keep the internet and phone records of every UK citizen, are unlawful.

It means significant parts of Mrs May's *Investigatory Powers Act* (IPA), a pet project while she was Home Secretary, are unlawful and must be changed.

The original challenge was to the Data Retention and *Investigatory Powers Act* (DRIPA) - a temporary law set to expire on December 31.

But last month, Parliament passed the IPA, which vastly expanded the same powers to collect and store citizens' data without a warrant.

DRIPA forces communications companies to store every person's "communications data" - the who, what, when, where and how of every email, text, phone call, and internet communication, including those of lawyers, doctors, MPs and journalists.

EU judges ruled that DRIPA breaks the law because it "allows general and indiscriminate retention of all communications data."

*Snooper's Charter* passes into law giving British intelligence services sweeping internet surveillance powers

The IPA widened the scope of the law, allowing dozens of public bodies - including the NHS and Department for Work and Pensions - to access the records without suspicion of serious criminality.

Tom Watson said: "This ruling shows it's counter-productive to rush new laws through Parliament without a proper scrutiny.

"At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

"Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe, but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit. It's for judges, not Ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts."

These are the 48 organisations that can see EVERYTHING you do online - even if you delete it

Martha Spurrier, Director of Liberty, who backed the legal challenge said: "Today's judgment upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant. The Government must now make urgent changes to the *Investigatory Powers Act* to comply with this.

"This is the first serious post-referendum test for our Government's commitment to protecting human rights and the rule of law. The UK may have voted to leave the EU - but we didn't vote to abandon our rights and freedoms."

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH
Brexit Secretary David Davis just took Theresa May to the EU Court of Justice and won;
In a victory for both privacy campaigners and absurdity, the EU court agreed with David Davis that parts of the Snooper's Charter are unlawful

BYLINE: By Mikey Smith

SECTION: NEWS, UK NEWS

LENGTH: 651 words

The Brexit Secretary has taken the Prime Minister to an EU court and won, in a victory for anti-surveillance campaigners.

A group successfully brought a case against parts of Theresa May's Snooper's Charter. But in an embarrassing moment for the Prime Minister's Brexit team, one of the leading figures in the group was David Davis, the minister responsible for taking Britain out of the EU - and the court's jurisdiction.

The group, which also included Deputy Labour leader Tom Watson, challenged Mrs May's Investigatory Powers Act, which covers state surveillance.

The court ruled parts of the law, which allows the government to collect and keep the internet and phone records of every UK citizen, are unlawful.

It means significant parts of Mrs May's Investigatory Powers Act (IPA), a pet project while she was Home Secretary, are unlawful and must be changed.

The original challenge was to the Data Retention and Investigatory Powers Act (DRIPA) - a temporary law set to expire on December 31.

But last month, Parliament passed the IPA, which vastly expanded the same powers to collect and store citizens' data without a warrant.

DRIPA forces communications companies to store every person's "communications data" - the who, what, when, where and how of every email, text, phone call, and internet communication, including those of lawyers, doctors, MPs and journalists.

EU judges ruled that DRIPA breaks the law because it "allows general and indiscriminate retention of all communications data."

Snooper's Charter passes into law giving British intelligence services sweeping internet surveillance powers.
The IPA widened the scope of the law, allowing dozens of public bodies - including the NHS and Department for Work and Pensions - to access the records without suspicion of serious criminality.

Tom Watson said: "This ruling shows it's counter-productive to rush new laws through Parliament without a proper scrutiny."

"At a time when we face a real and ever-present terrorist threat, the security forces may require access to personal information none of us would normally hand over. That's why it's absolutely vital that proper safeguards are put in place to ensure this power is not abused, as it has been in the recent past.

"Most of us can accept that our privacy may occasionally be compromised in the interests of keeping us safe, but no one would consent to giving the police or the government the power to arbitrarily seize our phone records or emails to use as they see fit. It's for judges, not Ministers, to oversee these powers. I'm pleased the court has upheld the earlier decision of the UK courts."

These are the 48 organisations that can see EVERYTHING you do online - even if you delete it

Martha Spurrier, Director of Liberty, who backed the legal challenge said: "Today's judgment upholds the rights of ordinary British people not to have their personal lives spied on without good reason or an independent warrant. The Government must now make urgent changes to the Investigatory Powers Act to comply with this.

"This is the first serious post-referendum test for our Government's commitment to protecting human rights and the rule of law. The UK may have voted to leave the EU - but we didn't vote to abandon our rights and freedoms."

A Home Office Spokesperson said: "We are disappointed with the judgment from the European Court of Justice and will be considering its potential implications.

"It will now be for the Court of Appeal to determine the case. The Government will be putting forward robust arguments to the Court of Appeal about the strength of our existing regime for communications data retention and access.

"Given the importance of communications data to preventing and detecting crime, we will ensure plans are in place so that the police and other public authorities can continue to acquire such data in a way that is consistent with EU law and our obligation to protect the public."

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

Copyright 2016 Trinity Mirror, Plc.
All Rights Reserved

Return to List

39 of 100 DOCUMENTS

telegraph.co.uk

December 21, 2016 Wednesday 10:10 AM GMT

Theresa May's Snoopers' Charter dealt major setback as EU court rules against 'indiscriminate' collection of internet data

BYLINE: By James Titcomb

SECTION: TECHNOLOGY
Theresa May's surveillance laws have been dealt a major setback after an EU court ruled that the bulk collection of citizens' internet browsing history is illegal under European law.

Wednesday's ruling strikes at the centre of the Investigatory Powers Act - dubbed the "Snooper's Charter" - which requires internet providers to store 12 months of everybody's browsing data and make it available to dozens of Government bodies.

The European Court of Justice ruled that EU laws forbid the "general and indiscriminate" retention of internet data, following a challenge to British surveillance powers originally brought by Conservative MP David Davis and Labour's Tom Watson.

FAQ | Investigatory Powers Act

"EU law precludes national legislation that prescribes general and indiscriminate retention of data," the court said.

"The fact that the data is retained without the users of electronic communications services being informed of the fact is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance.

"Such national legislation therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society, as required by the directive, read in the light of the [EU Charter of Fundamental Rights]."

The legal challenge was not against the Investigatory Powers Act itself but its predecessor, 2014's Data Retention and Investigatory Powers Act, which expires at the end of this year.

However, the new legislation, which recently came into law, contains similar powers and Wednesday's ruling opens up legal challenges to it.

The laws were challenge by Labour's Tom Watson

Legal experts said the Government may now have to significantly reduce the reach of the legislation, justifying it under national security laws instead of for fighting crime. This could dramatically diminish the number of bodies that can access the browsing histories of citizens, which internet providers must store for 12 months.

Dozens of government agencies including the Food Standards Agency and HMRC are able to access internet connection records under the Act, which Kristina Holt, a data privacy lawyer at Pinsent Masons, said may have to be scaled back to a handful including GCHQ and the police.

Mr Davis withdrew from the legal challenge when he joined the cabinet this year. The ruling is likely to be seized on by Brexit campaigners as an example of why the UK should not be subject to European courts.

A Home Office spokesman said: "We are disappointed with the judgment from the European Court of Justice and will be considering its potential implications.

"It will now be for the court of appeal to determine the case. The government will be putting forward robust arguments to the court of appeal about the strength of our existing regime for communications data retention and access.

"Given the importance of communications data to preventing and detecting crime, we will ensure plans are in place so that the police and other public authorities can continue to acquire such data in a way that is consistent with EU law and our obligation to protect the public."

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication
Spying on Press is the e-version of using a baton;  
COMMENT

BYLINE: KEVIN MAGUIRE

SECTION: NEWS; Pg. 4,5

LENGTH: 216 words

WELCOME to Stasi Britain, where cops spy on journalists investigating credible allegations of police corruption.

If this had been in Putin’s Russia, our PM and Foreign Secretary would rightly denounce state intimidation and an unwarranted assault on press freedom.

So we must now hold to account the high-ranking uniforms who abused positions of trust to cover up bad behaviour by public servants. Covertly monitoring calls by my respected colleague Jeremy Armstrong rode roughshod over his right to privacy and civil liberties. The police happily tracing calls in the hope of unmasking a mole tells me they were more anxious to avoid embarrassment than ensure public money was spent wisely.

But a broader, more terrifying truth is this alerts us to the danger of the police as a law unto themselves, prepared to stamp on anybody who gets in their way.

Gagging papers, halting probes would make their life easier at the expense of the public good. The disinfectant of daylight keeps the authorities honest.

Spying on the Press is the e-version of a baton. I condemn cases where journos broke laws with no public interest defence - and we must equally robustly stand up to the snooper cops.

Journalism at its best speaks truth unto power, so we should be concerned that’s why the police accessed records.

LOAD-DATE: December 19, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: DMR
Police unlawfully intercepted Mirror reporter's phone records after disgraced chief's lies were exposed; Force unlawfully snooped on us and others after its £191,000-a-year Chief Constable, later sacked in disgrace, had an affair with a colleague, lied about it, and spent thousands of pounds of taxpayers' money on jollies with her

BYLINE: By Jeremy Armstrong

SECTION: NEWS, UK NEWS

LENGTH: 1008 words

A police force last night faced stinging criticism for unlawfully snooping on the Daily Mirror after we revealed its Chief Constable blew taxpayers' cash to conduct an affair with a colleague.

Bosses used powers designed to track terrorists and dangerous criminals to access my phone records as well as those of other journalists, officers and a solicitor in a bid to find who was leaking information about alleged racism within its ranks.

We had told how £191,000-a-year Cleveland Chief Constable Sean Price was having a fling with his chief staff officer Heather Eastwood.

He claimed the romance started after he had left his wife Jackie, but that turned out to be a lie.

Later sacked for gross misconduct and branded a liar and a bully, he also spent £57,800 on a force credit card, which included bills for hotels and flowers.


And a tribunal in London heard it breached communication data powers to get hold of the information. It claimed the move was done by mistake.

But former Shadow Home Secretary Yvette Cooper branded the breach "very serious".

**Snooper's** Charter passes into law giving British intelligence services sweeping internet surveillance powers

The Commons Home Affairs Select Committee chairwoman said: "Communications data powers exist so the police can investigate serious crimes, not so they can prevent journalists holding them to account.

"In a democracy the freedom of the Press is incredibly important and needs to be protected not undermined."

Stockton North Labour MP Alex Cunningham added: "As a former journalist, I know how precious the protections that exist for the media are.

"For a police force to stand up in court and admit it misused security powers to spy on its own officers, lawyers, newspaper offices and reporters beggars belief." Redcar's Labour MP Anna Turley branded the snooping "shocking".

She said: "Having a free Press in this country is a vital part of our democracy. We do not live in a police state."
The Investigation Powers Tribunal in London was told our reporter's calls were checked between January 1 and May 1, 2012, under RIPA. Its excessive use for information other than terror or crime is a threat to civil liberties.

At the time, a "damning" review into racism and other confidential documents within the force had been leaked and bosses were trying to find the source.

Family of GCHQ worker who killed himself after mystery arrest blames spybase bosses for his death

The force also allegedly snooped on former officers Mark Dias and Steve Matthews, Northern Echo reporters Graeme Hetherington and Julia Breen and a lawyer. It denies the claim.

But tribunal judges indicated their ruling, due in the New Year, would find it acted unlawfully on this matter. They also raised concerns about the amount of data seized and the length of the request - four months' worth of Mirror records.

Mr Dias and Mr Matthews claimed an equality report was in the public interest. Mr Dias told how he had been standing up to racism in the police.

He said: "They used RIPA to identify contacts between police officers, members of the public and journalists. It was a fishing expedition and unlawful."

Mr Matthews' representative Hugh Tomlinson QC added: "The tribunal indicated it will find the accessing of communications was unlawful. These are supposed to be draconian powers used in extreme circumstances."

In 2010, the Mirror told how Price had started a fling with Eastwood, now his wife. An internal report by Cleveland Police told how he tried to cover up his affair when we first broke the story.

Terror plot foiled "in its final few hours" after spooks hack attackers' phones and emails

But in interviews with officers investigating alleged corruption, Price admitted the affair started in 2009, when he was still in the £750,000 home he shared with Jackie and their young son.

The report into his conduct said the information released on his behalf was "inaccurate and misleading". It added: "He allowed the view to be reported that they had met socially after they both separated. This was untrue."

And the probe into their conduct detailed tens of thousands of pounds of public cash spent on trips abroad.

Price blew £57,800 on his force credit card over five years to June 2011. He stayed at top London hotels with Eastwood and splashed out on food, travel and drink.

Rooms were booked but not used as they apparently tried to hide their relationship. The couple went to conferences in Estonia and Denver, USA. Eastwood claimed all the trips were "necessary and for a policing purpose".

But during one from Estonian capital Tallinn, she emailed her mum and told her: "One of my key tasks was to find a pub with the football on!!!!"

Price had insisted no public money had been used to accommodate them.

But the report stated: "On occasions, Price did use public funds in furtherance of his personal relationship with Eastwood."

UK security "failing" to protect Brits from fraud and cyber criminals warn experts - 7 ways you can stay safe online

Operation Sacristy, which looked at allegations of corruption, said the evidence was "strongly suggestive of dishonest use of significant public funds to the benefit of Price's relationship".

He told investigators that "at no time did I cause the Mirror to report that my relationship with Heather had begun later than it had. I did not speak to any reporter at the Mirror about this matter."

But the probe found "three occasions" prior to the story where the evidence suggested that they shared a room.

Five months after our phone records were accessed, Price became the first chief constable to be sacked in 35 years.

We also told how the force tried to claim back £330,000 in bonuses paid to him. That was later dropped.
Price was yesterday spotted leaving his home in Northallerton, North Yorks. He made no comment. Cleveland Police said: "We have fully co-operated with the tribunal and process and await the determination of the panel in the coming weeks."

LOAD-DATE: December 18, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

13 ways your online privacy was violated in 2016 - and what you can do about it;
Founder of MeWe and privacy expert Mark Weinstein looks back at 2016 - and it hasn't been a great year when it comes to online privacy

BYLINE: By Jo-Anne Rowney

SECTION: TECHNOLOGY

LENGTH: 1981 words

This year hasn't been the best - and we're not even talking about the 'real' world here. Just take a look back at what has happened in terms of our online privacy and try not to shiver in fear. The digital world has not been kind to us in 2016.

While some of in the tech industry have made progress, we continue to encounter violations that halt any real, transformative change, especially in the privacy department.

Founder of MeWe and privacy expert Mark Weinstein has put together a list of 2016's top privacy and security violations that will make you rethink everything you use online.

If these don't keep you up at night (probably because more often than not we were all unaware of them), they will by the time you finish reading.

WhatsApp originally prided itself on privacy. Then it got bought by Facebook.

Close to one year later, WhatsApp announced that, under its new terms and conditions, it will now share your personal information with its parent company; Facebook.

WhatsApp claimed that these changes were in the best interest of the user (fighting spam and increasing business-to-consumer communication).

We'll leave it up to you to decide if sacrificing your privacy in your own best interest.

How high-tech Christmas presents could steal your identity and drain your bank account
Uber updated its app to track users' locations even when they're not using the app. Uber said it was just data collection and analysis for improving the pickup and drop-off experience. That's questionable thinking, but scarier is the precedent such an action takes, suggesting this practice is okay. It's not.

Earlier this year, Uber also had to pay a $20,000 fine to the FTC for providing unauthorised third-party access to drivers' personal information and using aerial tracking to identify riders. Let's hope that such actions don't become the norm.

We all know that Google tracks the location, text messages, and call logs of its devices users. What we didn't know until recently was that information went not only to Google, but also to a mysterious server in China.

To make matters worse, the backdoor used for the practice comes through pre-installed monitoring software, meaning it's not malware or a security breach. It's part of the device. According to the New York Times, American authorities don't know if the data is being collected for advertising purposes or government surveillance. That's not very comforting.

UK security “failing” to protect Brits from fraud and cyber criminals warn experts - 7 ways you can stay safe online

2016 saw a surge in fitness trackers, which while a helpful resource, revealed a lack of data protection. That's because The Health Insurance Portability and Accountability Act, better known as HIPAA, protects sensitive patient data according to the world as we knew it in 1996. These regulations predate mobile devices and the common use of the internet. Now in the 21st century, we're learning there's little online protection of our health information. Basically you share everything with products from companies such as Fitbit and in return they sell it to advertisers. You'd think we'd be in control of our medical profiles and our personal fitness habits.

Pokémon Go became a worldwide phenomenon, but at what price?

A big hullabaloo arose about Pokémon Go's full functionality requiring access to a user's entire Google account on iOS, including your location data, email and browsing history. Seems a bit much? How else do you think Google can help you find a Squirtle or Caterpie near you?

Pokémon Go has to mine where you go, how you get there, and how long you stay. But your email? That's bizarre and creepy. Other location apps such as Foursquare and Tinder do the same thing, as does Facebook. Pokémon Go however, can do it to a level no other app ever has before as they monitor every step, literally. That's not the kind of gameplay we need to be encouraging. The game is great, but the privacy behind it is non-existent and a black hole for your “permanent record” as they store, monitor and pave the way to a world where they could even sell what you've been up to - naughty or nice.

Snapchat introduces hi-tech sunglasses with built-in camera which captures 10-second clips - and it's a bargain

Glasses help us put the world into focus. SnapChat's Spectacles help us survey, record and post that view, without the permission of those caught on video.

With one simple tap, ten seconds of someone's soul gets automatically uploaded onto the recorder's account.

If that sounds disturbing, it's because it is. Generation Z is the most recorded generation in history - willingly.

Even they would be less likely to express themselves freely or be true to themselves if they felt they were being recorded at all times though.

Such technology is invasive and impedes innovation. Remember Google Glass? People don't really seem to want this.

Late this year, the Chinese government introduced a system that connects citizens' financial, social, political and legal credit ratings to create a social score - as if they weren't monitored enough already.

Then Facebook openly and willingly offered to provide every tidbit of data on their Chinese members and censor news on its site - then the Communist nation would let the social media app back into the
country. In western democracies, such blatant actions would be a clear violation of people's rights and freedom of speech.

Facebook's Mark Zuckerberg in 'fake news' crackdown on as he creates new executive job to lead purge

Back in May, we learned that trending news on Facebook was controlled and edited by people - who were capable of discerning real news from fake news.

It seems this particular team overreached a bit and also 'manipulated' what appeared, but really why is this a surprise?

Forget privacy here - we already know Facebook assigns political labels to users based on what they see them do. This led to an uproar when conservatives discovered that stories in line with their beliefs were being 'suppressed' by liberal-leaning editors. No matter where you stand on the political spectrum, this is first a remarkable privacy violation, and second, incredible censorship. We aren't supposed to censor or filter real news on social media. Then Facebook fired their filtering team. Of course humans still programme the algorithms. What was the result? Facebook's algorithms boosted and spread fake headlines and news stories, distorting reality and very likely impacting the USA election.

Mark Weinstein: Did Facebook elect Trump President? The role it played with 'fake news'

Algorithms used to be equations assigned to math books. Time travel used to be the fodder of science fiction. Now social media sites and search engines use algorithms to change the order of time.

This year saw major sites such as Facebook and Instagram radically change algorithms, which changes everyone's news feeds. In other words, your news feeds and timelines aren't shown to you in real time - the algorithms of Facebook, Snapchat, Instagram and Twitter manipulate them - to display posts and content they think you want to see. A lot of people aren't happy with this and with good reason. Part of the fun of these apps is that we get to see what people are doing or saying or what's happening in the actual real life moment. Algorithms take that away. They ruin relevancy and introduce delay. News feeds are meant to be objective, yet these equations make them subjective. That subjectivity comes from mining through what we do online. So in the end, we are violated twice - by the invasion of privacy and the control of what we see - what we don't see, and when we see it.

Earlier this year, Twitter, Facebook and Instagram were called out by the California branch of the ACLU for sharing user data with a social media monitoring tool that tracks activists' conversations. That isn't very democratic. Even worse, the product can be manipulated to target activists of color, which has forced some Black Lives Matter activists off of social media and underground.

Facebook similarly got called out in 2016 for letting advertisers exclude specific "Ethnic Affinities," which the company unveiled by collecting facts about users likes and friends. This is not only totally racist, but it also violates federal law.

The Fair Housing Act of 1968 and the Civil Rights Act of 1964 detail how you can't exclude people based on race, gender, print notices or ads that show preferences or limitations based on the same criteria. Facebook must have missed that civics lesson.

Our federal government tried to make Apple open a backdoor so it could peruse information in a suspect's smartphone. Apple CEO Tim Cook became a privacy advocate/hero fighting back. A lawsuit looked inevitable, until the government said it found a way on its own to achieve the same end goal. Rather than end the debate, such an announcement appears to be dynamite to the whole subject. If government can bypass manufacturers in one instance, then what stops it from doing it over and over again? Devices are a convenience meant to keep us connected to people and our content. Turning them into evidence against ourselves or a confessional platform endangers the future of us and our technology.

Yahoo hack: What to do if you use Yahoo email, Tumblr, Flickr or Yahoo Finance

1) In September, Yahoo announced that 500 million user accounts had been breached and the data within them compromised. That alone would make for a bad year.

2) In November, word leaked that Yahoo had allowed U.S. intelligence agencies to read through its user emails in search of red flag phrases or keywords. Everything users have written suddenly available to be held against them in a court of law - as part of their "permanent record," that nasty electronic dossier that lives forever in the hands of those who watch. It was an egregious violation of epic proportions and a perfect end to Yahoo's year, until of course Yahoo reported at year's end that....
3) one billion user accounts had been hacked back in 2013. Yes, within one calendar year, Yahoo had managed to achieve three epic acts of privacy ineptitude. What is going on at Yahoo?

**Snoopers' Charter passes into law giving British intelligence services sweeping internet surveillance powers**

Yes, even the UK has co-opted reasonable privacy mores. Officially known as The Investigatory Powers Act 2016, the Snoopers Charter in many ways gives UK police and spy agencies a carte blanche for keeping tabs on citizens. It supports the legalisation of global surveillance, data collection, government hacking, decryption, data mining of emails and app activity and as the cherry on top, monitoring all internet browsing - the good, the bad, and the none of your business. Edward Snowden called it: "The most extreme surveillance in the history of western democracy." While most of these invasive actions will require a warrant, don't expect a lot of pushback from governments who request permission to spy on its population.

It's clear that there are several large perpetrators and everything you do at Facebook, Google, Snapchat and so on, is stored in your online permanent record: what you like, your politics, your partying, your religion, your health issues, who you are friends with, what you say... and now It all affects your ability to get a job, get into school, your car insurance - basically everything. Is this ok?

There are websites that allow you to network without tracking them.

Maybe it's time for all of us to take action and end our support for privacy violators, demand better laws to protect our privacy rights, and join apps and networks that eliminate unnecessary corporate and 'Big Brother' surveillance.

Are you worried about your online privacy?

See any privacy violations missing from our list? Join in the conversation! Use #WORSTyear4privacy and let me know what you think were the worst privacy crimes this year.

**LOAD-DATE:** December 21, 2016

**LANGUAGE:** ENGLISH

**PUBLICATION-TYPE:** Newspaper; Web Publication

**JOURNAL-CODE:** WEBDMI

Copyright 2016 Trinity Mirror, Plc.
All Rights Reserved

Return to List

43 of 100 DOCUMENTS

i-Independent Print Ltd

**December 16, 2016**
First Edition

**Think ethical and make a gift special**

**BYLINE:** SOCIETY Elaine Ritch

**SECTION:** NEWS; Pg. 22

**LENGTH:** 333 words

Let's be honest, many Christmas gifts this year will end up in landfill, taking hundreds of years to decompose, contributing to climate change all the while.
And yet, from interviews I conducted, I found people took extra pleasure in the back stories to ethical gifts they had previously received. "Cleaner" production behind the gift also meant both giver and recipient were more connected to the product. And yet the trick, invariably, is to still give something that the recipient wants. So what are the top ethical but interesting gift ideas? Here are my suggestions. 1. Remakery Centres dedicated to repairing and reusing old products have been catching on in recent years. London has at least one while I'm aware of five in Scotland.

My local Edinburgh Remakery not only sells upcycled and secondhand products but holds workshops teaching people how to repair broken items in their home, covering everything from computers to furniture to books.

2. Local design collectives A good example is Snooper's Attic in Brighton, which sells a variety of locally designed and produced goods including jewellery, homewares and clothes. As well as offering novel and unique designs, many of these wares use reclaimed or sustainable materials. Supporting collectives like these also provides employment for young local designers - giving them an alternative to unpaid internships in bigger cities, while registering a protest against unfair trade at the same time.

3. Making something Your mum probably still has the cards and drawings you gave her when you were little, and she will never throw them out. And remember getting a mixtape from a boy/girl and how special that felt? In both cases, the value was in the giver spending time thinking about someone and creating something just for them - whether it's jams, infused oils, cakes, biscuits paintings, photo collections or baskets. Personally, I have my knitting needles out.

THE CONVERSATION Elaine Ritch is a lecture in marketing at Glasgow Business School

LOAD-DATE: December 15, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: III

Copyright 2016 Independent Print Limited
All Rights Reserved

Return to List

44 of 100 DOCUMENTS

mirror.co.uk

December 15, 2016 Thursday 12:01 AM GMT

UK security "failing" to protect Brits from fraud attacks, fake goods, and cyber criminals - 7 ways you can protect yourself;

A new investigation has warned that the UK's security system is not protecting consumers from modern scams, unfair trading, and unsafe goods - leading to billions of successful attacks each year

BYLINE: By Emma Munbodh

SECTION: MONEY

LENGTH: 1166 words

The UK is failing to keep up with online fraud, and consumers are increasingly being left vulnerable to scams, unfair trading, and unsafe goods, according to the National Audit Office (NAO).
The NAO estimated that consumers lost at least £14.8 billion to fraud last year, of which £4.2 billion is thought to be hidden from crime such as mass marketing fraud and counterfeit goods.

Consumer protection cost around £165 million over the year, with local Trading Standards services receiving around £124 million and Citizens Advice receiving £18 million, the NAO calculated.

But it said the system as a whole "has not yet demonstrated that it provides value for money in protecting consumers from modern scams, unfair trading, and unsafe goods".

This scam email claims you've been caught speeding - and then empties out your bank account

National Trading Standards, which was set up in 2012 had made a "good impact" into consumer protection, preventing £345 million worth of losses since April 2014.

But the NAO said funding for this remained small compared with the size of the problem.

It warned that the system was not keeping pace with the growth in online consumer fraud within the UK's e-commerce market - now the third largest globally.

Local Trading Standards teams have also lost 56% of full-time equivalent staff since 2009, with 20 services in England suffering funding cuts by over 60% since 2011 and some offices left with one qualified officer.

But despite this, the teams were expected to enforce 263 different pieces of legislation "with little direction from government on the priority of these".

The 12 cons of Christmas revealed - and what you can do to make sure you avoid them

NAO head Amyas Morse said: "As the threats consumers face become increasingly wide-ranging, the system has not kept pace with the changes, leaving consumers inadequately protected in a number of areas.

"While the improvements are welcome, the system as a whole has not yet shown it provides value for money."

Leon Livermore, chief executive of the Chartered Trading Standards Institute, said: "The amount spent on trading standards has fallen from £213 million in 2011 to £125 million today, so it's not surprising the system is struggling to cope.

"It has left consumers inadequately protected and has helped to set the conditions for issues like the horsemeat and hoverboards scandals and the ongoing problems with Whirlpool and VW."

Fraudsters and criminals are hard at work this time of year. A number of Mirror Money readers have already been in touch to share their experiences following a new wave of email, post and telephone scams, trying to lure customers into giving out sensitive information under false pretenses.

As it currently stands, over two thirds of us are worried about keeping personal information secure online and almost three quarters feel they are as much at risk of being a victim of a cyber-attack as a celebrity, according to research by credit reporting service Noddle and Cyber Aware - the Government's cyber security initiative.

"Your Amazon order cannot be shipped" - the scam email to AVOID as online giant kick off Black Friday sale

A huge 86% of those surveyed confessed they don't always read the terms and conditions when downloading a new app, with one in five of us disabling security settings online to access an app.

Commenting on the findings John Cannon, Fraud & ID Director at Noddle told Mirror Money: "Being Cyber Aware is about taking steps to protect yourself that are simple and effective and - crucially - not time consuming"

Noddle has teamed up with GCHQ to put together five top tips to stay safe online, using the mnemonic AWARE.

A - Always download software updates: Software and app updates contain vital security upgrades which help keep your devices secure. Turn on auto updates to make sure you're benefitting from these upgrades.

W - Watch out for bogus friend requests: Don't always accept friend requests on social media as you could end up with more foes than intended.
A - Actively check your privacy and security settings: Never disable the security settings on your device, social media profiles or online banking and check your privacy settings are high on the services you use, like Facebook.

R - Random words make for strong passwords: A strong password is your first defence against hackers and cyber criminals. Use three random words to make a strong password.

E - Every shopping basket should be secure: Check for the padlock symbol or 'https' in the URL before finalising any online purchase.

We've teamed up with Get Safe, Action Fraud and NordVPN, a Virtual Private Network service provider to bring you some top tips for shopping online this Christmas.

When is the last day to order online for Christmas: Argos, Amazon, John Lewis and more delivery dates for your diary

Before you start shopping online secure your device. Whether it's a personal computer, tablet or phone, by updating its operating system and anti-virus software if installed.

Only use secure websites for purchases, never buy anything from a site that does not have 'https' at the start of the URL and also look for the icon of a locked padlock at the bottom of the screen.

Always use common sense, don't be seduced by "bargains" from companies which you don't know, if something appears too good to be true, it probably is.

If you get an email with a "bargain" on it don't, even if you know the company, click the link instead go directly to the web site. If you click the link you could be taken to a copy of the web site where your details will be captured, or worse ransomware could be downloaded onto you device. Just delete them because even an "unsubscribe" link could be malicious.

Only shop with companies you know and trust. If you don't know the company you need to do some background checks. Watch out for fake websites that look like real one. You can tell by checking the URL of the website, it may have a different spelling or a different domain name that ends in .net or .org.

If your shopping online shop from home, not on the go. Using public WiFi hotspots such as those offered by coffee shops, libraries and bars could leave you vulnerable. If it won't wait until you get home use your own 3G/4G network.

Public Wi-Fi networks are common hunting grounds for attackers and data snoopers who try to access your personal information and use it for their benefit on your expense. Since public networks have negligible security, you should try and avoid using them while making online payments. If you must do online transactions while using a public network, then you have to use a VPN to stay safe.

Always log out of accounts, including online Banking, as the session you have just had stays active for a period and could be high-jacked.

Be careful of follow-up responses that appear to arrive after your purchases. Such as an email that asks you to click on a link and enter your details to rearrange a delivery, but doesn't tell you what the item is - similar to this one.
UK security "failing" to protect Brits from fraud attacks, fake goods, and cyber criminals - 7 ways you can protect yourself;
A new investigation has warned that the UK's security system is not protecting consumers from modern scams, unfair trading, and unsafe goods - leading to billions of successful attacks each year

BYLINE: By Emma Munbodh

The UK is failing to keep up with online fraud, and consumers are increasingly being left vulnerable to scams, unfair trading, and unsafe goods, according to the National Audit Office (NAO).

The NAO estimated that consumers lost at least £14.8 billion to fraud last year, of which £4.2 billion is thought to be hidden from crime such as mass marketing fraud and counterfeit goods.

Consumer protection cost around £165 million over the year, with local Trading Standards services receiving around £124 million and Citizens Advice receiving £18 million, the NAO calculated.

But it said the system as a whole "has not yet demonstrated that it provides value for money in protecting consumers from modern scams, unfair trading, and unsafe goods".

This scam email claims you've been caught speeding - and then empties out your bank account

National Trading Standards, which was set up in 2012 had made a "good impact" into consumer protection, preventing £345 million worth of losses since April 2014.

But the NAO said funding for this remained small compared with the size of the problem.

It warned that the system was not keeping pace with the growth in online consumer fraud within the UK's e-commerce market - now the third largest globally.

Local Trading Standards teams have also lost 56% of full-time equivalent staff since 2009, with 20 services in England suffering funding cuts by over 60% since 2011 and some offices left with one qualified officer.

But despite this, the teams were expected to enforce 263 different pieces of legislation "with little direction from government on the priority of these".

The 12 cons of Christmas revealed - and what you can do to make sure you avoid them

NAO head Amyas Morse said: "As the threats consumers face become increasingly wide-ranging, the system has not kept pace with the changes, leaving consumers inadequately protected in a number of areas.

"While the improvements are welcome, the system as a whole has not yet shown it provides value for money."

Leon Livermore, chief executive of the Chartered Trading Standards Institute, said: "The amount spent on trading standards has fallen from £213 million in 2011 to £125 million today, so it's not surprising the system is struggling to cope.

"It has left consumers inadequately protected and has helped to set the conditions for issues like the horsemeat and hoverboards scandals and the ongoing problems with Whirlpool and VW."

Which? director of campaigns and communications, Vickie Sheriff, said: "With consumer losses of around £14.8 billion annually, it cannot be right that some Trading Standards services have suffered dramatic cuts leaving people so poorly protected against scams and other threats.

"The Government must take action urgently to ensure that a sustainable and robust system is in place to protect consumers."
A Government spokeswoman said: "We will carefully consider the NAO’s findings as part of our ongoing work to examine the consumer protection regime and will publish a Green Paper in spring 2017."

Fraudsters and criminals are hard at work this time of year. A number of Mirror Money readers have already been in touch to share their experiences following a new wave of email, post and telephone scams, trying to lure customers into giving out sensitive information under false pretenses.

As it currently stands, over two thirds of us are worried about keeping personal information secure online and almost three quarters feel they are as much at risk of being a victim of a cyber-attack as a celebrity, according to research by credit reporting service Noddle and Cyber Aware - the Government’s cyber security initiative.

"Your Amazon order cannot be shipped" - the scam email to AVOID as online giant kick off Black Friday sale

A huge 86% of those surveyed confessed they don't always read the terms and conditions when downloading a new app, with one in five of us disabling security settings online to access an app.

Commenting on the findings John Cannon, Fraud & ID Director at Noddle told Mirror Money: "Being Cyber Aware is about taking steps to protect yourself that are simple and effective and - crucially - not time consuming"

Noddle has teamed up with GCHQ to put together five top tips to stay safe online, using the mnemonic AWARE.

A - Always download software updates: Software and app updates contain vital security upgrades which help keep your devices secure. Turn on auto updates to make sure you're benefitting from these upgrades.

W - Watch out for bogus friend requests: Don't always accept friend requests on social media as you could end up with more foes than intended.

A - Actively check your privacy and security settings: Never disable the security settings on your device, social media profiles or online banking and check your privacy settings are high on the services you use, like Facebook.

R - Random words make for strong passwords: A strong password is your first defence against hackers and cyber criminals. Use three random words to make a strong password.

E - Every shopping basket should be secure: Check for the padlock symbol or 'https' in the URL before finalising any online purchase.

We've teamed up with Get Safe, Action Fraud and NordVPN, a Virtual Private Network service provider to bring you some top tips for shopping online this Christmas.

When is the last day to order online for Christmas: Argos, Amazon, John Lewis and more delivery dates for your diary

Before you start shopping online secure your device. Whether it's a personal computer, tablet or phone, by updating its operating system and anti-virus software if installed.

Only use secure websites for purchases, never buy anything from a site that does not have 'https' at the start of the URL and also look for the icon of a locked padlock at the bottom of the screen.

Always use common sense, don't be seduced by "bargains" from companies which you don't know, if something appears too good to be true, it probably is.

If you get an email with a "bargain" on it don't, even if you know the company, click the link instead go directly to the web site. If you click the link you could be taken to a copy of the web site where your details will be captured, or worse ransomware could be downloaded onto you device. Just delete them because even an "unsubscribe" link could be malicious.

Only shop with companies you know and trust. If you don't know the company you need to do some background checks. Watch out for fake websites that look like real one. You can tell by checking the URL of the website, it may have a different spelling or a different domain name that ends in .net or .org.

If your shopping online shop from home, not on the go. Using public WiFi hotspots such as those offered by coffee shops, libraries and bars could leave you vulnerable. If it won't wait until you get home use your own 3G/4G network.
Public Wi-Fi networks are common hunting grounds for attackers and data snoopers who try to access your personal information and use it for their benefit on your expense. Since public networks have negligible security, you should try and avoid using them while making online payments. If you must do online transactions while using a public network, then you have to use a VPN to stay safe.

Always log out of accounts, including online Banking, as the session you have just had stays active for a period and could be high-jacked.

Be careful of follow-up responses that appear to arrive after your purchases. Such as an email that asks you to click on a link and enter your details to rearrange a delivery, but doesn't tell you what the item is - similar to this one.

LOAD-DATE: December 15, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

Cod bless them all;
The decline of fish 'n' chips is hard to swallow in Brexitland

BYLINE: My View Grace Dent

SECTION: NEWS; Pg. 13

LENGTH: 606 words

In an only slenderly "United" Kingdom in need of no real reason to bicker, I am here to chuck petrol on the Brexit bonfire by declaring the death of cod and chips.

Yes, the Great British Cod Supper is under threat, according to research led by Dr John Pinnegar of Cefas, the Centre for Environment, Fisheries and Aquaculture Science, and it is soon to be replaced with the more readily available calamari. It is time to learn to love squid. It looks like a gonad and tastes of nothing especially but, frankly, needs may lead to must.

Pinnegar's outlook for 2025 and beyond suggests that seawater temperatures will continue to rise. "As a result," he says, "UK waters will become more hospitable for some species and less suitable for others." Most commercial species will move northwards, he predicts, and in the meantime, squid numbers in the North Sea have increased rapidly.

Essentially, once the post-Brexit bunfight over sea territories has subsided, it seems likely that Britain's little patch of watery turf, which we must ransack daily to support ourselves, is likely to be Squid City. It's perfectly agreeable, incidentally, fresh and sliced thinly, wrapped in a light, crisp batter and served with a punchy, homemade aioli and nice bottle of Picpoul de Pinet. But I'm not helping, am I? None of this will delight cod lovers, climate change deniers and staunch Brexiteers. And especially those who tick all three boxes at once.
I like to imagine two such women, in Huddersfield, right this moment, clad in Union Jack minidresses bought on eBay, with home highlights, spam arms and flinty eyes, currently penning a pithy protest song for their YouTube channel rhyming "Evil, stupid Pinnegar" with "Give us back our salt 'n' vinegar." Or perhaps "Calamari" with "Gonna need a bigger army".

But, on a slightly more serious note, it is the erosion of "British things" that is an especially touchy subject with many right now, and "cod and chips under threat" creates the perfect storm of Little Englander anxiety.

Many said in the run-up to Brexit that the Leave campaign's best selling point was the promised return of little slices of a cosy halfremembered yesteryear. Back doors left open, morris dancers on high days, cream teas, friendly bobbies on every corner, and a time when sitcoms littered with freedom of speech rendered us weak with mirth.

This revisionist vision no doubt stretches to a time of cod and chip shops on every street served by twinkly eyed chippy-owners who asked after your old mum, selling enormous, non-costly cods wrapped in yesterday's local gazette.

None of your chicken shish, pickled chillies, pizzas or cartons of curry sauce. None of your NHS nanny state snoopers pointing out the pitfalls of diabetes, albeit a long-winded, highly effective way to spend less on socks.

I'm guessing that many of the 52 per cent may refuse to acquiesce to a narrative where global warming, combined with the country's intention to rethink Europe's imperfect but nevertheless workable agreements over fishing territories, has led to their local chippy now serving mainly puntillitas salteadas.

Nonsense: it will be the fault of those immigrants, coming over here, with their spicy, delicious multiculturalism.

Or it will be Brussels fault. Those fat cats with their unfair new fishing boundaries, steamrolling over the Great British Cod and Chips. Saying that, in a sense blaming Europe and Angela Merkel for our lack of cod, does have cosily nostalgic ring to it. Those bloody Germans. Yet again, they bombed our chippy.

Blaming Europe and Angela Merkel does have a cosily nostalgic ring to it
In an only slenderly "United" Kingdom in need of no real reason to bicker, I am here to chuck petrol on the Brexit bonfire by declaring the death of cod and chips. Yes, the Great British Cod Supper is under threat, according to research led by Dr John Pinnegar of Cefas, the Centre for Environment, Fisheries and Aquaculture, soon to be replaced with the more readily available calamari. It is time to learn to love squid. It looks like a gonad and tastes of nothing especially but, frankly, needs may lead to must.

Pinnegar's outlook for 2025 and beyond suggests that seawater temperature will continue to rise. "As a result," he says, "UK waters will become more hospitable for some species and less suitable for others." Most commercial species will move northwards, he predicts, and in the meantime, squid numbers in the North Sea have increased rapidly.

Essentially, once the post-Brexit bunfight over sea territories has subsided, it feels to me likely that Britain's little patch of watery turf, which we must ransack daily to support ourselves, is likely to be Squid City. It's perfectly agreeable, incidentally, fresh and sliced thinly, wrapped in a light, crisp batter and served with a punchy, homemade aioli and nice bottle of Picpoul de Pinet. But I'm not helping, am I?

None of this will delight cod lovers, climate change deniers and staunch Brexiteers. And especially those who tick all three boxes at once. I like to imagine two of these women, in Huddersfield, right this moment, clad in Union Jack mini-dresses bought off eBay, with home highlights, spam arms and flinty eyes, currently penning a pithy protest song for their YouTube channel rhyming "Evil, stupid Pinnegar" with "Give us back our salt 'n' vinegar." Or perhaps "Calamari" with "Gonna need a bigger army". But, a tad more seriously, it is the erosion of "British things" that is an especially touchy subject with many right now, and "cod and chips under threat" creates the perfect storm of Little Engander anxiety.

Many said in the run-up to Brexit that the Leave campaign's most insidious gift was the promised return of little slices of a cosy half-remembered yesteryear. Back doors left open, morris-dancers on high days, cream teas, friendly bobbies on every corner, and a time where sitcoms littered with freedom of speech rendered us weak with mirth.

This revisionist puddle-vision will no doubt stretch to a time of cod and chip shops on every street served by twinkly-eyed chippy-owners who asked after your old mum, selling enormous, non-costly cods wrapped in yesterday's local gazette. None of your chicken shish, pickled chillis, pizzas or cartons of curry sauce. None of your NHS nanny state snoopers pointing out the downfalls of diabetes, albeit a long-winded highly effective way to spend less on socks.

I'm guessing that many of the 52 per cent may refuse to acquiesce to a narrative where global warming, combined with the country's intention to rethink Europe's imperfect but nevertheless workable agreements over fishing territories, has led to their local chippy now serving mainly puntillitas salteadas. Nonsense: it will be those immigrants' fault, coming over here, with their spicy, delicious multiculturalism.

Or it will be Brussels' fault. Those fatcats with their new unfairly shared-out fishing boundaries, steamrolling over the British Great Cod and Chips. Saying that, in a sense blaming Europe and Angela Merkel for our lack of cod does have cosily nostalgic ring to it. Those bloody Germans. Yet again, they bombed our chippy.
The Walking Dead, season 7, episode 8, Hearts Still Beating review: Rick finally wakes up and smells the viscera in a bloody mid-season finale

BYLINE: By Ed Power
SECTION: TV
LENGTH: 1537 words

Warning contains spoilers for season 7, episode 8 of The Walking Dead

There was plenty of guts but not much glory as The Walking Dead signed-off with a mid-season finale likely to trigger further complaints regarding the show's over-the-top violence.

With an Ofcom investigation underway following the bloody first episode of the new series - google "Glenn" and "eyeball" if you're in the dark/feeling brave - the zombie melodrama bowed out with another grisly flourish. Apropos of very little, a character's stomach was slit open and out gushed bucketloads of Eighties horror movie gore. Was the Walking Dead actively daring the wavering elements among its fanbase (ratings have dipped ominously of late) to take offence?

As with Negan's earlier attack on Glenn and Abraham, the bloodshed, once again at the hands of the Saviour leader, was brief and intense. It was also entirely gratuitous, with smooth operator Spencer (Austin Nichols) crowbarred into an unnecessary confrontation with Negan (Jeffrey Dean Morgan) that left the former splashing around in his own internal organs.

That Spencer should have ended up in this situation did little to further the plot - the Walking Dead put him there simply to end the first half of the season in a rhapsody of body horror.

True, terrible special effects - Spencer's "guts" looked like something purloined from 'round back at a butcher's stall - and hammy acting resulted in a scene more comedic than shocking. Still, for all the silliness, it's easy to imagine the sequence leaving an unpleasant taste among more sensitive viewers (i.e. anyone not raised on straight-to-video horror film).

Yet there was a sunny aspect to this orgy of disembowelling, in that it removed Rick's blinkers. Finally (finally!) the supine Sheriff (Andrew Lincoln) understood there was no compromising with the Saviours and their leering boss. If Alexandria's surviving inhabitants didn't fight back, they would inevitably suffer Spencer's grisly fate. So fight they would. Here is the rest of what we learnt:

1: Of course Spencer's plan to betray Rick went wrong

We knew it was curtains for aspiring power-player Spencer the moment he presented the Saviour kingpin with that bottle of scotch. Negan, we have learned, reserves a particular enmity for anyone underestimating him as a brainless thug. Thus it was inevitable that Spencer's naked ploy (inveigle his way into Saviours's inner circle, then topple them from within) would bring out the villain's vengeful side.

Because the story demanded it, Negan initially played along. He swigged hooch on the porch with his new bestie and agreed to a game of pool, with the table dragged onto the main street so that key characters could watch. There Spencer made his pitch: Rick was an unpredictable leader while he, the son of a politician, would make for a perfect liaison between the Savours and Alexandria.

Credit:      Fox     2: Spencer's death was simultaneously horrible and comedic

Negan had fun delivering one of his grandiose speeches. Rick was even now out in the wilderness scavenging for his new master, he declared. Meanwhile, here was Spencer mooshing about in the safety of Alexandria. You could - drum roll please - even say he "lacked guts".
Can you guess what happened next? Yes, you can. Negan plunged a dagger into Spencer's midriff, his would-be ally gawping as viscera spilled down his lap.

"How embarrassing," cackled Negan, bravely pushing on with his "guts" gag. "They were inside you the whole time." It was a tragic end for Spencer. His cunning plan had come unstuck. Worse still, the last thing he heard as his life slipped away was Negan cracking up at one of his own terrible jokes. It isn't how any of us would choose to go.

3: Rick's redemption felt unearned but we'll take it anyway

All season Rick has been a mopey bore, with Andrew Lincoln endlessly recycling his repertoire of sad / very sad expressions (turns out he doesn't have that many). Now we were asked to believe that, after all that bowing and scraping before Negan, he has rediscovered his fighting spirit. And just in time for the mid-season finale, too.

"I didn't listen," Rick confessed to Michonne during one of their tearful snogs. "I couldn't ...I can now." Fair enough, the stakes had been ratcheted up with Spencer's and Olivia's deaths at the hands of the Saviours. But just as Rick's original moral cave-in didn't convince, his rebirth felt like a writers' room contrivance rather than an organic development. Still, Sad Rick has been an enormous drag so let's not complain too loudly. We'll take the old character back regardless of how his strained the turnabout feels.

4: How are we coping with Olivia's death?

Spencer's icky demise was the twist everyone saw coming. He had spent the past few episodes quietly undermining Rick - even attempting to turn the saintly Father Gabriel against the leader of Alexandria. So his comeuppance had a whiff of just desserts (anyone for a second helping of terrormisu?).

In contrast, the random execution of Olivia (Ann Mahoney) as punishment for Rosita's botched assassination attempt rated as a genuine surprise. Though she was very much a second string protagonist, viewers will have grown to appreciate Olivia's solid book-keeping and mid-level lemonade making.

That her death tugged harder at the heartstrings than Spencer's gory demise was a reminder, moreover, that Walking Dead doesn't need spraying arteries to deliver its point. Just make us care, even a little, about a character before you kill them off.

Credit:      Fox     5: When Lucille stopped Rosita's bullet, the Walking Dead turned into a slapstick comedy

With just one bullet with which to take down Negan - honestly, why didn't she ask Eugene to cook her up a batch? - Rosita (Christian Serratos) contrived to ping his baseball bat Lucille instead. As the smoke cleared, Jeffrey Dean Morgan was required to look momentarily terrified, the first time all season his range has extended beyond 50 shades of smarminess.

But if the scene worked (just about) at a dramatic level, it kicked sand in the face of logic. Could a length of wood - even a really cool length of wood garlanded in barbed wire - get in the way of a point-blank shot?

Never mind the ballistics, this was just silly, with confusing editing adding to the unintentional hilarity. More unforgivable still was the fact that Rosita's big moment was essentially tacked on as an afterthought while we were still processing Spencer's death. She deserved better, and so did the audience.

6: Daryl has gone to the dark side

Chained, beaten, forced to listen to upbeat indie rock for weeks on end, something has snapped within Daryl (Norman Reedus). In an otherwise shaggy and dialogue-heavy episode, the point was demonstrated with chilling efficiency as the escaping prisoner blundered into Negan's comedy sidekick Fat Joseph. The old Daryl might have considered letting this accidental eye-witness go. But all that torture has snuffed out his humanity, as we discovered as he matter-of-factly beat Joseph to a bloody smear.

Credit:      Fox     7: We finally had a decent zombie scene

That the Walking Dead is more interested in the rag-tag societies springing up in the wake of the zombie apocalypse than in the undead themselves is no secret. Nonetheless, the series will now and then pander to straight-up horror aficionados by throwing in some tasty undead action. We had a super-sized helping this week as Rick and Aaron (Ross Marquand) were overwhelmed by the ghouls
sloshing around in the moat as they splashed their way towards that houseboat. Though we obviously knew Rick was safe, Aaron's fate was less certain. There was real tension as he was pulled under only to somehow stage a miraculous escape.

It's obvious how the rest of the season is going to play out.

Operation Neutralise Negan is officially underway. Rick and the gang returned to the Hilltop, exchanging Significant Glances with Maggie and Sasha as they strode purposefully towards Gregory's mansion (the only absentee was Eugene, whose bullet-making skills have earned him a one-way ticket to the Saviour compound). Meanwhile, Richard, Ezekiel's second in command at the Kingdom (please tells us you remember the Kingdom), wishes to recruit Carol and Morgan for a heave against their mutual enemies. The race to topple Negan has begun.

As with everything on the Walking Dead this will in all likelihood be a marathon rather than a sprint, as Jeffrey Dean Morgan has revealed his character will survive until next season at least. He's by far the most entertaining protagonist this year, so we should enjoy in his super-sized villainy for as long as it lasts. Without Negan swaggering around disembowelling everyone, what would there be to talk about?

Who is the watcher from afar?

The episode had one final twist, with a post-credit sequence in which a hooded figure with binoculars spied on Alexandria under cover of dark. Was the snooper a potential friend or another foe Rick and company haven't met yet? All will (presumably) be revealed.

The Walking Dead is broadcast in the UK on Fox, 9pm, Mondays

Walking Dead: Most Shocking Deaths

LOAD-DATE: December 12, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDTNS

Copyright 2016 Telegraph Media Group Limited
All Rights Reserved

Return to List

49 of 100 DOCUMENTS

Financial Times (London, England)

December 9, 2016 Friday
London Edition 1

The CIA snooper who learnt how to whistle;

FILM

BYLINE: Nigel Andrews

SECTION: ARTS; Pg. 10

LENGTH: 1275 words

Snowden (15)
Oliver Stone
AAAEE
Oliver Stone gets clattered by both the left and the right. He was attacked by the first for *Nixon* and *W* - too kind to Tricky Dick and George Dubya - and is now being attacked by the second for *Snowden*. Too kind to the traitor who sprayed US surveillance secrets around the world. They have a point. Partiality is the heel in this Achilles film; though to this Achilles film's credit, it also outruns, as storytelling, the tortoise forebodings we might have had about a true-life plot so cerebral and cyber-centric.

Joseph Gordon-Levitt plays Edward Snowden with a passable physical likeness, a skilful vocal one and the puppyish alertness of a school swot suddenly shot - self-shot - to the top of the world notoriety class.

For the film's first half he's sweet, well-meaning and in love (with Shailene *Allegiant* Woodley, swapping YA kitsch for true-life morality drama). He's schooled in CIA and NSA craft by sinister whisperers - Rhys Ifans, doing Clint Eastwood, and Scott Eastwood, doing (surprise) ditto - before conscience coaxes him to rebellion. A clever graphics sequence, mid-movie, presents US snooping as a pattern of whizzy, sparkling trajectories circling most of Cosmos Earth.

It's true: who can doubt it? But then those, too, may have truth on their side who accused Snowden of carelessness in risking lives by blowing covers - and of thoughtlessness about who might benefit from this info spill, among states hostile to freedom. (In one of which he now lives.)

The Snowden antagonists don't get a voice in the movie. Stone knows how to cut between time-zones and land-zones: we shuttle cleverly between a Hong Kong "present", with Ed holed in the Mira Hotel alongside reporter Glenn Greenwald (Zachary Quinto) and documentarist Laura Poitras (Melissa Leo), and a US past that pieces itself together in extended flashback. The director also cuts cannily between moods: the intimate music of Snowden's love life in fugal counterpoint with the Snoop-topia fever dreams of Langley and Washington. But the film has no idea, or no inclination, when it comes to cutting between pro-Ed and anti-Ed.

*Snowden* ends up as hagiography, pure and dimpled. It even gets Ed himself to fill the screen at the end with a glowing smirk, as if to say: "Yup, I changed history." He may have. He may even have improved it. Then again, he may have hazarded others' safety to create a world in which future leaders will maintain Snoop-topia with an even more fanatical care that leakers don't leak and the wicked (to them) don't Wiki.

No UK press show. Barely any UK release. (What are distributors Studiocanal thinking of?) Yet *Krisha*, Trey Edward Shults's first feature, already paean'd by some, is the best American independent movie of the year. At least it's out on DVD early next year.

The title character's emotional breakdown is filmed over a Thanksgiving Day in a big family home. Krisha Fairchild, Trey Shults's aunt, plays Krisha, white-haired, big-framed, piercing-eyed. Trey himself plays her estranged, resentful son. Krisha's sister and the drama's hostess, Robyn, is played by Robyn Fairchild, Trey's mum. It's her house they shoot in.
And what do they shoot? A long day's journey into Hell, filmed with choreographic power and murderous wit. The camerawork - from mocking, stately zooms to whirlly-angled arabesques - serves the changing moods. So does the music. The dainty Zen of oriental percussion; later, sombrely classical, then shriekily discordant strings.

Krisha is a recovering addict returning to the family embrace after long absence. It doesn't go well. Conversations turn to spats. Reconciliations unravel. And there's an astonishing scene, or extended shot, with a catastrophe-destined roasted turkey - a scene/shot right up there with Kubrick's bone-into-spaceship or Buñuel's Andalusian eyeball. If this isn't the first work of a major filmmaker I'll eat my review. And I'll film it for you on YouTube.

I Am Not a Serial Killer is Dostoevsky in Minnesota. Spiritually if not literally. The troubled youngster with the morbidly turning mind (Max Records) might be a sociopath. That's why mum minimises his workload in the family morgue. The creepy old neighbour (Christopher Back to the Future Lloyd) who kills and raids organs is definitely a sociopath. That's why the boy stalks him. He's a sleuth honed by kinship.

Robbie Ryan, the world's best indie cinematographer - Irish, like writerdirector Billy O'Brien - films this boondocks Walpurgisnacht with a moody incandescence. It's Notes from Underground with added, luminous sleaze. That and a haunted mirror play of motifs. The blood relationship of disturbed minds. The "healthy" eviscerations of the morgue twinned, or kinned, with the dedicated insanity of the murderer. And of course, in a film about organs, all that gothic organ music on the soundtrack.

There's a rough and ready enchantment - a magic of mood and landscape - in the prizewinning Nepalese film The Black Hen. The friendship of two boys defies the strife afflicting a nation and rural community during the country's civil war (1996-2006). Prakash (Khadak Raj Nepali) and Kiran (Sukra Raj Rokaya) search for a beloved hen, a diminutive pledge of peaceful prosperity, stolen and re-sought through writer-director Min Bahadur Bham's mazy fable.

The village busies itself with intrigues, barter, even a wedding. The war surges through, once, twice. Only in the last reel, a boys' journey, do the carnage and casual horror spread through the story. But even then there is a piquant, poignant detachment to this film, seeing tragedy more clearly by holding it at arm's length.

Nate Parker wrote, produced, directed and stars in The Birth of a Nation. Does he think he's Orson Welles - as well as African-America's D.W. Griffith? If so, he has bitten off more than he can chew. And more than the audience, presented with this helping of melodrama-with-a-message, can swallow.

It's the truth-based story of a slave uprising that took the lives of dozens on both sides. But the film sets it in Caricature County, Rhetoric State. Nate Parker plays his near namesake Nat Turner, black preacher and leader, with fire and force. But he doesn't share those virtues around; or only to light the torches of a generic, pantomime indignation in the slaves and a generic, pantomime brutality in the whites.

Armie Hammer, as Turner's master, is briefly ambivalent before turning into a tuppence-dreadful version of Michael Fassbender in 12 Years a Slave. The whole film is a tuppence-dreadful 12 Years a Slave. Its gurning white villainy, overblown music and kitschy visions of a white-winged black angel - mixed messaging, surely, in the chromatics of agitprop? - is further proof (after Selma, A United Kingdom and Co) that soapbox didacticism and complex drama can never coexist.

Life, Animated, directed by Roger Ross Williams, is a touching documentary about autism. Owen Suskind, now 23, lost his powers of normal speech at age three. Parents and older brother, unable to decode his sounds, mourned a baby lost to Babel. Then came the discovery moment. Owent's "gibberish" was copied from Disney animation movies. This autistic boy was a savant - of sorts. He could recite every line in every script from Bambi to The Lion King (with exact voices). The rest became history - a key to communication found, and, with Owen's family reaching out, a communion of insight founded with others.

LOAD-DATE: December 8, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper
A Conservative general election majority dangles like a bauble on the Number Ten Christmas Tree;

Please send your letters to letters@independent.co.uk

BYLINE: Letters

SECTION: VOICES

LENGTH: 817 words

After Theresa May's midweek Article 50 coup and the Conservative's win at Sleaford, Labour has barely "24 months" to save itself to become a credible political force again. Under Corbyn and Abbott's Marxist junta, Labour is becoming a footnote, little more than an irrelevant sideshow, not a serious contender to form the next government.

On the basis of the Sleaford result, her first real test as Prime Minister, May should not sack Boris Johnson but promote him to her general election mascot on a war footing. May has already proved herself more than capable of winning a majority at a snap general election on her own merits. With her St Bernard Boris on board, she may gamble on ascending to Alpine peaks at the next general election.

To fall out with Boris at this stage would leave him languishing on the back benches as a stalking horse, Heseltine-style, poisoning the well, always ready to pounce and make his bid for Number Ten. Just as the glittering prize of a May majority dangles like a bauble on the Number Ten Christmas Tree, sending Boris down would see it smashed on the pavement, with any hope of a the first Tory landslide for decades dashed for good.

May has the kugels to win big, but only with Boris unleashed, not shut up in the kennel with a muzzle.

Anthony Rodriguez
Middlesex

Gina Miller

In response to your article (Man arrested 'for threatening woman' who led Brexit legal challenge, 7 December).

How shameful that in the UK today anyone who speaks out for what they believe in is subjected to abuse and death threats, even more shameful that the threats are based on gender and race.

Is this what our country has become now - a place where the only views that count are those of bigoted white males? On the other hand how wonderful that the person making a stand for democracy in our multi-cultural country is neither white nor male.

I am deeply grateful to Gina Miller for attempting to ensure that the terms of Brexit are properly scrutinised by our elected representatives. For most of us, this is the most momentous political event of our lifetimes, so thank goodness someone is making sure it is given the most careful possible consideration.

Lynda Newbery
Bristol

The Warsaw Uprising
Robert Fisk is right to remind us of the unspeakable horror of the Warsaw Rising in 1944. But not everyone stood aside. As he mentions, the Royal Air Force did try, and in particular the South African Air Force made 12-hour flights from Italy to drop supplies - weapons, food and medical equipment. Sixty-nine South Africans were killed and twenty-five SAAF Liberators were shot down. For every ton of supplies dropped into Warsaw, one bomber was lost. It was perhaps the South African Air Force's costliest single campaign.

Euan Nisbet
London

Snooper's Charter stokes online privacy fears

This week the chief of MI6 gave a rare briefing to journalists on the threat caused by cyberattacks and defended the new Investigatory Powers Act or "Snooper's Charter".

Government and businesses face a huge challenge to overcome consumer fears around privacy being eroded by technology. Consumer trust is low and our research shows that two-thirds do not trust the Government with their personal data. Technology companies, including social media groups, are not far behind.

In addition our research confirms the huge incidence of cybercrime: almost 1 in 5 UK consumers told us they had been the victim of fraud or hacking online, which supports the ONS figures that show cybercrime is almost as common as all other crime combined in the UK.

It's clear that consumers understand sharing personal information is a necessary part of modern life, but the priority now must be to allay their anxieties about privacy, or risk alienating those who should draw the greatest benefit from all this digital innovation.

Chris McMillan, Partner, Oliver Wyman Digital
London

The majority aren't always right

The wishes of the majority are not always right. Indeed they are often terribly wrong.

In 1940 when France capitulated, it was only a united effort by Churchill and Atlee that overturned a motion in parliament to seek a settlement with Germany - by just two votes! Had this decision been put to the people of Britain then a majority (estimated at 72 per cent) would have voted for such a settlement and to leave Europe to its fascist fate.

There are times when the majority of people make terrible decisions - especially when incited by fear, hate and anger. On these occasions it is the duty of the minority to fight on for what they know to be right. To merely submit to the mass would be a dereliction of our duty to society.

I will, until my dying day, fight for the retention of unity in Europe.

The EU is an imperfect but all embracing unity that was created by great statesmen and stateswomen over sixty five years. We the (48.5 per cent) minority have a duty to fight on to retain that unity.

Martin Deighton
Woodbridge
A Conservative general election majority dangles like a bauble on the Number 10 Christmas Tree;
Please send your letters to letters@independent.co.uk

BYLINE: Letters
SECTION: VOICES
LENGTH: 830 words

After Theresa May's midweek Article 50 coup and the Conservative's win in the Sleaford and North Hykeham by-election, Labour has barely 24 months to save itself to become a credible political force again. Under Jeremy Corbyn and Diane Abbott's Marxist junta, Labour is becoming a footnote, little more than an irrelevant sideshow, not a serious contender to form the next government.

On the basis of the Sleaford result - her first real test as Prime Minister - May should not sack Boris Johnson but promote him to her general election mascot on a war footing. May has already proven herself more than capable of winning a majority at a snap general election on her own merits. With her St Bernard Boris on board, she may gamble on ascending to Alpine peaks at the next general election.

To fall out with Boris at this stage would leave him languishing on the backbenches as a stalking horse, Heseltine-style, poisoning the well, always ready to pounce and make his bid for No 10. Just as the glittering prize of a May majority dangles like a bauble on the No 10 Christmas Tree, sending Boris down would see it smashed on the pavement, with any hope of a the first Tory landslide for decades dashed for good.

May has the kugels to win big, but only with Boris unleashed, not shut up in the kennel with a muzzle.
Anthony Rodriguez
Middlesex

Gina Miller deserves praise, not abuse

In response to your article (Man arrested 'for threatening woman' who led Brexit legal challenge, 7 December), how shameful that in the UK today anyone who speaks out for what they believe in is subjected to abuse and death threats, and even more shameful that the threats are based on gender and race.

Is this what our country has become now - a place where the only views that count are those of bigoted white males? On the other hand, how wonderful that the person making a stand for democracy in our multicultural country is neither white nor male.

I am deeply grateful to Gina Miller for attempting to ensure that the terms of Brexit are properly scrutinised by our elected representatives. For most of us, this is the most momentous political event of our lifetimes, so thank goodness someone is making sure it is given the most careful possible consideration.

Lynda Newbery
Bristol

Not everyone stood aside at the Warsaw Uprising

Robert Fisk is right to remind us of the unspeakable horror of the Warsaw Rising in 1944. But not everyone stood aside. As he mentions, the Royal Air Force did try, and in particular the South African Air Force made 12-hour flights from Italy to drop supplies - weapons, food and medical equipment. Sixty-nine South Africans were killed and 25 SAAF Liberators were shot down. For every ton of supplies dropped into Warsaw, one bomber was lost. It was perhaps the South African Air Force's costliest single campaign.
Snooper's charter stokes online privacy fears

This week the chief of MI6 gave a rare briefing to journalists on the threat caused by cyberattacks and defended the new Investigatory Powers Act or "snooper's charter".

Government and businesses face a huge challenge to overcome consumer fears around privacy being eroded by technology. Consumer trust is low and our research shows that two-thirds do not trust the Government with their personal data. Technology companies, including social media groups, are not far behind.

In addition our research confirms the huge incidence of cybercrime: almost 1 in 5 UK consumers told us they had been the victim of fraud or hacking online, which supports the ONS figures that show cybercrime is almost as common as all other crime combined in the UK.

It's clear that consumers understand sharing personal information is a necessary part of modern life, but the priority now must be to allay their anxieties about privacy, or risk alienating those who should draw the greatest benefit from all this digital innovation.

Chris McMillan, partner, Oliver Wyman Digital

The majority aren't always right

The wishes of the majority are not always right. Indeed they are often terribly wrong.

In 1940 when France capitulated, it was only a united effort by Churchill and Atlee that overturned a motion in parliament to seek a settlement with Germany - by just two votes! Had this decision been put to the people of Britain, then a majority (estimated at 72 per cent) would have voted for such a settlement and to leave Europe to its fascist fate.

There are times when the majority of people make terrible decisions - especially when incited by fear, hate and anger. On these occasions it is the duty of the minority to fight on for what they know to be right. To merely submit to the mass would be a dereliction of our duty to society.

I will, until my dying day, fight for the retention of unity in Europe.

The EU is an imperfect but all embracing unity that was created by great statesmen and stateswomen over sixty five years. We the (48.5 per cent) minority have a duty to fight on to retain that unity.

Martin Deighton

Woodbridge

LOAD-DATE: December 9, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI

Copyright 2016 Independent Digital News and Media Limited
All Rights Reserved
Last week the Investigatory Powers Bill was granted Royal Assent. The new Act updates our surveillance laws and provides powers to enable our intelligence agencies and police to fight crime and terrorism. The previous tangle of laws has been swept away and a single, consistent and transparent new surveillance framework has been introduced.

As terrorists, paedophiles and other criminals move their activities on to the internet, it is vital that those who protect us from these threats can operate there as effectively as they can in the non-digital world, and that they have the right legal structure to do so.

The sort of terrorist attacks that we have seen in Paris, Brussels and Nice could just as easily happen here in Britain. In 2005 they did.

There is a daily battle by MI5, the other security agencies, the police and our allies to prevent more attacks. Andrew Parker, the Director General of MI5, has recently stated that as many as 12 attacks have been prevented here in the past three-and-a-half years. To stand a chance of succeeding in this struggle it is essential that those who work on our behalf have the tools to do the job.

Today those tools include access to bulk data sets that throw light on where a suspect has been, with whom, and the people they are in contact with - vital elements in identifying a potential attacker before they can act.

One of the reasons that the UK has been relatively successful in containing the terrorist threat in recent years is that we were ahead of the curve in investing in, and legislating for, technical capabilities to identify and keep track of suspects.

The Government has set a world-leading example of transparency and accountability. We need to maintain this edge over our enemies - they are innovative and flexible in their approach and we need to be the same. Some other European countries have not updated their laws and made these investments. They are more vulnerable as a result.

The new Act provides strong powers but they are balanced by strong new controls. Authorisations that previously required only the consent of a government minister now, through the so called "double lock" process, also require the involvement of a judge. This was recommended by one of the three independent reviews commissioned by the government before the draft Bill was published.

Meanwhile, any suggestion that the Act's powers will be used to "snoop" on the innocent activities of ordinary people is absurd.

GCHQ won't be reading your private messages - unless you are a terrorist.

From my time in MI5 I know that we had more than enough to do without wasting our time spying on ordinary members of the public. Even if we had thought that this was a good idea, the new controls mean that we would need the agreement not only of a government minister but also of a senior judge before we could proceed. Moreover, the new Act lays down clear sanctions for misuse of the powers.

The way that the Government managed the process of bringing this legislation before Parliament was exemplary. The level of scrutiny the new law has undergone is perhaps unprecedented in our recent history.
In addition to the three independent reviews undertaken before the draft Bill was published, three parliamentary committees also reviewed the legislation, and as a result the Government agreed to many amendments and improvements in both Houses of Parliament.

The Investigatory Powers Bill has its origins in Theresa May's time as Home Secretary. Credit: Jack Taylor/WPA Pool/Getty Images

Others have remarked on the role of the Prime Minister in initiating this legislation when home secretary, but mention should also be made of the work done by Sir Keir Starmer, who led for the Opposition. As a first-rate lawyer and former Director of Public Prosecutions, his contribution not only improved the Bill but also made cross-party support possible.

In the event, the passage of the legislation in such a potentially sensitive area was marked by serious and detailed debate and ran surprisingly smoothly. For those of us worried that rational argument was falling out of fashion in political discourse in this country and beyond, this can only be an encouragement.

The country can be proud of this new Act.

The Government has set a world-leading example of transparency and accountability. No other country has been as candid about the investigatory powers used by its secret agencies, nor submitted to such strong independent oversight.

In the rapidly changing world of communications, the new Act gives as much "future proofing" against technological change as we are likely to achieve. It is no surprise that several of our allies have been watching our ongoing debate with interest and close attention.

It will be interesting to see how far the approach that the UK has pioneered in this area is taken up elsewhere.

At the end of a process that started way back in 2011, Parliament has chosen to provide our police and intelligence agencies with the powers they need to keep us safe in an uncertain and changing world. It was right to do so.

Lord Evans of Weardale was Director General of the Security Service, MI5, from 2007-2013.
A porn website that has taken umbrage with the Investigatory Powers Bill is urging everyone that visits its site to sign a petition calling for the recently-passed legislation.

Visitors to xHamster from the UK are being greeted with a pop-up message that asks them if they're aware of the new "surveillance" law and calls for them to sign a petition against it.

The Investigatory Powers Bill, which critics dub the Snoopers' Charter, has been controversial among the privacy conscious. It ratifies hacking and surveillance powers for the country's security services, as well as the ability to break encryption.

It also includes a provision for the bulk data collection of Britons' browsing habits, requiring internet and communications service providers to store the metadata of websites visited for 12 months.

FAQ | Investigatory Powers Bill

The petition, which has over 170,000 signatures, describes the bill as "an absolute disgrace to both privacy and freedom and needs to stop!" It also says that as the legislation is yet to receive Royal Assent it isn't too late for it to be revoked - but the charter was in fact ratified at the end of November and will come into force in 2017. It is not the first

The Petitions Committee said it would not be scheduling another debate. And the Government responded: "The Investigatory Powers Act dramatically increases transparency around the use of investigatory powers. It protects both privacy and security and underwent unprecedented scrutiny before becoming law."

It is highly unlikely that additional signatures will have an effect on the legislation, which passed despite widespread criticism from rights organisations and major technology companies, including Apple, Google, Facebook and Microsoft.

The last three of these teamed up to submitted evidence that said the bill "could have far reaching implications - for our customers, for your own citizens and for the future of the global technology industry".

The UK has just legalized the most extreme surveillance in the history of western democracy. It goes farther than many autocracies. https://t.co/yvmv8CoHrj

- Edward Snowden (@Snowden) November 17, 2016

Meanwhile Edward Snowden, the whistleblower who revealed GCHQ's extensive surveillance powers, described it as "the most extreme surveillance in the history of western democracy".
Freedom and the right to privacy are considered bedrocks of democracy. This week they became fundamentally under threat.

The Investigatory Powers Act, known colloquially as the Snooper’s Charter, permits the police and security agencies to remotely hack into and bug civilians’ smartphones and computers, and requires telecoms and internet service providers to keep extensive records of phone calls made, websites accessed, apps used and messages sent for 12 months. This data can be accessed by authorities and other public sector bodies.

The whistleblower Edward Snowden called it "the most extreme surveillance in the history of Western democracy"; while Tim Berners-Lee, inventor of the World Wide Web, said the bulk hacking powers "risk making the internet less safe for everyone". The Snooper’s Charter is Theresa May's baby, and has been designed to intercept communications around terrorism, espionage and cyber attacks, in the aim of making the UK a safer place to live. While no one would argue against the importance of arming ourselves against these threats and helping to prevent crime and exploitation along the way, this is not the way to achieve it.

The internet has become an unavoidable, integral part of our working and personal lives. The data collected on each and every one of us will draw an incredibly detailed picture of our shopping habits, interests and hobbies, friends, sexual preferences, the exact nature of our work - ultimately, who we are. This is collected regardless of whether we are suspected of criminal activity, and effectively creates neat data logs which in turn are vulnerable to hacking by the very criminals the law intends to catch.

The Conservative MP David Davis, speaking in 2012, said the Bill stood to only catch "the innocent and the incompetent". The true criminals will be smart enough to work their way around the measures, while the incompetent would have been caught without the powers. The authorities should have the power and means to pursue those they have reason to believe are involved with terrorism and other criminal activities. But that should not extend to blanket spying on the public.
EUROPEAN cities face "unprecedented levels of threat" from terrorists, the Security Minister has declared - as he lashed out at civil liberties groups.

Home Office Minister Ben Wallace has said campaigners fighting to scrap new surveillance laws are opposing democracy and freedom.

The senior Tory delivered the broadside in an article for The Sun to mark the controversial Investigatory Powers Act getting royal assent this week.

After a year of Parliament debate, spy and police chiefs can now use the long-called for powers, dubbed by critics "the Snooper's Charter".

Mr Wallace said: "Our first priority must always remain the safety of the British public."

READ the full article at www.thesun.co.uk

The internet needs to be policed;
The Opinion Matrix COMMENT FROM HOME & ABROAD
'SNOOPER'S CHARTER'

The Times In more than 30 years as a parliamentarian, I have seen no new law so extensively scrutinised. Strict rules are laid out, and harsh penalties for breaches. Tim Berners-Lee has failed to recognise the monsters that have resulted from his creation, and our need to deal with them. (Alex Carlile) The Conversation With the passing of the Act we have taken a step into a new world of permanent surveillance that was not deemed necessary in 30 years of "The Troubles", four decades of the Cold War, or during two world wars. (Paul Lashmar)

LOAD-DATE: December 1, 2016
Snooper's charter: dissent over the royal assent

Snooper's charter: dissent over the royal assent Read more at www.thetimes.co.uk

No, Sir Tim, this act is not a 'snooper's charter' Alex Carlile

No, Sir Tim, this act is not a 'snooper's charter' Alex Carlile

No, Sir Tim, this act is not a 'snooper's charter' Alex Carlile
The Investigatory Powers Act became law this week. It allows the security services and police, and other appropriate authorities, to obtain information from internet service providers about our activities if we are suspected of terrorism or other serious crime. The great Sir Tim Berners-Lee, inventor of the internet, has railed against the act, adopting the familiar and misleading assertion that it is a snooper's charter. Yet a moment's reflection should persuade him away from his Victor Frankenstein moment, in which he seems to have lost sight of the often terrifying consequences of what he invented.

In more than 30 years as a parliamentarian, I have seen no new law so extensively scrutinised. The "triple lock" contained in the act extends the doctrine of the separation of powers, so that a cohort of senior judges is given the final say over investigatory decisions. Strict rules are laid out, and harsh penalties for breaches.

Who are these "snoopers" Sir Tim fears? Does he believe that those unsung public servants who protect us from political violence have the inclination (or the time) or are so incompetent as to ignore the law out of idle curiosity about matters unrelated to their crucial work? Recently those who are responsible for our protection have been removing terrorist websites at the rate of several thousand each week. This has the benefit of protecting impressionable and vulnerable people from committing the most serious of crimes, and their potential victims from the consequences. The provisions in the act mean that the authorities can follow and detect dangerous communications that might lead even to murder, and to the undermining of our institutions.

The inventors and developers of the internet space have facilitated on a huge scale, and intentionally, the surrender of privacy far beyond anything that went before. All of us who use it have given away our sizes and shapes, our tastes and desires, our proclivities and our opinions. There are forms of encryption and concealment previously unimagined. Much of this is beneficial to our daily lives. Sir Tim apparently applauds those benefits. Unfortunately he fails to recognise the monsters that have resulted from his creation, our need to deal with them, and the measured response of the new act.

Lord Carlile was independent reviewer of terrorism legislation from 2001-2011
Thousands of terrorist websites are being removed each week
Security services and the police will have new powers to hack phones and computers after the controversial "Snooper's Charter" became law.

Amber Rudd, the Home Secretary, hailed the Investigatory Powers Act 2016, which received royal assent yesterday, as "world-leading legislation" and said the intelligence services needed more powers to keep people safe.

But campaigners say the Act, which extends the reach of state surveillance in Britain, will provide a "beacon" for authoritarian regimes around the world to justify their own surveillance powers. A petition calling for it to be repealed has already garnered more than 130,000 signatures. Bella Sankey, policy director for Liberty, said: "It's a sad day for our democracy as this Bill, with its eye-wateringly intrusive powers and flimsy safeguards, becomes law.

"The Home Secretary is right that the Government has a duty to protect us, but these measures won't do the job. Instead they open every detail of every citizen's online life up to state eyes, drowning the authorities in data and putting innocent people's personal information at massive risk. This new law is world-leading, but only as a beacon for despots everywhere. The campaign for a surveillance law fit for the digital age continues, and must now move to the courts."

The new law aims to bring surveillance tactics used by police and spy agencies under one legal umbrella.

It requires internet and phone companies to store data on people's web use for up to a year and gives police, security services and official agencies unprecedented access.

Ministers say the Act will ensure that law enforcers and security and intelligence agencies have the powers they need in the digital age to disrupt terrorist attacks.

It includes a "double lock" regime for the most intrusive techniques, so that warrants issued by a secretary of state will require the approval of a senior judge.

A new Investigatory Powers Commissioner will also be created, while those misusing the powers could face sanctions including criminal charges.

Comment, page 27 Snooper's Charter What the Act will mean to us What is it? New legislation drawn up in an attempt to bring the powers available to police and intelligence agencies to tackle terrorism and serious crime in the digital age under one legal umbrella for the first time.

Why is it needed? The current system is seen as an unwieldy patchwork of powers covered by different laws. But there is also a logistical reason - the main existing legislation is due to expire at the end of 2016.

What powers will the Act cover? Current tactics such as access to communications data - the who, when and where, but not the content; targeted interception of communications; the collection of bulk data; and the ability to mount IT attacks.

Are there any new powers? Firms will now be required to store data relating to people's web use for up to a year, but the Government has repeatedly stressed that internet connection records (ICRs) will not cover users' full browsing history or the content of communications.

Does everyone think this is good news? No. Campaign group Liberty said it was a "sad day for our democracy", claiming the Act includes "eyewateringly intrusive powers".

LOAD-DATE: November 29, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: III

Copyright 2016 Independent Print Limited
All Rights Reserved

Return to List
Can you beat the state snoopers?;
TECHNOLOGY Encryption and proxies can still protect you, explains Rhiannon Williams

How much do you value your privacy? If you use the internet on a regular basis, defending it is about to get a whole lot harder. The Investigatory Powers Bill, known colloquially as the Snooper's Charter due to its intrusive nature, received Royal Assent to become law yesterday.

As you may have read, the law - which now becomes an Act of Parliament - means that internet providers, apps and other online services will be required to keep a 12-month history of which websites their users are visiting, and share data with authorities on demand.

It also potentially allows police and security services to hack into devices and networks, if they are given permission by the Home Secretary, allowing them to monitor use or even download data remotely.

Given that the law sanctions tracking the personal web habits of millions of innocent civilians every day, is there anything to be done to avoid it? Well actually, yes.

Personal privacy has long been a concern for many tech companies, and you may be already using numerous encrypted apps and services without realising it.

When you exchange messages within an encrypted app, for example, the text is scrambled and cannot be deciphered without an encryption key. The Facebook-owned WhatsApp and Apple's iMessage app use end-to-end encryption, meaning messages can only be read by the sender and recipient and no one else - not even Facebook or Apple.

Apple has taken on the mantle of privacy warrior in the US over the past year, through its refusal to aid the FBI by creating a "backdoor" into an iPhone belonging to the San Bernardino gunman Syed Rizwan Farook, who, with his wife, Tashfeen Malik, shot and killed 14 people last December.

Despite the nature of the crime and the demands of investigators, the company's chief executive, Tim Cook, said opening up the iPhone to the authorities would have "set a dangerous precedent". The FBI eventually found a way to access the phone's data, but it took months without Apple's help.

Although Apple's refusal riled US President-elect Donald Trump, who said while campaigning that he agreed "100 per cent with the courts", the move was praised by the tech community for defending public liberty.

Another useful method is SecureGmail, an extension for Google's Gmail service, which encrypts and decrypts emails to prevent interception.

Outside messaging, there are also ways to keep your internet browsing private. The Snooper's Charter requires internet service providers to log the websites you've visited, but not details of the pages within them. However, if you're still concerned, you can mask this through using proxy servers or virtual private networks, known as VPNs.

Proxy servers act as gateways between your computer and the internet, and can be used by companies to block inappropriate sites within the workplace. Anonymous proxy servers mask the computer making the request from the receptive server, but are not always secure.

A VPN, such as Hide My Ass or TorGuard, creates a private encrypted internet connection by masking your IP address, and is commonly used to bypass licensing restrictions - perhaps to watch the BBC iPlayer abroad - and for security while using public wi-fi connections.
Not all VPNs are secure and many are quite slow, but some offer a decent level of anonymity by not logging traffic, time spent on web pages or any other kind of information.

While the majority of search engines (particularly Google) track your searches to present you with faster, more relevant results and tailored adverts, rivals such as DuckDuckGo claim not to collect or share personal information to preserve user privacy.

Nevertheless, critics may have a point when they say that, in this day and age, the best way to avoid being tracked online entirely is simply to avoid going online at all.

Apple has taken on the mantle of privacy warrior in the US over the past year.
Snooper's charter undermines our rights, says web inventor

BYLINE: Fiona Hamilton

SECTION: NEWS; Pg. 2

LENGTH: 479 words

Wide-ranging surveillance powers that became law yesterday have no place in modern democracy and will ride roughshod over privacy, according to the inventor of the world wide web.

Sir Tim Berners-Lee described elements of the new legislation as "disproportionate" and said that the strengthening of snooping powers for police and security services undermined people's fundamental rights.

The Investigatory Powers Bill received royal assent despite a protest petition of more than 100,000 signatures. It sets out each surveillance power used by the police and security services, with extended powers in some cases.

Among the most controversial aspects is a requirement for internet companies to keep records of individual visits to websites for 12 months.

Police powers to check internet records, which involve the acknowledgment of a visit but not the nature of browsing or communications, have been extended to when it is considered "necessary and proportionate for an investigation".

The rights of the security and intelligence services to carry out bulk data collection and bulk hacking, have also been asserted. It means that they are able to hack entire areas in foreign countries to gather intelligence and sift through vast troves of data here.

Some police forces, and the National Crime Agency, will be able to carry out targeted hacking to prevent serious crime or "death or injury or damage to a person's physical or mental health", such as in missing persons cases.

Intelligence services and law enforcement agencies say that such powers are essential to gather information in a modern world to thwart terrorism and fight crime.

The Home Office hailed the legislation as containing necessary powers in a digital age, "subject to strict safeguards and world-leading oversight". However Sir Tim told the BBC; "This snooper's charter has no place in a modern democracy. It undermines our fundamental rights online."

He said that bulk hacking risked "making the internet less safe for everyone".

The government pointed to the introduction of a "double-lock" regime for the most intrusive techniques, so that warrants issued by a secretary of state will require the approval of a senior judge.

Amber Rudd, the home secretary, said: "The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight."

Main points Internet records Web and phone companies must store web page visits by the public for a year.

Hacking Security services will be able to collect data such as travel details or information.

Some police forces, and the National Crime Agency, will be able to carry out targeted hacking.

Double-lock Ministerial authorisation will need to be agreed by judicial commissioners, who are given the power of veto.

LOAD-DATE: November 30, 2016

LANGUAGE: ENGLISH
The "snooper's charter" bill extending the reach of state surveillance in Britain was given royal assent and became law on Tuesday as signatures on a petition calling for it to be repealed passed the 130,000 mark.

The home secretary, Amber Rudd, hailed the Investigatory Powers Act 2016 as "world-leading legislation" that provided "unprecedented transparency and substantial privacy protection".

But privacy campaigners warned that it would provide an international standard to authoritarian regimes around the world to justify their own intrusive surveillance powers.

The new surveillance law requires web and phone companies to store everyone's web browsing histories for 12 months and give the police, security services and official agencies unprecedented access to the data.

It also provides the security services and police with new powers to hack into computers and phones and to collect communications data in bulk. The law requires judges to sign off police requests to view journalists’ call and web records, but the measure has been described as "a death sentence for investigative journalism" in the UK.

The Home Office says some of the provisions in the act will require extensive testing and will not be in place for some time. However powers to require web and phone companies to collect customers' communications data will be in force before 31 December, the date when the current Data Retention and Investigatory Powers Act 2014 expires.

The home secretary said: "The Investigatory Powers Act is world-leading legislation, that provides unprecedented transparency and substantial privacy protection.

"The government is clear that, at a time of heightened security threat, it is essential our law enforcement and security and intelligence services have the power they need to keep people safe. The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight."

380
Jim Killock, executive director of the Open Rights Group, responded to the home secretary's "world-leading" claim, saying: "She is right, it is one of the most extreme surveillance laws ever passed in a democracy. The IP Act will have an impact that goes beyond the UK's shores. It is likely that other countries, including authoritarian regimes with poor human rights records, will use this law to justify their own intrusive surveillance powers."

He said the legislation was debated and passed while the public, media and politicians were preoccupied with Brexit: "Now that the bill has passed, there is renewed concern about the extent of the powers that will be given to the police and security agencies.

"In particular, people appear to be worried about new powers that mean our web browsing activity can be collected by internet service providers and viewed by the police and a whole range of government departments. Parliament may choose to ignore calls for a debate but this could undermine public confidence in these intrusive powers."

The European court of justice is due to clarify its rulings on state surveillance shortly, in a case brought by the deputy leader of the Labour party, Tom Watson. The court's ruling could lead to parts of the new legislation being declared unlawful and in need of amendment, including restrictions on how the personal confidential data involved can be used and accessed.
Has the age of online privacy come to an end?;
SURVEILLANCE Questions remain on how the Snooper's Charter will work, reports Jill Lawless

SECTION: NEWS; Pg. 27
LENGTH: 526 words

After months of wrangling, the contentious "snooper's charter" will be given Royal Assent this week. The Investigatory Powers Act will hand many authorities - from police and spies to food regulators, fire officials and tax inspectors - powers to look at the internet browsing records of everyone in Britain.

The law requires telecoms companies to store for one year a list of websites that each person has visited and the apps and messaging services they used - though not the individual pages they looked at or the messages they sent - creating databases of personal information that the firms worry could be vulnerable to leaks and hackers.

Civil liberties groups argue that the law establishes mass surveillance of British citizens, following innocent internet users from the office to the living room and the bedroom. Yesterday a petition asking the Government to repeal the Act topped 118,000 signatures, meaning it must be considered for debate.

Big questions remain about how the Act will work, and the Government acknowledges it could be 12 months before internet firms have to start storing the records.

The Government says it will be key to tackling terrorism, and has called the information it collects the modern equivalent of an itemised phone bill. But critics say it's more like a personal diary.

Julian Huppert, a former Liberal Democrat MP who opposed the Bill, says: "People may have been to the Depression Alliance website, or a marriage guidance website, or an abortion provider's website, or all sorts of things which are very personal and private," he says.

Officials won't need a warrant to access the data, and the list of bodies that can see it includes not just the police and intelligence services, but government departments, revenue and customs officials and even the Food Standards Agency.

Some aspects of the new law remain clouded by secrecy. Not all internet companies will have to comply - only those that are asked to by the Government. The Government won't say who is on that list, and the firms involved are forbidden from telling their customers.

Service providers are also concerned by the law's provision that firms can be asked to remove encryption to let spies access communications. Internet companies say that could weaken the security of online shopping, banking and a host of other activities that rely on encryption.

The Government says the law incorporates protections against intrusion, including an investigatory powers commissioner to oversee the system, and judges to scrutinise government-approved warrants to hack into electronic devices or look at the content of communications.

David Anderson, a lawyer who serves as Britain's independent reviewer of terrorism legislation, said the new law "creates powerful new safeguards" and provides transparency on "all the powers which police and intelligence agencies already use".
Investigatory Powers Bill officially passes into law, giving Britain the 'most extreme spying powers ever seen';
The Bill received large opposition from petitions, but not within parliament

BYLINE: Andrew Griffin

SECTION: NEWS

LENGTH: 494 words

Britain's intelligence services have officially been given the "most extreme spying powers ever seen".

The Investigatory Powers Act has now been given royal assent, meaning that those surveillance rules will pass into law. The bill was officially unveiled a year ago and passed through the House of Lords earlier this month, but the act of being signed off means that those powers now go into effect.

It adds new surveillance powers including rules that force internet providers to keep completely records of every website that all of their customers visit. Those will be available to a wide range of agencies, which includes the Department for Work and Pensions as well as the Food Standards Agency.

As well as those internet connection records, surveillance agencies will also be given new powers to force companies to help hack into phones, and to collect more information than ever before on anyone in Britain.

The Home Office hailed the new law as a "landmark Bill which sets out and governs the powers available to the police, security and intelligence agencies to gather and access electronic communications". It said in a statement that it "brings together and updates existing powers while radically overhauling how they are authorised and overseen".

Powers covered by the new regime include:

Internet connection records: Communications firms will be required to store data relating to what sites a device connects to - but not a user's full browsing history or the content of a communication - for up to a year.

Bulk powers: The tactics used by MI5, MI6 and GCHQ to collect vast troves of data.
Equipment Interference: The official phrase used for operations involving hacking into suspects' smartphones and PCs, which are seen as increasingly important as advanced encryption makes monitoring targets more difficult.

Not all of the powers available in the Bill will be rolled out straight away. Some require testing so will not be ready for some time, the Home Office said.

But others replace the Data Retention and Investigatory Powers Act 2014, also known as Dripa, which is set to expire on 31 December and so urgently needed updating with the new bill.

Home Secretary Amber Rudd said: "This Government is clear that, at a time of heightened security threat, it is essential our law enforcement, security and intelligence services have the powers they need to keep people safe.

Read more
All the people who can now see your entire internet history
"The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight.

"The Investigatory Powers Act is world-leading legislation that provides unprecedented transparency and substantial privacy protection."

The Bill has been opposed by tens of thousands of people in a petition. But that is thought to have begun too late and so is likely not to lead to any change in the law.
Britain's intelligence services have officially been given the "most extreme spying powers ever seen". The Investigatory Powers Act has now been given royal assent, meaning that those surveillance rules will pass into law. The bill was officially unveiled a year ago and passed through the House of Lords earlier this month, but the act of being signed off means that those powers now go into effect.

It adds new surveillance powers including rules that force internet providers to keep completely records of every website that all of their customers visit. Those will be available to a wide range of agencies, which includes the Department for Work and Pensions as well as the Food Standards Agency.

As well as those internet connection records, surveillance agencies will also be given new powers to force companies to help hack into phones, and to collect more information than ever before on anyone in Britain.

The Home Office hailed the new law as a "landmark Bill which sets out and governs the powers available to the police, security and intelligence agencies to gather and access electronic communications". It said in a statement that it "brings together and updates existing powers while radically overhauling how they are authorised and overseen".

Powers covered by the new regime include:

Internet connection records: Communications firms will be required to store data relating to what sites a device connects to - but not a user's full browsing history or the content of a communication - for up to a year.

Bulk powers: The tactics used by MI5, MI6 and GCHQ to collect vast troves of data.

Equipment Interference: The official phrase used for operations involving hacking into suspects’ smartphones and PCs, which are seen as increasingly important as advanced encryption makes monitoring targets more difficult.

Not all of the powers available in the Bill will be rolled out straight away. Some require testing so will not be ready for some time, the Home Office said.

But others replace the Data Retention and Investigatory Powers Act 2014, also known as Dripa, which is set to expire on 31 December and so urgently needed updating with the new bill.

Home Secretary Amber Rudd said: "This Government is clear that, at a time of heightened security threat, it is essential our law enforcement, security and intelligence services have the powers they need to keep people safe.

Read more

All the people who can now see your entire internet history

"The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight."

"The Investigatory Powers Act is world-leading legislation that provides unprecedented transparency and substantial privacy protection."
The Bill has been opposed by tens of thousands of people in a petition. But that is thought to have begun too late and so is likely not to lead to any change in the law.

Civil liberties group Liberty said that the law served as a "beacon for despots everywhere".

"It's a sad day for our democracy as this Bill - with its eye-wateringly intrusive powers and flimsy safeguards - becomes law," said Bella Sankey, the group's policy director.

"The Home Secretary is right that the Government has a duty to protect us, but these measures won't do the job. Instead they open every detail of every citizen's online life up to state eyes, drowning the authorities in data and putting innocent people's personal information at massive risk.

"This new law is world-leading - but only as a beacon for despots everywhere. The campaign for a surveillance law fit for the digital age continues, and must now move to the courts."

LOAD-DATE: November 29, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI

Britain's spies enter a new era as powers to sweep up vast troves of call, email and text data are signed into law

BYLINE: TIM SCULTHORPE, MAILONLINE DEPUTY POLITICAL EDITOR

SECTION: NEWS

LENGTH: 672 words

Investigatory Powers Bill received royal assent after a year in Parliament
While discussed in detail, the new laws faced little opposition from MPs
But outside Parliament they were bitterly contested by civil liberty groups

Britain's intelligence services entered a new era today as controversial new spying laws took effect.

The landmark Investigatory Powers Bill - described by former prime minister David Cameron as one of the most important pieces of legislation of this parliament - was officially given royal assent today.

First unveiled a year ago, the legislation aims to bring surveillance tactics used by police and spy agencies in the digital age under one legal umbrella.

Powers covered by the new regime include:

:: Internet connection records: Communications firms will be required to store data relating to what sites a device connects to - but not a user's full browsing history or the content of a communication - for up to a year.

:: Bulk powers: The tactics used by MI5, MI6 and GCHQ to collect vast troves of data.
:: Equipment Interference: The official phrase used for operations involving hacking into suspects' smartphones and PCs, which are seen as increasingly important as advanced encryption makes monitoring targets more difficult.

The Bill has attracted intense scrutiny, with a string of parliamentary reports calling for revisions while it has come under attack repeatedly from civil liberties groups.

WHAT DOES INVESTIGATORY POWERS ACT ALLOW?

Powers covered by the new regime include:

Internet connection records: Communications firms will be required to store data relating to what sites a device connects to - but not a user's full browsing history or the content of a communication - for up to a year.

Bulk powers: The tactics used by MI5, MI6 and GCHQ to collect vast troves of data.

Equipment Interference: The official phrase used for operations involving hacking into suspects' smartphones and PCs, which are seen as increasingly important as advanced encryption makes monitoring targets more difficult.

But ministers say it will ensure law enforcement and the security and intelligence agencies have the powers they need in a digital age to disrupt terrorist attacks.

The Home Office said the legislation brings together and updates existing powers while radically overhauling how they are authorised and overseen.

It includes the introduction of a ‘double lock’ regime for the most intrusive techniques, so that warrants issued by a Secretary of State will require the approval of a senior judge.

A new Investigatory Powers Commissioner will be created, while those misusing the powers could face sanctions including criminal charges.

Home Secretary Amber Rudd said: 'This Government is clear that, at a time of heightened security threat, it is essential our law enforcement, security and intelligence services have the powers they need to keep people safe.

'The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight.

'The Investigatory Powers Act is world-leading legislation that provides unprecedented transparency and substantial privacy protection.'

Some of the provisions in the Bill will require extensive testing and will not be in place for some time, the Home Office said.

In the meantime, measures required to replace the Data Retention and Investigatory Powers Act 2014 (DRIPA), which expires on December 31, will take effect.

Assistant Chief Constable Richard Berry, National Police Chiefs' Council lead for Communications Data, said: 'We are working across law enforcement and with the Home Office to make the necessary changes to our processes and to inform and train our staff ready for implementation of the Act.

'Necessity, proportionality and ethics will be at the heart of our approach to the updated powers working within a robust new oversight regime.'
Snoopers' Charter passes into law giving intelligence services controversial new spying powers;
Ministers say it will ensure law enforcement and the security and intelligence agencies have the powers they need to disrupt terrorist attacks

**BYLINE:** By Hayden Smith

**SECTION:** TECHNOLOGY

**LENGTH:** 525 words

Britain's intelligence services have entered a new era after controversial new spying laws took effect. The landmark Investigatory Powers Bill - described by former prime minister David Cameron as one of the most important pieces of legislation of this parliament - was given royal assent on Tuesday.

First unveiled a year ago, the laws aim to bring surveillance tactics used by police and spy agencies in the digital age under one legal umbrella.

Powers covered by the regime include:

- Internet connection records: Communications firms will be required to store data relating to what sites a device connects to - but not a user's full browsing history or the content of a communication - for up to a year.
- Bulk powers: The tactics used by MI5, MI6 and GCHQ to collect vast troves of data.
- Equipment Interference: The official phrase used for operations involving hacking into suspects' smartphones and PCs, which are seen as increasingly important as advanced encryption makes monitoring targets more difficult.

The Bill has attracted intense scrutiny, with a string of parliamentary reports calling for revisions while it has come under attack repeatedly from civil liberties groups.

But ministers say it will ensure law enforcement and the security and intelligence agencies have the powers they need in a digital age to disrupt terrorist attacks.

The Home Office said the legislation brings together and updates existing powers while radically overhauling how they are authorised and overseen.

It includes the introduction of a "double lock" regime for the most intrusive techniques, so that warrants issued by a Secretary of State will require the approval of a senior judge.

A new Investigatory Powers Commissioner will be created, while those misusing the powers could face sanctions including criminal charges.

Home Secretary Amber Rudd said: "This Government is clear that, at a time of heightened security threat, it is essential our law enforcement, security and intelligence services have the powers they need to keep people safe.

"The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight.

"The Investigatory Powers Act is world-leading legislation that provides unprecedented transparency and substantial privacy protection."

[388]
Some of the provisions in the Bill will require extensive testing and will not be in place for some time, the Home Office said.

In the meantime, measures required to replace the Data Retention and Investigatory Powers Act 2014 (DRIPA), which expires on December 31, will take effect.

Bella Sankey, policy director for campaign group Liberty, said: "It's a sad day for our democracy as this Bill - with its eye-wateringly intrusive powers and flimsy safeguards - becomes law.

"The Home Secretary is right that the Government has a duty to protect us, but these measures won't do the job.

"Instead they open every detail of every citizen's online life up to state eyes, drowning the authorities in data and putting innocent people's personal information at massive risk."

Snoopers' Charter passes into law giving British intelligence services sweeping internet surveillance powers; Ministers say it will ensure law enforcement and the security and intelligence agencies have the powers they need to disrupt terrorist attacks

BYLINE: By Hayden Smith

SECTION: TECHNOLOGY

LENGTH: 573 words

Britain's intelligence services have entered a new era after controversial new spying laws took effect.

The landmark Investigatory Powers Bill - described by former prime minister David Cameron as one of the most important pieces of legislation of this parliament - was given royal assent on Tuesday.

First unveiled a year ago, the laws aim to bring surveillance tactics used by police and spy agencies in the digital age under one legal umbrella.

Powers covered by the regime include:

Internet connection records: Communications firms will be required to store data relating to what sites a device connects to - but not a user's full browsing history or the content of a communication - for up to a year.

Bulk powers: The tactics used by MI5, MI6 and GCHQ to collect vast troves of data.
Equipment Interference: The official phrase used for operations involving hacking into suspects’ smartphones and PCs, which are seen as increasingly important as advanced encryption makes monitoring targets more difficult.

The Bill has attracted intense scrutiny, with a string of parliamentary reports calling for revisions while it has come under attack repeatedly from civil liberties groups.

These are the 48 organisations that can see EVERYTHING you do online - even if you delete it

But ministers say it will ensure law enforcement and the security and intelligence agencies have the powers they need in a digital age to disrupt terrorist attacks.

The Home Office said the legislation brings together and updates existing powers while radically overhauling how they are authorised and overseen.

It includes the introduction of a "double lock" regime for the most intrusive techniques, so that warrants issued by a Secretary of State will require the approval of a senior judge.

A new Investigatory Powers Commissioner will be created, while those misusing the powers could face sanctions including criminal charges.

Home Secretary Amber Rudd said: "This Government is clear that, at a time of heightened security threat, it is essential our law enforcement, security and intelligence services have the powers they need to keep people safe.

"The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge. But it is also right that these powers are subject to strict safeguards and rigorous oversight.

Theresa May's Snooper's Charter could cost taxpayers £1 billion just to get started

"The Investigatory Powers Act is world-leading legislation that provides unprecedented transparency and substantial privacy protection."

Some of the provisions in the Bill will require extensive testing and will not be in place for some time, the Home Office said.

In the meantime, measures required to replace the Data Retention and Investigatory Powers Act 2014 (DRIPA), which expires on December 31, will take effect.

Bella Sankey, policy director for campaign group Liberty, said: "It's a sad day for our democracy as this Bill - with its eye-wateringly intrusive powers and flimsy safeguards - becomes law.

Labour peer Shami Chakrabarti is dubbed a 'sell-out' as it's claimed she won't vote against 'Snooper's Charter'

"The Home Secretary is right that the Government has a duty to protect us, but these measures won't do the job.

"Instead they open every detail of every citizen's online life up to state eyes, drowning the authorities in data and putting innocent people's personal information at massive risk."

LOAD-DATE: November 29, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDMI

Copyright 2016 Trinity Mirror, Plc. All Rights Reserved

Return to List

71 of 100 DOCUMENTS
What is the Investigatory Powers Bill and what does it mean for my privacy?

BYLINE: By Cara McGoogan

SECTION: TECHNOLOGY

LENGTH: 813 words

The Queen has given Royal Assent to the controversial Investigatory Powers Bill, which ratifies the snooping powers of the UK’s intelligence agencies.

Introduced by Theresa May when she was home secretary, the bill legitimises the security services’ surveillance powers while adding checks on their ability to gather information about citizens without a warrant. It introduces the need for a judge’s sign-off on “the most intrusive powers”, as well as a new Investigatory Powers Commissioner to monitor how they’re used.

The bill, which passed in the House of Lords last week, will come into force at the beginning of 2017.

"At a time of heightened security threat, it is essential our law enforcement, security and intelligence services have the powers they need to keep people safe," said Home Secretary Amber Rudd. "The internet presents new opportunities for terrorists and we must ensure we have the capabilities to confront this challenge.

"But it is also right that these powers are subject to strict safeguards and rigorous oversight."

FAQ | Investigatory Powers Bill

However, critics of the legislation have dubbed it the “Snoopers’ Charter” and technology experts and civil rights advocates have slammed it for being invasive. The IP Bill extends the powers of GCHQ, MI6, MI5 and the police to hack into people’s computers with a warrant. It also dictates that internet and communications service providers must store top-level information about British citizens’ browsing for 12 months after the fact.

Before it received the royal sign-off a petition calling for the powers to be repealed had already gained more than 100,000 signatures.

The UK has just legalized the most extreme surveillance in the history of western democracy. It goes farther than many autocracies. https://t.co/yvmv8CoHrj

- Edward Snowden (@Snowden) November 17, 2016

What does it mean for my privacy?

Technology giants including Google, Facebook and Microsoft teamed up to attack the bill earlier this year, claiming that weakening encryption and requiring companies to store more information about customers "could have far reaching implications - for our customers, for your own citizens and for the future of the global technology industry".

One of the clauses they were referring to is the requirement that ISPs and CSPs save the internet and communications history of everyone in the UK for a year after the fact so that it can be called upon in any investigations. This refers to the meta data of web browsing and communications, rather than the content. So it would be what site you went to and who you messaged, but not what you did or said.

Some 48 authorities will be able to request access to this information, including the Met Police, British Transport Police, GCHQ, the MoD, the Department of Health, HM Revenue and Customs, and the Home Office.

Such information can help build an accurate picture of who a person is and, critics say, is an invasion of privacy. There is little that you can do to prevent the information from being collected, although some rights activists have suggested that privacy-conscious citizens could use a VPN or identity-masking browser such as Tor.
Theresa May introduced the IP Bill into Parliament when she was still Home Secretary Credit: Julian Simmonds

The provisions of the bill also give the security services the power to hack into computers, mobile devices and networks without alerting the owners. It is the first time that such powers have been available to law enforcement.

Described in the bill as "equipment interference", this clause gives police and intelligence officials the ability to use tricks more commonly associated with cyber criminals such as installing malicious software onto a device that lets them download information stored on it.

The petition warned that, "With this bill they will be able to hack, read and store any information from any citizen's computer or phone without even the requirement of proof that the citizen is up to no good.

"This essentially entitles them to free reign of your files, whether you're a law abiding citizen or not."

There is little that can be done to protect your information from such techniques. You can go some way to bolstering your privacy by using encrypted messaging services and saving information to an external hard drive or cloud before deleting it.

But the bill's writers maintain that only those suspected of being a security risk will be monitored in this way. The Home Office has also said that nothing is going to change immediately, and that some elements of the bill will require "extensive testing" at first.

LOAD-DATE: November 29, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBDTNS

Snooping bill rebounds

SECTION: NEWS; Pg. 10

LENGTH: 60 words

A petition calling for the scrapping of the Investigatory Powers Bill, branded a snooper's charter, has gathered almost 130,000 signatures and must be considered for parliamentary debate. The bill, passed by the Commons and Lords, requires internet companies to keep a 12-month record of the websites customers view and gives security services new hacking powers.

LOAD-DATE: November 29, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper
We let technology into our lives. And now it's starting to control us; Internet giants are accessing vast amounts of personal data and using it to shape our behaviour. It's reminiscent of East Germany under the Stasi

BYLINE: Rachel Holmes

SECTION: OPINION

LENGTH: 1418 words

In 1998, I joined the UK launch team for an e-commerce startup named after the world's largest river. The smart idea was to harness the unprecedented cataloguing capacity of the emerging internet to sell books - a product with a long shelf-life - online. In those days, now regarded as the classical era in tech history, the boundary between the product consumed and the medium used to deliver it was clear.

Increasingly, the boundary between product and platform is dissolving before our eyes. First, we offered the freedom of the biggest selection of books in the world. Then we said: "If you liked that, you will like this." We were following you into the bookshop, recording your purchasing history and suggesting your future. It started with books, but it was always intended to be everything, in the end.

Two years later, in 2000, Harvard Law School professor Lawrence Lessig predicted that the internet would become an apparatus that tracks our every move, erasing important aspects of privacy and free speech in our social and political lives. "Left to itself," he said, "cyberspace will become a perfect tool of control." A sceptical reviewer scoffed: "Lessig doesn't offer much proof that a Soviet-style loss of privacy and freedom is on its way."

Sixteen years later, it's clear that the digital world born in freedom has evolved into a creature of control. Post-Snowden, we know the scale of NSA and GCHQ surveillance. We know we're being watched. But equally, we might consider that the employee who decides what does and doesn't go on Facebook for its 1.79 billion active users is the most powerful censor in the world. Do you know her name?

Related: The pedlars of fake news are corroding democracy | Andrew Smith

We also know that corporate internet giants gather data to maximise profits from our consumer habits, from grocery shopping to TV viewing patterns. Just like trawlers with dragnets, all sorts of other collateral data gets hauled in along the way. Data surveillance, once intangible and invisible, now blatantly announces its presence in our everyday lives. Mobile accessories and the interconnectivity between gadgets and appliances in our homes - the internet of things - create an unprecedented network of tracking devices capturing data for commerce and government.

The technology we thought we were using to make life more efficient started using us some time ago. It is now attempting to reshape our social behaviour into patterns reminiscent of the total surveillance
culture of the medieval village, East Germany under the Stasi, or the white supremacist state of South Africa in which I grew up.

In an increasingly online everyday life, our use of social media has become a medium for normalising the acceptability of intrusion and behavioural correction. We are bombarded by “helpful recommendations” on education, health, relationships, taxes and leisure matched to our tracked user profiles that nudge us towards products and services to make us better citizen consumers. The app told you that you only took 100 steps today. The ad for the running shoes will arrive tomorrow.

We risk allowing ourselves to become a vast network of informants on each other and ourselves. Think about GPS-based location tracking on your mobile phone; think about social media apps where we broadcast our spontaneous thoughts, social lives and relationships.

Related: Facebook isn't looking out for your privacy. It wants your data for itself

As individuals we behave on a spectrum of complicity with the demise of our privacy. We know Twitter is broadcasting. We're generally naive about the limits to our visibility and history on Facebook. We're in self-denial where there ought to be a reasonable expectation of privacy, as with texts, emails and online shopping. In truth we already know nothing's private because the corporates and government can get it anyway. And the icing on the cake is that we are paying for our surveillance out of our own hard-pressed pockets.

Whether the internet is a "public good" is a question that has so far focused primarily on anxiety about government intervention into our digital lives. We are rightly concerned that Donald Trump will soon get his hands on the NSA, and that Britain's snooper's charter legitimises rather than limits the vast intrusions exposed by Snowden. But just as the internet knows no international borders, neither does it recognise outdated distinctions between state and corporate power, citizens and consumers and platforms and products.

The fact that billions of us now use a handful of corporate-owned global platforms to manage pretty much every aspect of our daily lives indicates how fast the potential of digital culture is shrinking. A tectonic rift exists between the corporate apparatuses of Google, Facebook, WhatsApp (now owned by Facebook), Twitter, Apple and Amazon, and the open source and creative commons ideals of the "internet of public good”.

Our concern about government snooping sometimes distracts from self-awareness of our complicity as consumers of products so ubiquitous they have become everyday verbs.

So, I'm going to act. Of course there are all sorts of measures we can take to improve our internet security. Using encryption and password managers, securing our sources. We can even put our mobile phone in a heavy copper purse and drag it round with us. But while there are tools we can use to avoid surveillance and hackers, as a consumer I'm trying to avoid or limit using services offered by corporates who don't pay their taxes; are idolisers of borderless free trade but arch-enemies of the international labour movement; are destroying privacy and creating an architecture of commercial surveillance of every aspect of our existence.

Related: 2007, not 2016, is the year the world turned upside down | John Naughton

The so-called hippy libertarians in Silicon Valley are more like unelected tyrants. They demand free speech and low tax to suit them but impose de facto censorship, surveillance and behavioural correction on us. No privacy for us and barely any scrutiny of them. The barons who own the digital kingdom that most of us inhabit declare themselves libertarians but not when our liberties are at stake.

None of the internet giants has unionised employees. Trade unionists are derided by Silicon Valley as modern-day luddites. But the recent landmark UK court ruling that Uber drivers are not self-employed demonstrates that the gig economy does not, in the words of TUC general secretary Frances O'Grady, have to be a rigged economy. "Our role isn't to try to stop this progress, it's to make sure that technology is used to make working people's lives better, and to make sure the gains from new technology are fairly shared."

I'm also worried about how we use social media. The so-called neutral platforms facilitate hate against women, racism and homophobia, and they may have put Trump in the White House as well. It may not be the platform itself, but the way in which it favours those outside the conventional media establishment and its notions of balance. Analytics expert Lteeq Khan suggests a behavioural change in our social media habits: "As social media consumers, we should resist limiting ourselves to an echo chamber of like-minded voices."
Crooked Hillary should not be allowed to run for president. She deleted 33,000 e-mails AFTER getting a subpoena from U.S. Congress. RIGGED!- Donald J. Trump (@realDonaldTrump) November 1, 2016

Trump dominated rivals on social media. He tweeted, Facebookened and Instagrammed directly to followers, apparently personally and spontaneously. It wasn’t necessarily the content that people identified with, but the carefully crafted lack of spin. This modern-day Big Brother mastered Twitter by propagating a sense of immediacy, blatant expression and human risk, rather than balance and caution. What Trump tweeted at 3am, the mainstream media reported the next day.

So this is the action I’m taking. I have stopped using Google as my search engine and deactivated my Facebook account. WhatsApp followed when it announced in August that it had abandoned its principled pro-privacy stance and would share data with its new parent and others in the "Facebook family of companies". I'm putting on my tin hat, dusting off my open-source kitbag, and heading off to the dark woods to join the resistance. Like Patrick McGoohan playing Number 6 in The Prisoner, I expect it's going to take many failed attempts to try to escape the Village.

Index on Censorship: journalists now under 'unprecedented' attack;
Study finds growing hostility toward media around the world has lead to rise in assaults on individuals as well as press freedom

BYLINE: Jane Martinson

SECTION: MEDIA

LENGTH: 872 words

Journalists are facing an "unprecedented" wave of attacks around the world with increased hostility to the media leading to assaults on individuals as well as press freedom, according to a new report.

A series of crackdowns on media workers and news outlets in Europe as well as elsewhere has confirmed 2016 as one of the most dangerous times to be a journalist, according to the latest figures compiled by Index on Censorship.

Related: 13 countries where journalists have been killed with impunity

The study found 406 verified reports of violence, threats or violations throughout European Union member states and neighbouring countries including Russia, Turkey and Ukraine in the three months to the end of September.
Melody Patry, senior advocacy officer at Index, said the year so far had been striking for the increase in reports as well as range of attacks, from threats to media freedom to attacks leading to death. "The attacks are unprecedented in both scope and scale."

With a marked increase in attacks in Europe, long considered a bastion of press freedom, the latest research does not reflect increased violence in Asia or the US, which has seen an increase in assaults and abuse during a highly charged US election during which reporters were put in pens by President-elect Donald Trump.

"Hostility to the media is increasing globally," said Patry. "When the credibility and legitimacy of media outlets starts to be questioned it can easily spread and the sentiment easily becomes one of distrust."

As well as four murders, the Index report verified 54 incidents of physical assault, 107 arrests, 150 detentions and 112 reports of intimidation, which includes psychological abuse, sexual harassment, trolling or cyberbullying and defamation. The work of journalists was censored or altered 29 times and media professionals were blocked from covering a story in 89 cases.

Those campaigning to protect journalists suggest that the most extreme forms of violence have proliferated because of a feeling of impunity. Dunja Mijatovic, an expert on media law and regulation and representative for the Organisation for Security and Co-operation in Europe, said: "With nine out of every 10 murders of journalists never solved, the vicious cycle of impunity still prevails. It has to be broken."

Related: 'We became the news': staff at Turkey's Cumhuriyet speak out over arrests

Two journalists were killed in Ukraine: Pavel Sheremet, a journalist working for the online investigative newspaper Ukrayinska Pravda, was killed in a car explosion, and Alexander Shchetinin, founder of news agency Novy Region, was shot in the head in his apartment in Kiev. In Russia, Andrey Nazarenko, a cameraman for state TV channel Russia-1, was found dead in his apartment in Moscow with two bullet wounds.

In Turkey, soldiers shot and killed Mustafa Cambaz, a photographer, during the coup attempt on Turkey's democratically elected government in July. Following the failed coup, Turkish authorities forced more than 2,500 journalists out of their jobs, arrested and prosecuted 98 under trumped-up criminal charges, detained 133 and seized or shut down 133 media outlets, according to Index.

The report's 19% rise in the number of verified incidents in the third quarter compared with the previous three months is likely to represent an underreporting of the extent of the problem. Several attacks were reported under one case and there was also underreporting in some of the worst countries.

Patry said journalists in countries known as beacons of press freedom, such as the UK and France, feel "guilty" reporting threats. "There's a real sense that it's part of the job, that they should accept it and anyway it's not as bad as it is in Azerbaijan."

Among anti-press freedom laws introduced recently are the Investigatory Powers Act in the UK, or so-called snooper's charter, which legalises a whole range of tools for snooping and hacking by the security services and allows the authorities to in effective identify journalists' anonymous sources.

In France, the National Assembly passed an amendment where journalists would be subject to up to seven years' imprisonment for protecting sources.

Related: 'The world can be better': a tribute to journalist Pavel Sheremet

Just over a week after his election a group of 18 major journalism associations published an open letter to Trump, asking that the new administration take steps to protect freedom of the press in the United States. Index now wants to extend its mapping exercise to the US.

Recent attacks range from the death of David Gilkey, a photojournalist with National Public Radio, alongside his Afghan translator, Zabihullah Tamanna, in an ambush in Afghanistan in June, to the attack on Kyle Ludowitz, a photojournalist who was left with a fractured cheekbone after being attacked at an anti- Trump protest in California.

The Mapping Media Freedom project - run by the European Federation of Journalists and Reporters Without Borders and part funded by the European commission - has recorded over 2,400 incidents threatening media freedom from its launch in May 2014. Launched amid concern over rising attacks on the media, Patry said this year has proved that it is "needed more than ever".

LOAD-DATE: November 28, 2016
The rise of fake news must not lead to an increase in snooping and censorship

BYLINE: Media IAN BURRELL on Monday

SECTION: NEWS; Pg. 41

LENGTH: 791 words

What a tragedy it is, in this golden age of communication, that so many choose to exercise their freedom of speech by lying, trolling, spewing hate speech and through the cynical design of websites designed to carry fabricated news stories.

In the final days of the US presidential election there was a surge in activity on these sites; their false content - including claims that Hillary Clinton sold guns to the Islamic State and that the Pope endorsed Donald Trump - outranked the biggest election stories from mainstream news outlets in terms of activity on Facebook.

But while Facebook and Google must ensure that their algorithms no longer legitimise such sites as genuine news sources, we cannot ban them entirely. Because the line between false propaganda and political satire is a subjective one. And an alarming by-product of the information glut of the current era has been the growing demand for censorship.

In the charged political environment we inhabit, the symbolic setting alight of a copy of a novel might not sound as horrific as it first appeared when a fatwa against the writer Salman Rushdie prompted book-burning on the streets of Bradford. But given that this sorry act dates back nearly 28 years, to a time when the world was so much less connected - two months before Tim Berners-Lee devised the World Wide Web - it has proved remarkably prescient as an indicator of the complexities of modern discourse.

The Satanic Verses affair forced Rushdie into hiding for nine years. The episode flagged up anger in sections of the Muslim community over the treatment of Islam in the West and hinted at the 21st-century radicalisation of a minority of Muslim youth. Just as importantly, this milder precursor of the Charlie Hebdo atrocity in January 2015, gave an insight into what would be a growing demand for clampdowns on publications deemed to have caused offence.

Now we have the internet, and the threats to freedom of speech are unrelenting, coming from the left of the political spectrum as well as from conservative and religious quarters. Against all logic, in an era when two billion smartphones are in circulation globally, there is a growing tendency - shared by authoritarian governments and pressure groups alike - to respond to criticism with demands to shut down the conversation.
This year's extraordinary polls in Britain and America have generated an increase in the language of division. Some on the left have responded by demanding greater censorship, including bans on mainstream media outlets that backed their political opponents. Students at London's City University, which houses one of British academia's best regarded journalism departments, voted to ban campus distribution of the Daily Mail, Daily Express and The Sun, under a motion which claimed to be "opposing fascism and social divisiveness in UK media".

According to Jo Glanville, director of the freedom of expression campaign group English PEN: "There is a line that starts with Rushdie that it's so important to not cause offence to certain groups that it is worth sacrificing the protection of freedom of expression in order not to cause offence. That response has become stronger and stronger over a long period of time."

English PEN last week announced it would be staging You Can't Say That a comedy-based fundraiser in February, at which Stewart Lee, Jack Dee, Shappi Khorsandi and others will attempt to use humour to raise public awareness of the new threats to public expression, a subject that Glanville believes is not taken sufficiently seriously.

She points to the new Investigatory Powers Act (aka the Snooper's Charter) as "the most draconian bill of any democracy in this area. Journalists are under threat, she says, from being unable to guarantee protection of their sources unless they use extreme measures to cover their digital tracks. The right to privacy is also endangered by a law which ensures that the browsing history of UK internet-users will be accessible by Government departments for 12 months, Glanville says. "For any of us to be free we have got to have space to lead private lives."

And as social media posts replace conversation, the public finds itself sued under libel law. We are all treated as publishers now. For all its wonders, the internet is still in its infancy. It can make our lives easier but it can make them more difficult, too.

For Glanville, it's the price we now pay for protecting freedom of speech. "We have got to be technically savvy if we want to protect our privacy; we have got to be legally savvy to know when we are going to get into trouble [on social media]; and we have got to be savvy in assessing which news is reliable. It's just a much more complicated world."

Twitter: @iburrell

LOAD-DATE: November 27, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: III

Copyright 2016 Independent Print Limited
All Rights Reserved

Return to List

76 of 100 DOCUMENTS

telegraph.co.uk

November 28, 2016 Monday 9:32 AM GMT

Petition to repeal new surveillance powers reaches 100,000 signatures

BYLINE: By James Titcomb

SECTION: TECHNOLOGY

LENGTH: 518 words
A petition demanding that the UK’s new sweeping surveillance powers are repealed has garnered more than 100,000 signatures, the level at which Parliament can debate it.

Theresa May’s controversial Investigatory Powers Bill, which have been described as the most extreme snooping laws in a Western democracy, were approved by the House of Lords earlier this month and are set to pass into law in the coming weeks.

They require internet providers to store customers’ web histories for 12 months and make those records available to police, and write computer hacking by spy agencies into law.

The UK has just legalized the most extreme surveillance in the history of western democracy. It goes farther than many autocracies. https://t.co/yvmv8CoHrj

- Edward Snowden (@Snowden) November 17, 2016

The bill also requires companies to break encryption in certain circumstances, although groups such as Apple, Facebook and Google have argued that the parameters for this are hazy.

The petition warns that “With this bill, they will be able to hack, read and store any information from any citizen’s computer or phone, without even the requirement of proof that the citizen is up to no good.

“ This essentially entitles them to free reign of your files, whether you’re a law-abiding citizen or not!”

FAQ | Investigatory Powers Bill

On Monday morning the petition had received more than 118,000 signatures. At the 100,000 mark means a petition can be considered for debate in the House of Commons, although there is no obligation for Parliament to do so, and several petitions that have hit the level have not been debated.

Others include a demand for a second EU referendum, with over 4 million signatures, and one saying Donald Trump should be blocked from entering the UK, with over 500,000.

Opponents of the Investigatory Powers Bill believe that it has barely been scrutinised due to the fallout from June’s EU referendum.

It has been criticised on privacy grounds, with bulk data collection even of those not suspected of wrongdoing. Internet providers will not collect the individual web pages browsers visit, just the main domain (such as telegraph.co.uk), but this is still seen as an invasion of privacy.

Security experts have also raised fears that companies’ databases of browsing histories would be a boon for hackers.

The petition’s supporters have included Kim Dotcom, the flamboyant founder of Megaupload, and the Open Rights Group.

The bill also faces legal challenges from anti-surveillance groups.
Investigatory Powers Bill was passed by the House of Lords last week. Internet providers must keep data for a year and police can hack phones. An attempted amendment to the law from the Lords was rejected by MPs. Now a blogger has created a list of all the people who will be able to request to view your internet history.

The police, NHS and the tax man will now be able to hack into your phones and check your browsing history after the Snoopers’ Charter was passed by Parliament last week. The bill, officially called the Investigatory Powers Bill, forces electronic data to be stored by internet providers for 12 months, which can be subsequently collected by law enforcement. Now a blogger has created a list of all the people who will be able to request to view your internet history if the bill passes Royal Assent to become law.

Scroll down for video

THE SNOOPERS’ CHARTER

The bill, officially called the Investigatory Powers Bill, forces electronic data to be stored by internet providers for 12 months, which can be subsequently collected by law enforcement.

The act replaces the previous Regulation of Investigatory Powers Act. It was passed by the House of Lords last week after they backed down on an amendment. The amendment would have forced the press to pay court costs for both parties in any case involving allegations of phone or email hacking, even if they were completely spurious. The new law introduces new surveillance and hacking powers.

Chris Yui, who works in Edinburgh as a general manager at Uber, wrote in his personal blog: ‘I always wondered what it would feel like to be suffocated by the sort of state intrusion that citizens are subjected to in places like China, Russia and Iran.

‘I guess we’re all about to find out.’

He listed the 48 departments that will now have access to information such as internet browsing history, set out in Schedule 4 of the Act. These include police, GCHQ, government departments such as the Home Office, MoD, Department of Health, the Food Standards Agency, HM Revenue & Customs and the Gambling Commission. This part of the act also sets out the minimum office or rank each person within those organisations must be if they want access to the records.

In the police, viewers must be an inspector or a superintendent, for instance. The access also works regardless of whether or not you clear your history, because it will be held by your internet service provider.
Internet provider must keep logs for a year and hand them over to the government on request, whether users want them to or not.

The lists will include every website that has been visited, but not specific pages on those websites.

While critics have cited it as an attack on privacy, the Government believes the charter is essential for combating terrorism and organised crime.

The act replaces the previous Regulation of Investigatory Powers Act.

It was passed by the House of Lords last week after they backed down on an amendment.

The amendment would have forced the press to pay court costs for both parties in any case involving allegations of phone or email hacking, even if they were completely spurious.

One peer said it would have 'chilled' journalism and stopped papers writing about figures such as ex-BHS boss Sir Philip Green.

Lord Myners said the amendment to implement section 40 of the Crime and Courts Acts 2013 would have made it easier for the rich to sue on spurious grounds.

WHO CAN VIEW YOUR INTERNET HISTORY?

Metropolitan police force
City of London police force
Police forces maintained under section 2 of the Police Act 1996
Police Service of Scotland
Police Service of Northern Ireland
British Transport Police
Ministry of Defence Police
Royal Navy Police
Royal Military Police
Royal Air Force Police
Security Service
Secret Intelligence Service
GCHQ
Ministry of Defence
Department of Health
Home Office
Ministry of Justice
National Crime Agency
HM Revenue & Customs
Department for Transport
Department for Work and Pensions
NHS trusts and foundation trusts in England that provide ambulance services
Common Services Agency for the Scottish Health Service
Competition and Markets Authority
Criminal Cases Review Commission
Department for Communities in Northern Ireland
Department for the Economy in Northern Ireland
Department of Justice in Northern Ireland
Financial Conduct Authority
These are the 48 organisations that can see EVERYTHING you do online - even if you delete it;
Since the passing of the Snooper's Charter a whole host of organisations can now freely spy on your internet activity

BYLINE: By Jeff Parsons

SECTION: TECHNOLOGY
Both the Houses of Parliament have passed the Investigatory Powers Bill (IPB). Once the Queen gives Royal Assent, the Snooper's Charter will become law.

That gives the government unprecedented powers to snoop, spy and hack its way into your online private life.

Internet Service Providers (ISPs) like BT, Sky, Virgin or TalkTalk will be required by law to keep a record of your internet history for a year. It will be stored in a database available to the police or government whenever they need it.

This is just one aspect of a bill that also covers which apps you use on your phone and any messages you send on any service. The reasoning behind it is that it will help the government find terrorists.

The IPB represents the most intrusive digital surveillance of any democracy on the planet, and has been attacked for over a year by privacy campaigners.

Theresa May's Snooper's Charter could cost taxpayers £1 billion just to get started

In response to the Snooper's Charter passing through parliament, a general manager of Uber wrote a blog post outlining exactly which organisations will be able to see your data.

"I always wondered what it would feel like to be suffocated by the sort of state intrusion that citizens are subjected to in places like China, Russia and Iran," said Chris Yui, who works in Edinburgh.

"I guess we're all about to find out."

As Yui points out, the list of who has access to your records is laid out in Schedule 4 of the Act.

"It's longer than you might imagine," he wrote.

Here's the full list:

One of the main concerns experts have about the Investigatory Powers Bill is how the data is going to be protected.

Having that much information in one place is likely to create a huge target for cybercriminals.

Anyone able to break into your ISP's records or any of the above government departments could well get access to a huge amount of information about you.

The best means of protecting yourself is by setting up a virtual private network (VPN). This bounces your IP address around the world through a network of servers.

All your Internet Service Provider would be able to turn over is the fact that you were using a VPN - rather than a list of the websites you visited.

"The Snooper's Charter is bewildering in its current form and would allow the government to pry into our lives via technology that has seriously sinister abilities," Danvers Baillieu, the chief operating officer of VPN service Hide My Ass, told the Mirror.

"The fact remains that the Snooper's Charter has little regard for our privacy, and is therefore unsurprisingly difficult to distinguish from dystopian fiction.

"We firmly believe that everyone is entitled to a private digital life - free from unnecessary intrusions. As a result, we're seeing growing numbers of everyday web users using Virtual Private Networks to protect their personal data from prying eyes."
How can I protect myself from government snoopers?; Now that the Investigatory Powers Act 2016 - or snooper's charter - has become law, Charles wants to protect his privacy

BYLINE: Jack Schofield

SECTION: TECHNOLOGY

LENGTH: 1329 words

Now that the snooper's charter has been passed, how can I protect myself? Should I use a VPN? Charles

The UK has just passed the Investigatory Powers Act 2016, at the third attempt, and it will become law by the end of the year. The bill was instigated by the then home secretary, Theresa May, in 2012. It is better known as the snooper's charter.

Jim Killock, the director of Open Rights Group, described it as the "most extreme surveillance law ever passed in a democracy". It more or less removes your right to online privacy.

Related: The snooper's charter: one misspelled Google search for 'bong-making' and you'll be in an orange jumpsuit | Frankie Boyle

The law forces internet service providers to keep a record of all the websites - not the actual pages - you visit for up to a year. It also obliges companies to decrypt data on demand and gives government security services the power to hack your computers, tablets, mobile phones and other devices.

To some extent, the new law merely legalises the current "custom and practice" as revealed by Edward Snowden. The most obvious difference is that it makes your web history readily available to almost 50 assorted police forces and government departments. These include the British Transport Police, the Department of Health, the Food Standards Agency, the Gambling Commission, and the Welsh Ambulance Services NHS Trust.

Web tracking and proxies

When you sign up with an ISP, the traffic from your PCs and other devices goes to your ISP's servers, which feed most of it - except various blocked websites - on to the internet. You can track this process yourself using TraceRoute.

Your ISP therefore knows where you are going online. You can avoid this by using one or more anonymous proxy servers between your PC and your eventual destination. Your ISP will then know you visited the proxy server, but, if the anonymising is done properly, it won't know where you went from there.

Most people aren't interested in proxy servers, but often end up using them. For example, British people travelling or living aboard use UK-based proxy servers to watch TV programmes on BBC iPlayer, while people outside the US use American proxies to access Netflix and other services.

Enter the VPN

There are two big problems with using free proxies. First, you may not know who's running them. They could be helpful hackers or criminals, or even CIA honeypots. Second, they may be unreliable and slow. It's better to use a virtual private network or VPN.

Multinational corporations have long used VPNs as a way of extending their private networks across the public internet. If they encrypt all the traffic between computers in their British, American and other
offices, they can send their traffic securely over the internet without paying for expensive leased lines. VPN service providers offer the same facilities to ordinary users for a small monthly fee.

The traffic from your PC is automatically encrypted and sent to the VPN supplier's server, so your ISP can't see the final destination. The ISP's records should only contain the VPN company's server addresses.

Not many people use VPNs. However, I recommend them to people who travel a lot or work from public Wi-Fi hotspots, because they protect your traffic from snoopers who steal passwords - or worse. I also recommend them to people who are potential targets for other reasons. They might be diplomats, film stars, bankers or anyone with commercially sensitive data.

Choosing a VPN

Dozens of companies sell VPN services, and you can find plenty of reviews to help you choose. The things to look for include the number of servers and where they are located, their privacy policies, the applications they support (Tor, BitTorrent etc), speed and price. Some have applications for different devices. For example, NordVPN has them for Windows, MacOS, iPhone, iPad and Android.

If your motivation includes the snooper's charter, choose a VPN that is not UK-based, and that does not keep any logs. If they don't keep any logs, they can't hand them over to government raiders. TorrentFreak keeps an updated list of "which VPN services take your anonymity seriously": The Best Anonymous VPN Services of 2016.

For increased privacy, some VPN providers accept payments by dozens of different methods including Bitcoin and anonymous gift cards.

However, note that a VPN can't guarantee access to any particular website. For example, Netflix has taken to blocking most VPN services (where hundreds of users are coming from one IP address), though some are making technical efforts to maintain access. You may also have problems with Google's geolocation, PayPal's fraud detection software, and so on.

Also, remember that a VPN doesn't protect you from phishing emails, keyloggers, and websites that try to install "drive by" malware.

Web tracking

A VPN stops your ISP from logging your web visits, but they may still be logged. For starters, your own web browser is keeping a history. You're also being tracked by dozens of advertising services, including Google's. You can block trackers with a browser extension such as Ghostery or the EFF's Privacy Badger, but note that Privacy Badger only blocks trackers from third-party sites.

GRC has a "forensics" page, which checks whether you are being tracked by cookies.

For increased privacy, you could access the internet from a "virtual computer" loaded in your operating system, and then throw it away after use. VirtualBox is a good free example. VMware Workstation Player is also free for non-commercial use.

This may be the only way to avoid being tracked by "browser fingerprinting ". This is when the tracking company (or government agency) gives your PC a unique identifier based on variables such as screen resolution, browser version, extensions, fonts, timezone and so on. If you use a virtual PC, every session starts with a more-or-less generic fingerprint. It may not be perfect, but it's less identifiable than the alternative.

Mail, messaging and smartphones

The snooper's charter obviously covers too many services and devices for a single answer. However, you could consider switching to a secure email service such as ProtonMail, and a secure messaging service such as Signal. ChatSecure, WhatsApp and Apple's iMessage also encrypt messages.

You can't make smartphone use private because you're always being tracked by the cellular network. However, you can turn off Wi-Fi and Bluetooth when you're not using them - they can also be used to track you - and use a VPN for web access. Remember also that many smartphone apps request permissions that enable them to track you.

Last words

As an ordinary citizen with a life, you can't hide from the security services, any more than you can defend your house against a tank regiment. If they want to hack your devices, they will. If you're an investigative journalist, human rights campaigner, one of Snowden's collaborators etc, you need a higher level of security.
But if they are not out to get you, why act as though they should be? It's probably better to be as inconspicuous as possible, while limiting the amount of data that might turn up in some bored agency's random fishing expeditions.

I think that VPNs are - or soon will be - normal enough not to attract undue attention. There are already plenty of reasons for using a VPN, to protect yourself in a world of hostile Wi-Fi hotspots (hence HotSpot Shield, Hide My Ass etc) and other online threats. That's why many large businesses use VPNs. The fact that they may also shield you from some state snooping is just a bonus.

Have you got another question for Jack? Email it to Ask.Jack@theguardian.com

Pornography is just the first victim of this Government's censorship crusade

BYLINE: JERRY BARNETT

SECTION: COMMENT; Pg. 35

LENGTH: 503 words

On the surface the new measures to empower a media regulator to block "non-compliant" porn sites are an extension of existing regulations. In December 2014, a law was sneaked on to the statute books, outlawing the publication of extreme pornography, leading to the memorable face-sitting protest outside Parliament.

The British Board of Film Censorship (BBFC) banned depictions of female ejaculation, menstruation, face-sitting (as well as any other act that might conceivably suffocate someone), fisting, and any form of spanking, whipping or other fetish act that leaves marks. Of course nobody took any notice because the internet has long provided us with a huge diversity of pornography. Ban the publication of certain types of porn in the UK and it simply moves overseas.

Finally the Government has got round to amending this loophole. Under the Digital Economy Bill, internet service providers will be forced to block sites hosting content that would not be permitted for DVD sale by the BBFC. These standards are based on a moral judgment by the BBFC rather than law. In fact, all of the above acts are legal for adults above the age of consent.

Instead they are based on the old idea that content might "deprave and corrupt" viewers. This is the same test under which the book Lady Chatterley's Lover was prosecuted for obscenity in 1960, in which the prosecutor hilariously asked jurors whether "you would wish your wife or servants to read" such material.
In fact, the law will block far more than just "extreme" porn. It is likely to block any sexual or erotic material, even simple nudity, on sites that don't first verify the ages of their visitors. In practice this will be difficult to enact due to cost, causing millions of sites to be blocked.

But this isn't much about porn at all - it is about censorship. Although only sexual material is covered in this phase of the bill, regulators have already muttered about other threats to society. The BBFC already censors far more than pornography. For example, it will cut DVD works that "promote the misuse of drugs" or "actively promote illegal behaviour".

The UK has created an official censor with the power to block sites based upon the legality of their content. Pirating sites have long been blocked because they offer illegal services, but now the Government is banning sites based upon their content: fetish pornography which is illegal for distribution, but not for mutually consenting adults to perform.

Piracy sites have long been blocked via court orders, but this regime will circumvent the court system, giving the undemocratic BBFC the power to threaten online freedom of expression.

Under the Draft Communications Data Bill, nicknamed the Snooper's Charter, the Government can access our browser history and now under the digital economy bill, they'll be able to control what we see. First they'll come for your porn and who knows what they'll come for next.

Jerry Barnett is the founder of the Sex & Censorship campaign, and author of 'Porn Panic!'
Tech groups and privacy advocates say that nothing of substance has been altered in the final version of the bill. "In 20 years that I've been dealing with surveillance policy in this country I have never seen a more docile parliament," said Gus Hosein, executive director of the non-profit organisation Privacy International, regarding the bill's passage.

"I was there when we passed RIPA [the current surveillance law] in 2000 and after 9/11 in Washington and at 7/7 [the terrorist attacks in London], and at this moment parliament is sleeping."

The principal objections are to specific clauses that compel internet companies to keep bulk records of all users for up to a year, and allow the government to either coerce tech companies to hand them over when served with a notice and remove encryption when requested, or allow government agencies to hack into people's electronic devices.

However, the government will appoint an Investigatory Powers Commissioner and judicial commissioners as independent judges to oversee any warrants.

"There are some very extensive powers in the bill and in the wrong hands are capable of being abused, no doubt about that," said David Anderson QC, who was commissioned by David Cameron, the former prime minister, to conduct a review of surveillance laws; this work has been described as a blueprint for the new law. "But the bill does subject everything to a legal framework, so there is no excuse for agencies to do anything they are not fully authorised to do."

Here is a summary of the new legislation and how it could affect you.

**Bulk data collection**

The new law would allow mass and indiscriminate data collection of everyone in the UK. Internet and phone companies would have to keep the records of every phone call made and every website visited by any of their users for 12 months.

Not only would telecoms companies have a list of every site visited or call made, they would also record the date, time and duration of these actions.

MPs who voted against the bill during its draft stages, such as SNP MP Joanna Cherry, said they believed that "in order to protect civil liberties, surveillance should be targeted, with warrants from courts that ensure they are focused, specific and based on reasonable suspicion".

However, the bill allows bulk data collection, dashing the hope that surveillance will have to be targeted and "based on reasonable suspicion". Mr Hosein said: "No [western] government anywhere has passed such laws on bulk collection and bulk hacking because it's mass surveillance. Time and again, courts have ruled this is unlawful and unacceptable in a democratic society."

**Access to bulk data**

Dozens of public organisations and departments will be able to access your communications, in some cases without a warrant. These agencies range from the police, HM Revenue & Customs, customs officials and intelligence agencies, to the NHS, the Department of Health, the Food Standards Agency and the Gambling Commission.

To be given access to data pertaining to a specific person, no warrant will be needed, except in certain circumstances, such as when the police are trying to access data about a journalist’s source.

Surveillance data can also be requested in bulk by the intelligence agencies -- MI5, MI6 and GCHQ -- under a special warrant that needs the approval of an independent judge. The data can belong to an unlimited number of people who are not suspected of any criminal activity.

According to Privacy International's general counsel: "The intelligence agencies can obtain large amounts of communications data, and potentially content, through the acquisition of bulk personal data sets, which are defined as containing information about individuals that 'are not, and are unlikely to become, of interest to the intelligence services.'"

**Bulk hacking**

For the first time, the law will allow security agencies and law enforcement to hack into computers, phones and networks to eavesdrop on communications. They will require a warrant to do so.

Security and intelligence officials can even hack into computers outside the UK's borders under a warrant authorised by both the home secretary and an independent judge to download data from unattended mobile phones or remotely taking control of laptops.
Backdoors to encryption

This year, US tech giants including Apple, Google, Microsoft, Facebook and Twitter made written submissions to voice their concerns about the bill. "We reject any proposals that would require companies to deliberately weaken the security of their products via backdoors, forced decryption, or any other means," the document said.

The bill has retained the legal basis to force companies to create a backdoor even into encrypted services such as WhatsApp and iMessage -- although government agencies will need a warrant to make the companies give them access.

However, "a key left under the doormat would not just be there for the good guys. The bad guys would find it, too", Apple cautioned in its submission to parliament last December.

Tech companies have also been worried about the extraterritorial nature of the law, which will require foreign companies with British consumers to comply, even if their home countries have conflicting laws, as the US currently does.

LOAD-DATE: December 21, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

The snooper's charter passed into law this week - say goodbye to your privacy

BYLINE: SILKIE CARLO

SECTION: COMMENT; Pg. 32

LENGTH: 597 words

This week a law was passed that silently rips privacy from the modern world. It's called the Investigatory Powers Act.

Under the guise of counter-terrorism, the British state has achieved totalitarian-style surveillance powers - the most intrusive system of any democracy in history. It now has the ability to indiscriminately hack, intercept, record, and monitor the communications and internet use of the entire population.

The hundreds of chilling mass surveillance programmes revealed by Edward Snowden in 2013 were - we assumed - the result of a failure of the democratic process. Snowden's bravery finally gave Parliament and the public the opportunity to scrutinise this industrial-scale spying and bring the state back into check.

But, in an environment of devastatingly poor political opposition, the Government has actually extended state spying powers beyond those exposed by Snowden - setting a "world-leading"
precedent. Internet service providers must now store details of everything you do online for 12 months - and make it accessible to dozens of public authorities.


Government agencies have even won powers to hack millions of computers, phones and tablets en masse, leaving them vulnerable to further criminal attacks.

You might think that you have nothing to hide, and therefore nothing to fear. In that case, you may as well post your email and social media login details in the comments below.

But I don’t think we do feel that blasÉ about our privacy - we cherish our civil liberties. Everyone has a stake in guarding our democracy, protecting minorities from suspicionless surveillance, defending protest rights, freedom of the press, and enjoying the freedom to explore and express oneself online. These freedoms allow our thoughts, opinions and personalities to flourish and develop - they are the very core of democracy.

Has any country in history given itself such extensive surveillance powers and remained a rights-respecting democracy? We need not look too far back - or overseas to see the risks of unbridled surveillance. In recent years, the British state has spied on law-abiding environmental activists, democratically elected politicians, victims of torture and police brutality, and hundreds of journalists.

In fact, as the Bill finally passed on Wednesday evening, I was training a group of British and American journalists in how to protect themselves from state surveillance - not just from Russia or Syria, but from their own countries.

When Edward Snowden courageously blew the whistle on mass surveillance he warned that, armed with such tools, a new leader might "say that 'because of the crisis, because of the dangers we face in the world, some new and unpredicted threat, we need more authority, we need more power.' And there will be nothing the people can do at that point to oppose it".

The US finds itself with a President-elect who has committed to monitoring all Mosques, banning all Muslims, investigating Black Lives Matter activists and deporting two to three million people. And with the ushering into law of the UK-US free trade in mass surveillance, MPs may have a lot to answer for.

Liberty and its members fought tooth and nail against this new law from its inception to the moment it was passed. That fight is not yet over. Our message to Government: see you in Court.

Silkie Carlo is the policy officer at Liberty

LOAD-DATE: November 19, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: IA
Don’t let the crisp autumn chill put you off an English mini-break

SECTION: FABULOUS;FEATURES; Pg. 68,69

LENGTH: 777 words

THE WHITE HOUSE, BRIGHTON
Writer kate Wills discovers much more than just cheesy seaside fun

THE PAD
This boutique bolt-hole in the village-like area of Kemp Town in Brighton has sea views, Orla Kiely toiletries and fluffy robes. Rooms are bright, the hosts are super-chilled and the delicious brekkie includes wild mushrooms on toasted brioche.


REFUEL
Lunch at The Bull Seafood, eat food! in Ditchling is pub perfection, with old beams, local ale and a menu with treats such as popcorn panna cotta, £7 (www.Thebullditchling.com). Head to the iconic Grand hotel's terrace to watch wind-whipped walkers stroll on the promenade as you dig into a Seafood Afternoon Tea of oysters, fresh crab and caviar, from £22 (www.Grandbrighton.co.uk). Don’t miss Snooper’s Paradise in Brighton's North Laine has vintage finds galore, but hit the first floor for local hand-made jewellery (www.Snoopersattic.co.uk). Next, step into Tales From Woodlandia for a winter world pop-up, complete with boozy hot chocolate and activities such as wreath-making, open until February 28 (www.Patternsbrighton.com). Book it Doubles cost from £85 B&B (White www.housebrighton.com).Be taken for a ride (in a good way) on Brighton pier The hand & spear, SURREY assistant editor Claire frost checks out a cosy pub with boutique rooms the PaD Jump straight off the train at Weybridge into one of 12 individually decorated bedrooms in this pub next to the station. We loved Room 12, with its so-deep-you-can-float roll-top copper bath, retro curiosities and botanical prints. The cute mini-bar comes in a hamper, and there are complimentary chocolates and port. The highlight of dinner was the smokehouse board of delicious cured meats and devilled whitebait, £17. Plus, Copper load for a decadent the bar hosts live music - from jazz to acoustic - every Saturday night. Next morning, clear your head with avo eggs Benedict and spicy harissa.

EXPLORE At Brooklands Museum, a 15-minute walk away, sit in a replica F1 car and drive a virtual lap around the historic race track, or step onboard Concorde and learn about flying supersonic. Entry is from £11 (www.Brooklandsmuseum.com). Then take a stroll along the river to New Haw Lock and spy the cottage apparently haunted by a lock keeper’s wife - spooky! Refuel Brooklands Hotel is a short drive, and its two-AA Brooks COUNTRY house HOTEL, herefordshire senior sub-editor stacey Bartlett hits the Welsh border the PaD This Georgian manor has huge four-poster beds and is surrounded by acres of hills - so it's bliss even when the outdoor pool is closed for winter. Plus they make their own wine - try the Pengethley Estate white, £15 a bottle, accompanied by hake on a tomato and chorizo ragout, £25 for three courses.

EXPLORE The Forest of Dean is on your doorstep, so rent a bike, £14 for a half-day, and cyclethe family-friendly 12-mile trail in fairytaile woods (www.Pedalabikeaway.co.uk). This is cider country too, so take a tour of Weston’s Cider Mill, £10, and try uniquely flavoured brews such as damson and rhubarb (www.Westons-cider.co.uk). Come spring, Eastnor Castle opens and houses a mix of taxidermy owls, suits of armour and lavish decor. Entry costs £11 (www.Eastnorcastle.com). Refuel Stop by The Moody Cow for melt-in-the-mouth buttermilk chicken goujons with pesto, £7.50, or local three-cheese tart, £14.95 (www.Moodycowsir.com). We also pottered around Ledbury market town, and visited Delilah's cafe for rose and pistachio cake. Don't miss Across the border in Monmouthshire is TV presenter Kate Humble’s farm and rural skills school. Learn to forage or even help deliver baby lambs. We built an outdoor wood-fired pizza oven from mud, straw and clay. Courses start at £35 (www.Humblebynature.com). Book it Double rooms cost from £67 B&B (www.Brookscountryhouse.com).

rosette restaurant 1907 does a tasty Sunday lunch, £22.50 for two courses (www.Brooklandshotelsurrey.com). Or French Fancy’s serves a gorgeous afternoon tea, £17.95 (www.Frenchfancysteasalon.co.uk).
Don't miss Stunning RHS Garden Wisley is 15 minutes away, entry £13 (www.Rhs.org.uk/gardens/wisley), then pit-stop at the Valentina deli in Weybridge to stock up on Italian grub (www.Valentinafinefoods.com). Book it Double rooms cost from £109 B&B (www.Handandspear.co.uk).

LOAD-DATE: November 20, 2016

LANGUAGE: ENGLISH

GRAPHIC: water great time you'll have cycling in the forestcopper load of this for a decadent dip

Compiled by: Catherine Bennion-Pedley Photography: Getty Images, Shutterstock, Alamy

Be taken for a ride (in a good way) on Brighton pier take a hike at Devil's Dyke

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: SUN

Copyright 2016 NEWS GROUP NEWSPAPERS LTD
All Rights Reserved
A birth certificate to use the loo?;
Agony uncle

BYLINE: David Tang

SECTION: FT WEEKEND SUPPLEMENT - HOUSE & HOME; Pg. 2

LENGTH: 729 words

On the joint piece that Lucy Kellaway and I wrote recently (November 5), a sizeable mailbag arrived, mostly satisfactory I am glad to report. But I could not help noticing that there was also a group of whom I could only regard as FT voyeurs writing in with questions about the photographs and video. It was as if over porridge at the weekend breakfast table, Sherlock Holmes practitioners brought out their magnifying glasses to look for forensic clues in my set at Albany.
Several of them were suspicious that there were five cups and saucers when there were just two of us; and that there did not seem to be a teapot. To these charges, I should point out that while the dialogue took place only between Lucy and myself, we did also have in attendance two cameramen and a photographer. Ergo, there were five of us. I am disappointed that these snoopers did not have the courtesy to include the crew, who were the real workers. Although there was no teapot, there was a flask which I always use to keep my tea hot. Indeed, the flask is a very smart one designed by Lord Linley. It is much more efficient and much less dowdy than a tea cosy.

Another reader complained that I seemed to have invitations on my chimney piece in order to show off my connections in the social world. This was simply incorrect, as all the cards are shooting cards with wonderful records of dear friends as guns, and the drives we shot at, with the division of birds shot. These are not showing-off items but reminders of my indulgent passion for shooting. After all, the pheasant was originally indigenous to China and it is a beautiful bird to which I particularly relate.

Then someone else accused me of showing off by having a framed picture of myself with the Pope. As a Catholic, I regard my private audience with the Holy Father as a saintly encounter that is worthy of being an exceptional reminder. Otherwise I have over the years become rather indifferent to photographs. At my 60th birthday, attended by hundreds of guests, I did not take any photograph, nor did I ask a photographer to be there to snap away. I have not a single photograph of that happy occasion.

Anyway, I am flattered that readers had the time to tooth-comb my set at Albany for clues of my existence. One was particularly interested in what I read, and wished he could zoom in on my books in the book cupboards, of which I have six big ones. I can reveal that they are largely old books on the subjects of physics, philosophy and law from my student days, as well as a great number of biographies and art books. In one cupboard in my bedroom, I have 350 books of Chinese thrillers and tales of mysteries written in English. So Fu Manchu and Judge Dee figure prominently in front of me as I go to sleep.

What are the modern etiquettes regarding LGBT?

All I would say on this question is that one does not wish to be living in North Carolina, which in March 2016 passed a Bathroom Bill which requires a transgender person to use the lavatory appropriate to their birth-assigned gender. Therefore, in that state, a woman should not be surprised to find a transgender man barging into her lavatory and using the facility standing up; nor for a man to see a transgender woman enter the lavatory and hesitate about using the urinal.

I hope Britain will never see the day when someone using a public lavatory might have to produce their birth certificate before entering. In any event, long gone are the days when being gay or bisexual was remotely an issue. Transgender seems to be the current flavour and there seems to be a lot of fuss about who wants what.

I remember the cause célèbre in France in 1986 when a French diplomat was jailed for treason after passing secrets to his lover, a Chinese opera singer, who turned out to be a man. Apparently, for more than 20 years, the Frenchman thought his lover was a woman with whom he had a child, although the child had been secretly adopted. It was a bizarre case and remembering it makes me realise that nothing really shocks me any more.

Overall, I believe the right approach is to be totally relaxed about the issue of open sexuality, by which I mean we should accept everyone who wants to represent themselves as a man or a woman. I don't care unless I become romantically involved with them.

To post comments and questions, visit ft.com/david-tang or email david.tang@ft.com
'Extreme surveillance' becomes UK law with barely a whimper; Investigatory Powers Act legalises range of tools for snooping and hacking by the security services

BYLINE: Ewen MacAskil

A bill giving the UK intelligence agencies and police the most sweeping surveillance powers in the western world has passed into law with barely a whimper, meeting only token resistance over the past 12 months from inside parliament and barely any from outside.

The Investigatory Powers Act, given royal assent on Thursday, legalises a whole range of tools for snooping and hacking by the security services unmatched by any other country in western Europe or even the US.

The security agencies and police began the year braced for at least some opposition, rehearsing arguments for the debate. In the end, faced with public apathy and an opposition in disarray, the government did not have to make a single substantial concession to the privacy lobby.

US whistleblower Edward Snowden tweeted: "The UK has just legalised the most extreme surveillance in the history of western democracy. It goes further than many autocracies."

Snowden in 2013 revealed the scale of mass surveillance - or bulk data collection as the security agencies prefer to describe it - by the US National Security Agency and the UK's GCHQ, which work in tandem.

But, against a backdrop of fears of Islamist attacks, the privacy lobby has failed to make much headway. Even in Germany, with East Germany's history of mass surveillance by the Stasi and where Snowden's revelations produced the most outcry, the Bundestag recently passed legislation giving the intelligence agencies more surveillance powers.

The US passed a modest bill last year curtailing bulk phone data collection but the victory of Donald Trump in the US presidential election is potentially a major reverse for privacy advocates. On the campaign trail, Trump made comments that implied he would like to use the powers of the surveillance agencies against political opponents.

The Liberal Democrat peer Lord Strasburger, one of the leading voices against the investigatory powers bill, said: "We do have to worry about a UK Donald Trump. If we do end up with one, and that is not impossible, we have created the tools for repression. If Labour had backed us up, we could have made the bill better. We have ended up with a bad bill because they were all over the place.

"The real Donald Trump has access to all the data that the British spooks are gathering and we should be worried about that."

The Investigatory Powers Act legalises powers that the security agencies and police had been using for years without making this clear to either the public or parliament. In October, the investigatory powers tribunal, the only court that hears complaints against MI6, MI5 and GCHQ, ruled that they had been unlawfully collecting massive volumes of confidential personal data without proper oversight for 17 years.

One of the negative aspects of the legislation is that it fails to provide adequate protection for journalists' sources, which could discourage whistleblowing.

One of the few positives in the legislation is that it sets out clearly for the first time the surveillance powers available to the intelligence services and the police. It legalises hacking by the security
agencies into computers and mobile phones and allows them access to masses of stored personal data, even if the person under scrutiny is not suspected of any wrongdoing.

Privacy groups are challenging the surveillance powers in the European court of human rights and elsewhere.

Jim Killock, the executive director of Open Rights Group, said: "The UK now has a surveillance law that is more suited to a dictatorship than a democracy. The state has unprecedented powers to monitor and analyse UK citizens' communications regardless of whether we are suspected of any criminal activity."

Renate Samson, the chief executive of Big Brother Watch, said: "The passing of the investigatory powers bill has fundamentally changed the face of surveillance in this country. None of us online are now guaranteed the right to communicate privately and, most importantly, securely."

Trump's victory started speculation that, given his warm words for Vladimir Putin, he might do a deal with the Russian president to have Snowden sent back to the US where he faces a long jail sentence. Snowden has lived in Russia since leaking tens of thousands of documents to journalists in 2013.

But Bill Binney, a former member of the NSA who became a whistleblower, expressed scepticism: "I am not sure if the relationship a President Trump would have with President Putin would be bad for Snowden. In Russia, he would still be an asset that maybe Putin would use in bargaining with Trump. Otherwise, Snowden does have a large support network around the world plus in the US and Trump may not want to disturb that. Also, I think any move to get Snowden out of Russia and into US courts would also open up support for at least three other lawsuits against the US government's unconstitutional surveillance."

LOAD-DATE: November 19, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: WEBGNS

The House of Lords has passed the Investigatory Powers Bill, putting the huge spying powers on their way to becoming law within weeks. The bill - which forces internet companies to keep records on their users for up to a year, and allows the Government to force companies to hack into or break
things they've sold so they can be spied on - has been fought against by privacy campaigners and technology companies including Apple and Twitter.

But the Government has worked to continue to pass the bill, despite objections from those companies that the legislation is not possible to enforce and would make customers unsafe. The House of Lords's agreement to the text now means that it just awaits Royal Assent, at which point it will become law.

Despite criticism from almost every major technology and internet company - including usually reticent ones like Apple - and from senior parliamentary committees the legislation has received little opposition in parliament. Early on, the only amendment that the bill received from MPs was a measure that stopped themselves being spied on, and while Labour has raised objections to the sweeping spying powers it has not voted against the bill.

Those opposing the bill argue that it has been hastily written and is being pushed through parliament too quickly to ensure that it doesn't receive full scrutiny. That has led to the bill including measures that are still undefined and so could be used by the Government to force companies to do almost anything, tech firms have argued.

The main objections to the bill centre around the vast new powers that the Government is given to spy on its citizens. It includes powers to force companies to make their phones less secure so that they can be listened in on by spies, and others that would allow the Government to ask companies like Apple and Google to help them break or hack into phones.

Perhaps the most controversial measure will require internet service providers to keep detailed information on their customers' web browsing for the last year. There will be no way of opting out of that and the data will be collected on everyone, leading to fears that it could be stolen and leaked, especially given the huge scale of the Talk Talk hack earlier this year.

In all, the new bill includes a range of changes to the law that will affect normal people, and gives Britain perhaps the most extreme spying powers in the developed world. The apparently final part of the Government's fight to have the powers passed came as it refused to budge over its proposed new surveillance powers by rejecting for a second time amendments from peers linked to phone hacking.

Solicitor General Robert Buckland insisted it would be "simply not appropriate" to include within the Investigatory Powers Bill changes designed to ensure costs are awarded against newspaper and media organisations in phone hacking cases.

Peers have repeatedly sought to amend the Bill so it implements a key part of the Leveson Inquiry report by offering "protection" over costs for victims of press intrusion. But MPs voted to reject the latest Lords amendments by 295 votes to 245, majority 50.

A parliamentary process known as ping-pong is ongoing, which sees the Bill move between the Commons and the Lords until a final decision is taken over the text. It will return to the Lords for further scrutiny. The Bill gives a range of new powers to access data and internet communications to police and security services.

Elsewhere, ministers are also conducting a 10-week consultation which includes examining whether to implement legislation which would force newspapers to pay all of the costs of libel or privacy actions brought against them - even if they win their case. This would not apply to publications which sign up to a new state-backed press regulator.

Mr Buckland reiterated this consultation "speaks directly to the concerns" of those who support the Lords amendments. He recognised independent crossbencher Baroness Hollins had revised her amendments, but later told MPs: "They have no place in a Bill that relates to the regulation of investigative powers."

"This is all about national security, this is about dealing with crime whether it's child abuse, whether it's trafficking, whether it's drug dealing, whether it's the sort of criminality that we want to deal with in our society. That's why these amendments are not only out of place but also they pre-empt the outcome of the consultation launched by (Culture Secretary Karen Bradley)."

Tory MP Jacob Rees-Mogg (North East Somerset), intervening, said: "Wouldn't you go further and to say that putting restrictions on the press in a Bill on national security is actually precisely the wrong place to have restrictions on the press - it makes it look as if we're really trying to hit them hard?" Mr Buckland noted an "important point" had been made.

Shadow Home Secretary Diane Abbott backed the changes proposed by peers, telling the Commons: "I believe any member of the public who just heard the speech from the Government benches will be
puzzled as to the Government's continuing resistance to implementing an aspect of Leveson that it, in principle, agreed to some time ago.

"Labour fully supports this set of amendments to the Investigatory Powers Bill and on this side of the House we have consistently and genuinely called for the Leveson recommendations to be implemented in full."

SNP justice spokeswoman Joanna Cherry also supported the amendments and said: "Those who have not hacked, do not hack phones and do not intend to hack telephones or indeed emails have nothing to fear from these provisions."

But Mr Rees-Mogg said: "This is an absolutely dreadful amendment. It should be thrown out, rejected, sent back to the House of Lords. It is fundamentally wrong. It seeks to punish those who may be innocent, to fine them for telling the truth, for saying things that people in power do not like. It goes to the heart of our free press and it should be thrown in the bin."

LOAD-DATE: November 18, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper

JOURNAL-CODE: IA

Sir David Tang, the billionaire socialite and philanthropist who is said to be the best connected man in London (after my hobbit Grant), was interviewed at the Royal Geographical Society on Thursday. He said that he had come quite a long way since arriving in Britain as a 13-year-old without a word of English. "I failed my O Levels six times before passing," he said. "My English master said to me: 'Tang, I don't think you'll ever be fluent in English.'" Twenty years later they met again. "I must say, you seem pretty fluent now," the patronising teacher told him. Tang's response was a two-word Anglo-Saxon imperative meaning "go away", proving that those extra lessons had been well worth it.

Tang of salt to travel advice;
TMS diary@thetimes.co.uk | @timesdiary

SECTION: NEWS; Pg. 11

LENGTH: 489 words
On Monday, May will show that she is in control with a speech to the CBI conference, which is sponsored by Deloitte. Might make for a frosty conversation backstage.

where is shami's shame? Shami Chakrabarti made her maiden speech in the House of Lords on Thursday during a debate about foreign students. Eyebrows were raised that the shadow attorney-general hadn't made her debut the previous day, when the Lords debated the expansion of surveillance powers. Surely, as the director for 13 years of a civil liberties campaigning group, she might have had some insights. Apparently not. Labour supports the snoopers' charter and Chakrabarti, left, has traded her principles for www.ermine. No wonder some have rebranded her as Shameless.

Oh to be a fly on the wall at the first meeting of Shinzo Abe, the prime minister of Japan, and Donald Trump on Thursday night. "So tell me, Abe," I imagine Trump asking. "Did they name you after Lincoln?" that's enough rebel yell The 25th anniversary of the start of the Maastricht rebellion was marked, two months early, with a dinner at the House of Commons this week. Only four of the rebels remain in the lower chamber - Sir Bill Cash, Iain Duncan Smith, John Whittingdale and Bernard Jenkin. They were joined by peers and fellow travellers to feast on Gressingham duck (no Brussels sprouts). Oddly, Sir John Major did not pop in for old times' sake. Nor were there any speeches. As Sir Bill says: "I think we've all done more than enough speaking."

patrick kidd

Snooper’s Charter that will let police hack into phones and check anyone's browser history becomes law after peers backed down on amendments

BYLINE: PADDY DINHAM FOR MAILONLINE

SECTION: NEWS

LENGTH: 346 words

The Investigatory Powers Bill was passed by the House of Lords today
App companies must keep data for a year and police can hack your phone
An attempted amendment to the law from the Lords was rejected by MPs
The Government sees it as essential for tackling organised crime

Police will now be able to hack into your phones and check your browsing history after the Snooper’s Charter was passed by Parliament.
The bill - officially called the **Investigatory Powers Bill** - forces electronic data to be stored by app companies for 12 months, which can be subsequently collected by law enforcement.

While critics have cited it as an attack on privacy, the Government believes the charter is essential for combating terrorism and organised crime.


It was passed by the House of Lords today after they backed down on an amendment that would have forced the press to pay court costs for both parties in any case involving allegations of phone or email hacking, even if they were completely spurious.

One peer said it would have 'chilled' journalism and stopped papers writing about figures such as ex-BHS boss Sir Philip Green.

Lord Myners said the amendment to implement section 40 of the Crime and Courts Acts 2013 would have made it easier for the rich to sue on spurious grounds.

Last night, however, campaigners in the Lords signalled their intention to continue to push for the controversial changes by tacking them on to another bill.

The stand-off between the two houses came to an end after MPs rejected for a second time the peers' changes to the **Investigatory Powers Bill** on Tuesday.

And the following day the Lords accepted defeat in what will be seen as a victory for Press freedom.

Aside from the controversy surrounding its morality, the charter's effectiveness has also been questioned, with Virtual Private Network software already being highlighted as a potential way for internet users of getting around it.

Using a VPN means data will be scrambled and protected from the company that provides the connection.

**LOAD-DATE:** November 18, 2016

**LANGUAGE:** ENGLISH

**PUBLICATION-TYPE:** Web Publication

**JOURNAL-CODE:** WEBDM

Copyright 2016 Associated Newspapers Ltd.
All Rights Reserved

Return to List

91 of 100 DOCUMENTS

DAILY MAIL (London)

**November** 17, 2016 Thursday

**VICTORY FOR PRESS OVER LEGAL FEES FOR PHONE HACK CASES**

**BYLINE:** BY DANIEL MARTIN CHIEF POLITICAL CORRESPONDENT

**LENGTH:** 309 words

PEERS backed down last night in a battle with MPs over a new law that could have prevented newspapers exposing corruption and speaking out against injustice.

The House of Lords decided not to push through an amendment to the Investigatory Powers Bill - the so-called **Snoopers' Charter** - that would have forced papers to pay court costs for both parties in any case involving allegations of phone or email hacking.
One peer said it would have chilled journalism and stopped papers writing about figures such as ex-BHS boss Sir Philip Green.

Lord Myners said the amendment to implement section 40 of the Crime and Courts Acts 2013 would have made it easier for the rich to sue on spurious grounds.

Last night, however, campaigners in the Lords signalled their intention to continue to push for the controversial changes by tacking them on to another bill.

The stand-off between the two houses came to an end after MPs rejected for a second time the peers’ changes to the Investigatory Powers Bill on Tuesday.

Yesterday the Lords accepted defeat in what will be seen as a victory for Press freedom.

Independent crossbencher Lord Myners, former chairman of The Guardian, said many stories in the newspaper may not have been written in the way they were had the legislation succeeded.

He added: This clause is a charter for the venomous and the vexatious, the pernicious and the provocative, the scurrilous and the spiteful.’

Speaking for the Government, Earl Howe indicated that a new consultation would include examining whether to force newspapers to pay all of the costs of libel or privacy actions brought against them even if they win.

This would not apply to publications that sign up to a new State-backed Press regulator.

Lady Hollins, who introduced the original amendment, said: I do intend to return to this matter again in a more suitable Bill.'
The bill - which forces internet companies to keep records on their users for up to a year, and allows the Government to force companies to hack into or break things they've sold so they can be spied on - has been fought against by privacy campaigners and technology companies including Apple and Twitter.

But the Government has worked to continue to pass the bill, despite objections from those companies that the legislation is not possible to enforce and would make customers unsafe.

The apparently final part of the Government's fight to have the powers passed came as it refused to budge over its proposed new surveillance powers by rejecting for a second time amendments from peers linked to phone hacking.

Solicitor General Robert Buckland insisted it would be "simply not appropriate" to include within the Investigatory Powers Bill changes designed to ensure costs are awarded against newspaper and media organisations in phone hacking cases.

Peers have repeatedly sought to amend the Bill so it implements a key part of the Leveson Inquiry report by offering "protection" over costs for victims of press intrusion.

But MPs voted to reject the latest Lords amendments by 295 votes to 245, majority 50.

A parliamentary process known as ping-pong is ongoing, which sees the Bill move between the Commons and the Lords until a final decision is taken over the text.

Read more

Theresa May-led law could be killed by ruling from Europe

It will return to the Lords for further scrutiny.

The Bill gives a range of new powers to access data and internet communications to police and security services.

Elsewhere, ministers are also conducting a 10-week consultation which includes examining whether to implement legislation which would force newspapers to pay all of the costs of libel or privacy actions brought against them - even if they win their case.

This would not apply to publications which sign up to a new state-backed press regulator.

Mr Buckland reiterated this consultation "speaks directly to the concerns" of those who support the Lords amendments.

He recognised independent crossbencher Baroness Hollins had revised her amendments, but later told MPs: "They have no place in a Bill that relates to the regulation of investigative powers."
"This is all about national security, this is about dealing with crime whether it's child abuse, whether it's trafficking, whether it's drug dealing, whether it's the sort of criminality that we want to deal with in our society.

"That's why these amendments are not only out of place but also they pre-empt the outcome of the consultation launched by (Culture Secretary Karen Bradley)."

Tory MP Jacob Rees-Mogg (North East Somerset), intervening, said: "Wouldn't you go further and to say that putting restrictions on the press in a

Bill on national security is actually precisely the wrong place to have restrictions on the press - it makes it look as if we're really trying to hit them hard?"

Mr Buckland noted an "important point" had been made.

Shadow home secretary Diane Abbott backed the changes proposed by peers, telling the Commons: "I believe any member of the public who just heard the speech from the Government benches will be puzzled as to the Government's continuing resistance to implementing an aspect of Leveson that it, in principle, agreed to some time ago.

"Labour fully supports this set of amendments to the

Investigatory

Powers

Bill

and on this side of the House we have consistently and genuinely called for the Leveson recommendations to be implemented in full."

SNP justice spokeswoman Joanna Cherry also supported the amendments and said: "Those who have not hacked, do not hack phones and do not intend to hack telephones or indeed emails have nothing to fear from these provisions."

But Mr Rees-Mogg said: "This is an absolutely dreadful amendment. It should be thrown out, rejected, sent back to the House of Lords.

"It is fundamentally wrong. It seeks to punish those who may be innocent, to fine them for telling the truth, for saying things that people in power do not like.

"It goes to the heart of our free press and it should be thrown in the bin."

Additional reporting by agencies

LOAD-DATE: November 17, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI

Copyright 2016 Independent Digital News and Media Limited
All Rights Reserved

Return to List

93 of 100 DOCUMENTS

MailOnline

November 17, 2016 Thursday 12:19 AM GMT
Victory for the Press over 'charter' for the venomous' after peers back down in battle with MPs over new laws

BYLINE: DANIEL MARTIN CHIEF POLITICAL CORRESPONDENT FOR THE DAILY MAIL

SECTION: NEWS

LENGTH: 342 words

Lords decided not to push through Investigatory Powers Bill amendment
One peer said the amendment would have 'chilled journalism'
Would have 'stopped papers writing about ex-BHS boss Sir Philip Green'

Peers backed down last night in a battle with MPs over a new law that could have prevented newspapers exposing corruption and speaking out against injustice.

The House of Lords decided not to push through an amendment to the Investigatory Powers Bill - the so-called Snoopers' Charter - that would have forced papers to pay court costs for both parties in any case involving allegations of phone or email hacking even if they were completely spurious.

One peer said it would have 'chilled' journalism and stopped papers writing about figures such as ex-BHS boss Sir Philip Green.

Lord Myners said the amendment to implement section 40 of the Crime and Courts Acts 2013 would have made it easier for the rich to sue on spurious grounds.

Last night, however, campaigners in the Lords signalled their intention to continue to push for the controversial changes by tacking them on to another bill.

The stand-off between the two houses came to an end after MPs rejected for a second time the peers' changes to the Investigatory Powers Bill on Tuesday.

Yesterday the Lords accepted defeat in what will be seen as a victory for Press freedom.

Independent crossbencher Lord Myners, former chairman of The Guardian, said many stories in the newspaper may not have been written in the way they were had the legislation succeeded.

He added: 'This clause is a charter for the venomous and the vexatious, the pernicious and the provocative, the scurrilous and the spiteful.'

Earl Howe indicated that a new consultation would include examining whether to force newspapers to pay all of the costs of libel or privacy actions brought against them even if they win.

This would not apply to publications that sign up to a new State-backed Press regulator.

Lady Hollins, who introduced the original amendment, said: 'I do intend to return to this matter again in a more suitable Bill.'

LOAD-DATE: November 17, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

JOURNAL-CODE: WEBDM

Copyright 2016 Associated Newspapers Ltd.
All Rights Reserved
Amazon's app gives its customers X-Ray vision: Update can tell you exactly what's in a delivery box simply by pointing your phone's camera at it

**BYLINE:** STACY LIBERATORE FOR DAILYMAIL.COM and ANTHONY JOSEPH FOR MAILONLINE

**SECTION:** SCIENCE

**LENGTH:** 535 words

Users open the camera feature in the app and scan the barcode on the box
The items appear on the screen, which can be clicked for more information
However, users must have the latest version of the app to use the feature

Amazon is giving its customers the power of x-ray vision.

iOS users can see inside each box they receive from the e-commerce giant with a new feature called Package X-ray.

Users simply scan a barcode on the side of the box with the Amazon app camera and all the goodies inside of the package will be displayed on the screen.

Scroll down for videos

**HOW DOES IT WORK?**

Users must download the latest version of the Amazon app.
Then click on the camera icon located at the top of the page.
Once the camera is open, select the 'Package X-ray' button and hold the camera frame over the barcode on the side of the box.
Each item inside will be displayed on the screen, which users can click for more details.
The new feature is part of the firm's latest update that was released on Wednesday.
To get a quick look inside your packages, simply open the latest version of the Amazon app and tap the camera icon located near the 'What are you looking for' search box.
Once the camera is open, select the 'Package X-ray' button and hold the camera frame over the barcode located on the side of the box.
All of the times will then appear on the screen for you to look over.
The items displayed on your smartphone screen are also clickable, allowing you to see the item's page on Amazon.
And users can see a list of everything in the box, similar to how 'Your Orders' is displayed in the app.
However, this technology is designed to only work for the user who ordered the packages - blocking any snoopers from taking a peak.
The new feature is part of Amazon's big news that announced the firm is offering members more than 35 days of Black Friday Deals.
In order to keep up with the volume over the holiday season, the firm has more than 1,000 staff members inside its 550,000 sq ft warehouse in Peterborough, Cambridgeshire.
Bosss said they had the busiest Black Friday to date on November 27 last year, selling more than 7.4 million items - a rate of around 86 items per second.
The firm hired an extra 15,000 temporary staff across its UK distribution centers last year to cope with increased demand.
This year they have created an additional 20,000 seasonal and 3,500 permanent jobs across its offices and began their biggest ever sale on Monday.

The deals - which has seen up to 80 per cent slashed off some items - will run up until Black Friday next week.

Alongside the discounts on popular items, Amazon has also slashed the cost of its Prime subscription service.

Doug Gurr, Amazon's UK country manager, said: 'In response to positive customer feedback for Black Friday deals, we are introducing The Black Friday Sale - 12 days of fantastic deals on must-have gifts and products, saving our customers millions of pounds.

'We're also thrilled to have over a thousand small businesses featuring in our Black Friday Sale, broadening the selection for our customers and enabling those businesses to boost their sales in the run up to Christmas.'

Iraq war probe 'used Stasi tactics to spy on our troops': MP's accuse investigators of carrying out surveillance on serving personnel accused

Boss of Iraq Historical Allegations Team refused to deny spying allegations
It is unclear why they would need to carry out surveillance of British troops
They were using spying powers under the controversial Regulation of Investigatory Powers Act, supposed to be used for national security

Investigators probing soldiers' actions in incidents during the Iraq War were yesterday accused of 'Stasi-style' spying on British troops.

MPs put it to Mark Warwick, the boss of the controversial Iraq Historical Allegations Team (Ihat), that they had carried out surveillance on veterans and serving personnel as part of their £57million taxpayer-funded inquiry into decade-old allegations of abuse of civilians.

Mr Warwick refused to deny the spying allegations as he said surveillance was seen as an 'appropriate police tactic to use' in certain cases.
The inquiry heard that Ihat had used spying powers under the controversial Regulation of Investigatory Powers Act (Ripa), which is supposed to be used 'in the interests of national security'.

A serving commander last night told the Daily Mail: 'Are we now at the stage where we have Stasi-style spying on the British military with seemingly unlimited powers? This could affect morale and damage trust within the chain of command.'

It is unclear why Ihat would need to carry out surveillance of British troops, but it is believed that investigators are carrying out extensive checks into their backgrounds. The ex-girlfriend of one officer being investigated was asked whether he was racist, had tattoos, was an alcoholic or had extreme political views.

During yesterday's Defence Select Committee inquiry it also emerged that one of the Ihat investigators was charged with impersonating a police officer after he lied to try to get access to a military base.

The civilian employee - who used to be a police officer - tried to use his old warrant card to get into an Army barracks so he could quiz a soldier. MPs were told.

Mr Warwick, 53, also admitted he was taking a police pension - despite earning almost £100,000 a year with Ihat - and revealed that more than 300 troops have been grilled over five years. The spying revelations emerged during a heated exchange between MPs and Mr Warwick about Ihat's practices.

Madeleine Moon MP said: 'You're carrying out surveillance on our personnel and veterans, can you tell us why?'

Mr Warwick responded: 'I wouldn't confirm or deny that we are using surveillance methods because that's an appropriate police tactic to use if it is necessary in serious criminal investigations. 'The nature of our investigative caseload... it would be rare that we would use those tactics if we did use those tactics.'

But Mrs Moon said: 'We've been told very clearly that you are.' And MP Johnny Mercer said a previous report had found that the Ihat team had used Ripa powers. In response, Mr Warwick said: 'Ripa powers crosses a wide range of activities, from obtaining a piece of information from a public company.'

The controversial Regulation of Investigatory Powers Act was passed in 2000 by Labour to regulate spying and surveillance by police and the security services. It was intended for use 'in the interests of national security' but many critics have claimed it has been widely abused.

Mr Warwick, who was dragged before the committee for the first time to give evidence, also revealed how 300 witnesses had been quizzed as a result of 15 allegations of wrongdoing. He said the 147-strong Ihat team had also interviewed 27 suspect soldiers under caution - of which seven were arrested.

According to the latest figures, Ihat - which was set up in 2010 - has received a total of 3,367 allegations of criminality - out of those, 2,470 of the claims were lodged by Public Interest Lawyers, which closed down in August when legal aid funding was withdrawn. A further 718 claims were lodged by human rights law firm Leigh Day, the committee heard.

A team of Ihat investigators have thrown out thousands of the allegations - without a single prosecution. They now have 1,009 cases left to investigate.
Insurance company to trawl Facebook to judge if you are a safe driver;
Algorithm could judge excessive use of exclamation marks to demonstrate overconfidence, a trait which leads to bad driving

BYLINE: Ben Chapman

One of Britain’s biggest insurance companies is looking at people’s Facebook posts to analyse their personalities and judge how likely they are to crash their car.

In a move that will reignite fierce debate about privacy and use of personal data, Admiral Insurance has designed an algorithm to rate drivers for "safe" traits such as conscientiousness or organisation, based on how they interact with their friends and family on social media.

Customers judged by the company’s computer to have reckless personalities will pay higher premiums, while those deemed to be safe drivers will get cheaper insurance.

Read more
Privacy group threatens legal action over WhatsApp data policy change
Those who write lists, set a concrete time and place to meet friends and write in short, specific sentences, will be deemed to have the personality of a safer driver, the company suggested.

Conversely, excessive use of exclamation marks could be seen by the computer as "overconfident", as could liberal use of words like "always" or "never" instead of the more measured, "maybe".

Initially, only first-time drivers will be targeted by the pilot called firstcarquote, which is voluntary.

Yossi Borenstein, the principal data scientist told the Guardian that the system "could be revolutionary. It could be truly transformational."

He added: "Our analysis is not based on any one specific model, but rather on thousands of different combinations of likes, words and phrases and is constantly changing with new evidence that we obtain from the data. As such our calculations reflect how drivers generally behave on social media, and how predictive that is, as opposed to fixed assumptions about what a safe driver may look like."

Read more
Privacy group threatens legal action over WhatsApp data policy change
The snooper’s charter will infringe our right to privacy
Helen Skelton topless images’ branded gross and disturbing

Privacy campaigners have said the move is part of a drive to gather increasingly personal data about people and questioned whether it would be effective or even legal.

"If you are messy, does that make you an erratic driver?,” said Renate Samson, chief executive of Big Brother Watch.

"If you're clean and tidy and don't go to parties does that make you a good driver? Is a hot-head, more likely to have a crash?"
"There are no historic answers to these questions, so why all of a sudden does a company think they can be answered by a computer?

Samson said she believed the innovation was a ploy to get young people to hand over even more of their data. "The insurance companies think all young people are happy to share everything online with businesses, but they are more savvy than that," Samson said. "People shouldn't have to hand over such personal information just to get a good deal on their insurance."

Laws to be introduced in 2018 prevent companies from using personal data to build a profile of users. The full details of firstcarquote aren't yet known but mining people's social media profiles to establish personality traits would apparently be banned.

The scheme may also breach Facebook's own privacy policy which says: "Don't use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan."

The pilot, which was due to launch today but has been delayed while Admiral addresses what it describes as "a few outstanding issues".

A Facebook spokesperson said:"Protecting the privacy of the people on Facebook is of utmost importance to us. We have clear guidelines that prevent information being obtained from Facebook from being used to make decisions about eligibility.

We have made sure anyone using this app is protected by our guidelines and that no Facebook user data is used to assess their eligibility. Facebook accounts will only be used for login and verification purposes.

Our understanding is that Admiral will then ask users who sign up to answer questions which will be used to assess their eligibility."

The Independent has contacted Admiral Insurance for comment.
One of Britain's biggest insurance companies is looking at people's Facebook posts to analyse their personalities and judge how likely they are to crash their car.

In a move that will reignite fierce debate about privacy and use of personal data, Admiral Insurance has designed an algorithm to rate drivers for "safe" traits such as conscientiousness or organisation, based on how they interact with their friends and family on social media.

Customers judged by the company's computer to have reckless personalities will pay higher premiums, while those deemed to be safe drivers will get cheaper insurance.

Yossi Borenstein, the principal data scientist told the Guardian that the system "could be revolutionary. It could be truly transformational."

He added: "Our analysis is not based on any one specific model, but rather on thousands of different combinations of likes, words and phrases and is constantly changing with new evidence that we obtain from the data. As such our calculations reflect how drivers generally behave on social media, and how predictive that is, as opposed to fixed assumptions about what a safe driver may look like."

Privacy group threatens legal action over WhatsApp data policy change

Those who write lists, set a concrete time and place to meet friends and write in short, specific sentences, could be deemed to have the personality of a safer driver, the company suggested.

Punctuation, such as excessive use of exclamation marks could be seen by the computer as "overconfident", as could liberal use of words like "always" or "never" instead of the more measured, "maybe".

Initially, only first-time drivers will be targeted by the pilot called firstcarquote, which is voluntary.

Yossi Borenstein, the principal data scientist told the Guardian that the system "could be revolutionary. It could be truly transformational."

He added: "Our analysis is not based on any one specific model, but rather on thousands of different combinations of likes, words and phrases and is constantly changing with new evidence that we obtain from the data. As such our calculations reflect how drivers generally behave on social media, and how predictive that is, as opposed to fixed assumptions about what a safe driver may look like."

Does Keith Vaz really deserve respect for his privacy?

Privacy group threatens legal action over WhatsApp data policy change

WhatsApp privacy under threat as EU pushed to break encryption

The snooper's charter will infringe our right to privacy

Helen Skelton topless images' branded gross and disturbing

Privacy campaigners have said the move is part of a drive to gather increasingly personal data about people and questioned whether it would be effective or even legal.

"If you are messy, does that make you an erratic driver?," said Renate Samson, chief executive of Big Brother Watch.

"If you're clean and tidy and don't go to parties does that make you a good driver? Is a hot-head, more likely to have a crash?"

"There are no historic answers to these questions, so why all of a sudden does a company think they can be answered by a computer?"

Samson said she believed the innovation was a ploy to get young people to hand over even more of their data. "The insurance companies think all young people are happy to share everything online with businesses, but they are more savvy than that," Samson

Laws to be introduced in 2018 prevent companies from using personal data to build a profile of users. The full details of firstcarquote aren't yet known but mining people's social media profiles to establish personality traits would apparently be banned.

The scheme may also breach Facebook's own privacy policy which says: "Don't use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan."

The pilot, which was due to launch today but has been delayed while Admiral addresses what it describes as "a few outstanding issues".
According to Open Rights Group, Facebook has blocked the app because it breaches one of their policies.

The Independent has contacted Admiral Insurance and Facebook for comment.

Facebook blocks Admiral from reading your posts to judge if you are a safe driver;
Algorithm would have judged certain words and punctuation to demonstrate overconfidence, a trait which leads to bad driving

BYLINE: Ben Chapman

SECTION: BUSINESS NEWS

LENGTH: 716 words

Facebook has blocked one of Britain's biggest insurance companies from looking at people's Facebook posts to price their car insurance premiums.

Admiral Insurance designed an algorithm to rate drivers for "safe" traits such as conscientiousness or organisation, based on how they interact with their friends and family on social media.

Under the new system, customers judged by the company's computer to have reckless personalities were set to pay higher premiums than those deemed to be safe drivers.

Privacy group threatens legal action over WhatsApp data policy change
But Facebook has said the app will be in breach of its terms if it uses personal data to set prices.

A Facebook spokesperson said: "Protecting the privacy of the people on Facebook is of utmost importance to us. We have clear guidelines that prevent information being obtained from Facebook from being used to make decisions about eligibility.

We have made sure anyone using this app is protected by our guidelines and that no Facebook user data is used to assess their eligibility. Facebook accounts will only be used for login and verification purposes.

Our understanding is that Admiral will then ask users who sign up to answer questions which will be used to assess their eligibility."
Admiral said reading social media posts allow it to judge how big a risk customers pose. Those who write lists, set a concrete time and place to meet friends and write in short, specific sentences, could be deemed to have the personality of a safer driver, the company suggested.

Conversely, excessive use of exclamation marks could be seen by the computer as “overconfident”, as could liberal use of words like “always” or “never” instead of the more measured, “maybe”.

Read more

Does Keith Vaz really deserve respect for his privacy?

Privacy group threatens legal action over WhatsApp data policy change

WhatsApp privacy under threat as EU pushed to break encryption

The snooper’s charter will infringe our right to privacy

Helen Skelton topless images’ branded gross and disturbing

Initially, only first-time drivers will be targeted by the pilot called firstcarquote, which is voluntary.

Yossi Borenstein, the principal data scientist behind the project told the Guardian that the system “could be revolutionary. It could be truly transformational.”

He added: “Our analysis is not based on any one specific model, but rather on thousands of different combinations of likes, words and phrases and is constantly changing with new evidence that we obtain from the data. As such our calculations reflect how drivers generally behave on social media, and how predictive that is, as opposed to fixed assumptions about what a safe driver may look like.”

Privacy campaigners have said the move is part of a drive to gather increasingly personal data about people and questioned whether it would be effective or even legal.

“If you are messy, does that make you an erratic driver?,” asked Renate Samson, chief executive of Big Brother Watch.

“If you’re clean and tidy and don’t go to parties does that make you a good driver? Is a hot-head, more likely to have a crash? ”

“There are no historic answers to these questions, so why all of a sudden does a company think they can be answered by a computer? ”

Samson said she believed the innovation was a ploy to get young people to hand over even more of their data. "The insurance companies think all young people are happy to share everything online with businesses, but they are more savvy than that," Samson said. "People shouldn’t have to hand over such personal information just to get a good deal on their insurance."

Laws to be introduced in 2018 prevent companies from using personal data to build a profile of users. The full details of firstcarquote aren’t yet known but mining people’s social media profiles to establish personality traits would apparently be banned.

The scheme may also breach Facebook’s own privacy policy which says: "Don't use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan."

The pilot, which was due to launch today but has been delayed while Admiral addresses what it describes as "a few outstanding issues".

The Independent

has contacted Admiral Insurance for comment.

LOAD-DATE: November 2, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper; Web Publication

JOURNAL-CODE: WEBI
The government is expected to announce further consultation on press regulation in an attempt to stop the issue derailing the investigatory powers bill, or *snooper’s* charter.

The move by Karen Bradley is likely to be welcomed by the newspaper industry, which is opposed to an amendment in the bill which would introduce legal costs protection for phone-hacking victims.

Opening up one of the two remaining issues left unresolved by the Leveson inquiry on press misbehaviour, that of costs protection, will, however, infuriate campaigners for victims of press intrusion, such as Hacked Off.

Bradley, a former home office minister, is to make a statement to the Commons at lunchtime on Tuesday, announcing the plans for further debate on press regulation. In a recent appearance before the Commons culture select committee she raised the concerns of the local newspaper industry about the proposals.

Some Tory rebels were set to join the Labour party whip in favour of the proposed amendment to the law, which would implement one aspect of a key recommendation of the Leveson inquiry: that the victims of phone hacking should be protected from paying the costs of bringing their claims against newspapers in the civil courts.

Major newspaper groups and organisations, such as the Society of Editors, believe the legislation could erode their freedom to publish. It has already won the support of the House of Lords after Baroness Hollins put through an amendment to the investigatory powers bill, which would bring about cost protection for the victims of phone hacking.

Tom Watson, the shadow culture secretary and deputy leader of the Labour party, is expected to oppose Bradley's move.

*LOAD-DATE*: November 1, 2016

*LANGUAGE*: ENGLISH

*PUBLICATION-TYPE*: Newspaper

*JOURNAL-CODE*: WEBGNS
Kremlin dismisses 'unfounded and baseless' claims by MI5 chief that Russia is taking hostile measures against UK

BYLINE: LARISA BROWN DEFENCE CORRESPONDENT FOR THE DAILY MAIL

SECTION: NEWS

LENGTH: 601 words

Andrew Parker, head of MI5, claimed Russia was using cyber attacks
He warned that Russia was at 'work across Europe and in the UK'
But the Kremlin has hit back, saying: 'No-one has yet given any evidence'

The Kremlin has attacked 'unfounded and baseless' claims by the head of MI5 that increasingly aggressive tactics from Russia such as cyber attacks were a threat to Britain.

Andrew Parker, the director general of the home intelligence service, had warned Russia was at 'work across Europe and in the UK' and carrying out a 'high volume' of secret activity.

In an unprecedented interview, he said Russia had been a 'covert threat' for decades however there were now more methods available for its agents to use, such as propaganda, subversion and cyber-attacks.

But Russia hit back and said there was no evidence to support the claims. Kremlin spokesman Dmitry Peskov said: 'Those words to do correspond to the reality.

'We do not agree with them, and claims regarding cyber-attacks we have already commented on.

'No-one has yet given any evidence so we cannot consider claims that are not founded on evidence.

'Until someone produces proof, we will consider those statements unfounded and baseless.'

The Russian embassy in London posted a message on Twitter saying it was 'saddened to see a professional trapped to (sic) his own propaganda-created world'.

Alongside the message was a poster for the 1966 film The Russians are coming, The Russians are coming.

Intelligence sources told the Mail that MI5, MI6 and GCHQ had become increasingly worried about the activity of Russian spies and the difficulty in tracking their activities.

They have become harder to follow because of an increase in sophisticated encryption technology, the source said.

Mr Parker told the Guardian that Russia was adopting an 'increasingly aggressive' approach to pursuing its foreign policy goals.

He said Russia was carrying out a 'high volume' of activity 'out of sight'.

Mr Parker said that MI5 was working to disrupt the activities of Moscow's spies who were 'at work across Europe and in the UK'.

He took aim at Moscow for escalating tensions at a time when the West was trying to fight Islamist extremists.

He said that Russia had plenty of spies still working in Britain but that the difference between today and the Cold War era was that it was also using the weapon of cyber warfare.

Russia was targeting military secrets industrial projects economic information and government in foreign policy he said.
"It is using its whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive way involving propaganda, espionage, subversion and cyber-attacks. Russia is at work across Europe and in the UK today. It is MI5's job to get in the way of that."

The interview came as the Investigatory Powers Bill, the so-called Snoopers’ Charter, returned to the House of Commons so MPs could consider amendments made by peers.

Security services will be given greater powers and be able to hack into computers, networks, mobile devices and servers under the proposed plans.

Earlier this year the Mail revealed how there are now more Russian spies trying to gather intelligence in Britain than at the height of the Cold War.

A former GCHQ official said foreign intelligence agents were trying to intercept secret communications between arms companies making deadly weapons, members of the Armed Forces and the Ministry of Defence.

Techniques they were using include sending code to mobile phones which allows them to turn the device into an eavesdropping device, monitoring all calls, and also text messages, he said.

LOAD-DATE: November 1, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Web Publication

JOURNAL-CODE: WEBDM

Copyright 2016 Associated Newspapers Ltd.
All Rights Reserved
### 3. Themes and sources of 2015

<table>
<thead>
<tr>
<th>theme</th>
<th>Ind</th>
<th>Gua</th>
<th>Mail</th>
<th>Mirror</th>
<th>Tele</th>
<th>Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>outline</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Q&amp;A</td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>oversight</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>need</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>reasonable powers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Paris attacks</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>urgency to pass powers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>crack down on bullies &amp; online abuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>concessions</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>encryption</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>browsing data / weblogs</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>hacking / interference obligations</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>risks of weakening tech security</td>
<td></td>
<td></td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>surveillance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>media complicity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>rushing through of bill</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>improper scrutiny allowed</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>data storage risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Chinese spy laws</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Tech firm gag-order</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

436
<table>
<thead>
<tr>
<th>source</th>
<th>Ind</th>
<th>Gua</th>
<th>Mail</th>
<th>Mirror</th>
<th>Tele</th>
<th>Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>The government (source)</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>government sources/officials</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whitehall official(s)</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>officials</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>minister(s)</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>former ministers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>senior sources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Home Office (official(s))</td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>political rivals</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Labour</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Cameron</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>May</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Burnham</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Starmer</td>
<td></td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Davis</td>
<td></td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ashdown</td>
<td></td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carlile</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Clegg</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lucas</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Vaz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Graham</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Shields</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Strasburger</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Carmichael</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Cartlidge</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Anderson</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>police</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GCHQ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>MI5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Internet experts</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>computer scientists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Technical experts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>Ind</td>
<td>Gua</td>
<td>Mail</td>
<td>Mirror</td>
<td>Tele</td>
<td>Times</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>--------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>ISPA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hare (ISP CEO)</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tech companies</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tech insiders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cook</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doctorow</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Foundation</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>civil liberties groups / campaigners</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>privacy groups / campaigners</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>critics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>opponents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Big Brother Watch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liberty</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Rights Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Snowden</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>National Union of Journalists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Cannataci (UN Privacy Chief)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Don’t Spy on US</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Ditch the Label</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>International community</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Chinese Gov’t</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>others</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Walker (techUK)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
4. Themes and sources of 2016

<table>
<thead>
<tr>
<th>theme</th>
<th>FT</th>
<th>Ind</th>
<th>Gua</th>
<th>Mail</th>
<th>Mirror</th>
<th>Tele</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>assent of bill</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>outline / recap</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Q&amp;A</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>need</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>protection / security</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>attacks</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>listing of agencies with access</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data storage risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>risks / threats of powers</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>criticisms / fears</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>opposition</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>petition for repeal</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>questions over key powers</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECJ ruling</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>risks of ECJ ruling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECJ - Brexit implications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>surveillance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>voice</td>
<td>FT</td>
<td>Ind</td>
<td>Gua</td>
<td>Mail</td>
<td>Mirror</td>
<td>Tele</td>
<td>Time</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>--------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>The government (source)</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>minister(s)</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home Office (official(s))</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Duncan-Smith</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cameron</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Davis</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rudd</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Cherry</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watson</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Abbott</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paddick</td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strasburger</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huppert</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anderson</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lawyers for gov't</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECJ</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>police</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Omand (former GCHQ)</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evans (former MI5)</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MI5</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security agencies</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>experts</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security experts</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN COO</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tech / internet companies</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tech giants</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>blogger/Uber manager</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Berners-Lee</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>civil liberties groups / campaigners</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>privacy groups / campaigners</td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>critics</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>opponents</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>voice</td>
<td>FT</td>
<td>Ind</td>
<td>Gua</td>
<td>Mail</td>
<td>Mirror</td>
<td>Tele</td>
<td>Time</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>--------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Big Brother Watch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liberty</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Open Rights Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snowden</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Privacy International</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Linklaters partner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>solicitor for Priv Int &amp; ORG</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
The tendency towards increased state surveillance of digital communications which grew significantly in the wake of the 2001 attacks on the United States, shows no sign of abatement. Indeed, the UK, while not alone in its continued governmental calls for legislation to serve the needs of security and law enforcement agencies in their work to maintain security, has recently passed an act which has been criticised on several fronts for offering unjustified levels of surveillance to a wide range of agencies. Amongst the most prominent criticisms of the Investigatory Powers Act, is the ruling by the European Court of Justice, who heard the case after it was referred following the UK government’s decision to appeal their high court defeat. The summary of the ruling, included a statement that the ‘general and indiscriminate retention of data’ proposed and enabled by the Act, ‘exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society’.

In light of this, and atop the initial UK ruling against the government’s proposed legislation, I was curious to explore the justification for the bill, and originally considered examining the debates within the House of Commons relating to the passage of the legislation from draft to enactment, in order to get a sense of the themes and rhetoric used to provide evidence for its necessity. However, amid the current debate over the veracity and trustworthiness of news media, and in keeping with a longstanding interest in both the shape and the influence of news reporting, I reconsidered the site of my proposed examination. Relocating this from inside the House of Commons, a site of discussion which is freely accessible to the public, to the UK national newspapers, a site whose aim is to variously inform the public and influence its opinion, seemed to offer a richer source of possible discourse, and a more fitting way to understand the shape of the arguments around the Investigatory Powers Act.

To this end, I will select reports from national UK newspapers and their websites, between the appearance of the draft version of the Act in November of 2015, through to the end of 2016, after passage into law in November of that year. The selected articles will be subjected to critical discourse analysis, in an attempt to identify common themes used in reporting, and any variation in themes across time and between sources; some critical theories on communication may also be drawn on in order to provide broader context for the analysis, and Floridi’s ideas on informational ethics may also be referred to. It is hoped that the analysis may
be able to uncover alternative ways of framing opposition to the legislation, which might prove to be more effective than the argument for the individual right to privacy, which can easily be deflected by the appeal to the necessity of protecting collective security.

The aim of the proposed research, is to carry out an analysis of articles published by UK national newspaper outlets, where the reporting is centred upon the Investigatory Powers Act. In doing so, it is hoped that several aspects of the media discourse on the legislation might be brought to light. First amongst these, is the degree of consistency that each individual publication displays in its way of reporting the bill, relative to its implicit and perceived political and ideological leaning. Second, is the extent to which the same, or similar, themes are prevalent in multiple sources, and whether this similarity is confined to publications with general ideological alignment, or whether it crosses such boundaries: this point will provide some evidence as to the possible range of viewpoints represented in the selected media outlets. Thirdly, will be a view of the reporting offered across the time from the publication of the draft bill, to its final enactment and the ensuing legal challenges brought against it. Here, we will see if there is any shift in how the newspapers position the legislation, either individually or collectively. Finally, when analysing the articles, it will be noted how the reporting is categorised, and in which section of the news it appears, e.g. as technology news, or political news, etc.

In carrying out this project, a clearer view of how national newspapers in the UK report on, and discuss the issue of surveillance is sought. The Investigatory Powers Act represents the broadest mandate for government and law enforcement agencies to indiscriminately collect data on all citizens of the UK, and as such, it is a piece of legislation whose impact might be felt by any individual. If the research provides some perspective on how this issue is framed by national news, a key source of information for the public as a whole, and especially those without a particular interest in the issues at stake, then it might also be able to suggest - with the assistance of theory on information, communication, and information ethics - ways in which opposition to the Act might be reframed, assisting in the challenge to limit surveillance powers.

The scope of the research proposed is limited to reporting in national UK newspapers, including articles published on their respective websites. It is expected that the publications included when searching for relevant material will be: The Daily Mail, The Sun, (in the case of these first two, the Scottish editions will also be included in any instances of divergent reporting), The Times, The Telegraph, The Guardian, The Independent, The Financial Times, and The Mirror. These publications all have national coverage and are therefore expected to have a widely accessed output, a significant influence over the shape of discourse and
opinion, or both. In addition, the choice of newspapers is intended to provide the potential for a diverse range of reporting, by its inclusion of both tabloid and broadsheet titles, and titles from across the spectrum from right to left leaning in terms of typical stance.

The articles will be drawn from three periods during the time frame of the Act’s draft appearance and its enactment as law, where search results for ‘investigatory powers’ in the relevant newspapers show significant peaks in the Factiva database’s monthly time line view. These peaks, relative to neighbouring months, come in November and December of 2015, February and March of 2016, and November and December of 2016, and it is from these periods that articles will be selected for analysis. Though not included in the analysis itself, I will aim to familiarise myself with the draft and final versions of the Act, as part of my background reading for the research.

The proposed project is one that builds upon some existing explorations of the meaning and the reach of modern state surveillance of communications and information accessed by individual citizens. The literature of relevance, so far, appears in journals covering the themes one would expect: those concerning themselves with journalism and the press (Bakir, 2015; Curran and Seaton, 2010; Kuehn, 2017; Wahl-Jorgensen, Bennett & Cable, 2017); data and society (Mills and Sarikakis, 2016); information and its communication (Lischka, 2017); the internet and related policy (Bernal, 2016; Hintz, 2016; McCarthy, 2016); and, of course, publications with a specific focus on discourse in society (Barnard-Wills, 2011; Branum and Charteris-Black, 2015; Tiainen, 2017) and surveillance (Lyon, 2007). Some LIS literature offers an additional view of the issue (Black and Schiller, 2014; Buschman, 2012; Mathiesen 2015), and from the perspective of information ethics, Floridi (1999; 2005; 2013), Budd (2006), and Ess (2010) each make valuable contributions. Additionally, there are writers on communication in society whose thinking might prove to be of service in giving the work broader theoretical grounding (Bourdieu, 1991; Fuchs, 2016; Habermas, 1989; Myles, 2010).

In analysing the construction and representation of the Investigatory Powers Act, there are, of course, numerous sources which might be selected as sites for fruitful examination - including the debates held within Parliament - but the choice to focus on news reporting of the passage of the Act from draft through to legislation, is grounded in two factors. First, this reporting serves as a much more broadly public facing source of discourse on the subject than would debates in parliament; and second, the potential impact of this output on public opinion is much greater. The potential for more varied framings of the issue also exist within the news, though it may well be found that a certain homogeneity of discourse exists. The research project will seek to link the resultant analysis of the source material, with the broad social context within which the issue of surveillance sits,
while also considering the current informational landscape as it applies to news and the responsibilities of media outlets, and the health of the infosphere.

The research will primarily use the method of critical discourse analysis that Fairclough (2015) sets out in Language and Power, though his other writings, alongside those of other prominent figures in the field, such as Wetherell, Taylor and Yates (2001), Wodak and Krzyżanowski (2008), and Wodak and Meyer (2011), will likely be relevant to forming the overall shape of the analysis. Taking entire texts as the important unit of language, the methodology offered by Fairclough lists questions that can be posed regarding the vocabulary used in the text under consideration, its grammar, and any other textual structures that are used. Through an examination of these elements of selected texts, it is hoped that it will be possible to say something about the knowledge and beliefs they contain and express; the social relationships they suggest or reflect; and the expressive tone used to convey the information of the text. Analysing the structures of texts as a whole tells us about the sequencing of events or elements, and their relationship to one another, as well as highlighting the elements of a report which are included, implied, or omitted.

Applying the analysis to newspaper reporting, a site of substantial power and influence, is intended to make explicit this power and the ways in which it is wielded by individual publications, and collectively, by ‘the news’ as a source of public information on matters. It is hoped that the research will expose some of the institutional strands of discourse that are used in news reporting: a term which of course implies an ideologically neutral process. While laying bare the ideology is useful in itself, proponents of critical discourse analysis also suggest that this can and should be taken further. A crucial step in such research is the application of results to offer the possibility of resistance to the power being asserted. In the case of this project, such resistance may come in the shape of alternative opposing discourses that might be used to make the case against blanket surveillance such as the legislation provides for.

The proposed plan for carrying out and writing up the dissertation project is as follows:

¥ More detailed background reading on the critical discourse analysis methodology: three weeks - 15/5 - 4/6
The resources necessary to the current research are primarily news articles published by the outlets specified in an earlier section of the proposal. It is expected that these will be drawn from either NexisLexis or Factiva databases, a choice that will be determined by the respective number and quality of search results delivered. These articles will provide the materials for analysis, alongside consideration of the self-positioning of respective outlets. In addition, and by way of context, the text of the Act, both in its draft form, and in its final, passed iteration will be used, as will some parliamentary debates during the passage of the Act from draft to legislation. These materials will be included as appendices.

No additional resources will be required.

The source material to be drawn upon for analysis is material that has been published by news organisations in the UK, and is therefore freely accessible. Background material, including the text of the Act itself, and transcripts of parliamentary debates of the Act, are also available from the website of Parliament. As such, no issues of confidentiality relate to the research, and no likely ethical concerns are anticipated.


Floridi, L. (2005), The Ontological Interpretation of Informational Privacy, Ethics and Information Technology, vol. 7, no. 4, pp. 185-200.


Kuehn, K. (2017), Framing mass surveillance: Analyzing New Zealand’s media coverage of the early Snowden files, Journalism,


Myles, J. (2010), Bourdieu, language and the media, Palgrave Macmillan, Basingstoke.

Tiainen, M. (2017), (De)legitimating electronic surveillance: a critical discourse analysis of the Finnish news coverage of the Edward Snowden revelations, Critical Discourse Studies


SAGE, London.

Wodak, R., & Krzyzanowski, M., (2008), Qualitative discourse analysis in the social sciences, Palgrave Macmillan, Basingstoke.