Freedom House

United Kingdom

	2014	2015
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	2	2
Limits on Content (0-35)	6	6
Violations of User Rights (0-40)	16	16
TOTAL* (0-100)	**24**	**24**

* 0=most free, 100=least free

Population:	**64.5 million**
Internet Penetration 2014:	**92 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2015 Status:	**Free**

Key Developments: June 2014 – May 2015

- In February 2015, English and Welsh law was amended to criminalize pornographic images distributed online without the subject's permission and with the intent to harm the subject, so-called "revenge porn." The law, which went into effect in April 2015, made the offense punishable by up to two years in prison, an increase from six months (see **Legal Environment**).
- In what seems to have been the first instance in the UK of a revenge porn prosecution, a 21-year-old was sentenced to 12 weeks in jail in November 2014 for threatening a woman and disseminating naked photographs of her without her permission via social media (see **Prosecutions and Detentions for Online Activities**).
- Alaa Esayed, an Iraqi national living in the UK, was charged with publishing and disseminating terrorist material via Twitter and Instagram in December 2014, resulting in a three-and-a-half-year prison sentence in June 2015. While she argued she was simply "cutting and pasting" other people's messages, the court held that their dissemination encouraged young people to travel to foreign countries in order to commit terrorist acts (see **Prosecutions and Detentions for Online Activities**).
- In February 2015, the Investigatory Powers Tribunal ruled that the Government Communications Headquarters (GCHQ) had acted unlawfully in accessing information on millions of individuals collected by its U.S. partner, the National Security Agency (NSA), prior to December 2014 (see **Surveillance, Privacy, and Anonymity**). As a result, Privacy International set up an online tool through which users can ask the tribunal if the GCHQ has illegally monitored their activities (see **Digital Activism**).
- Shortly after the terrorist attacks in Paris in January 2015, Prime Minister David Cameron called for a ban on encryption in messaging apps. While the move was met with criticism from internet freedom and security activists who argued that it would be highly impractical, the government continued its plans and put forward a draft investigatory powers bill, dubbed the "snoopers' charter" by activists (see **Surveillance, Privacy, and Anonymity**).

Introduction

Online harassment, extremist speech, and privacy were the three main issues seen in internet policy in the United Kingdom (UK) over the past year. The UK was an early adopter of new information and communication technologies (ICTs), and internet access in the country has become near universal with competitive prices and generally fast speeds. Internet access through mobile phones is also becoming more prevalent as a result of the growing popularity of smartphones and the increasing availability of superfast networks. But the growth in technological capacities has simultaneously allowed expanded surveillance, leading to mounting fears of abuse by police and intelligence agents.

In February 2015, the Investigatory Powers Tribunal ruled that the Government Communications Headquarters (GCHQ) had acted unlawfully in accessing information collected by its U.S. partner, the National Security Agency (NSA), prior to December 2014—before the GCHQ practices were made public. The decision marked the first time the tribunal has ruled against any of Britain's three intelligence agencies—GCHQ, MI5, and MI6—that it is entrusted to oversee.

In another positive development, a government-commissioned report released in June 2015 found that the existing legislative framework on surveillance was "undemocratic, unnecessary and—in the long run—intolerable." David Anderson QC, the author of the report, recommended halting any new legislative proposals on surveillance until they were assessed for "lawfulness, likely effectiveness, intrusiveness and cost." However, continued statements by Prime Minister David Cameron highlight the government's worries over improved encryption standards. The new director of GCHQ referred to U.S. technology companies such as Twitter, Facebook, and WhatsApp as "command-and-control networks…for terrorists and criminals" and called for greater cooperation between companies and security agencies.[1]

Obstacles to Access

Access to the internet is considered to be a key element determining societal and democratic participation in the United Kingdom (UK).[2] ICT infrastructure in the country is generally strong, allowing high levels of access: the overwhelming majority of UK citizens use the internet frequently on a widening variety of devices. In recent years there have been substantial investments in superfast broadband, led by the government's Rural Broadband Programme,[3] which has led to better levels of service for many citizens and businesses. For financial and literacy reasons, however, there is still a small segment of the population that does not have internet access, specifically those over 75 and people in the lowest socioeconomic groups.[4] Policies and regulation in the country tend to favor access, although continuing revelations regarding extensive government surveillance practices may impact how citizens choose to access the internet.

1 "GCHQ's Robert Hannigan says tech firms 'in denial' on extremism," BBC News, November 4, 2014, http://www.bbc.com/news/uk-29891285.

2 Ofcom, *Internet Citizens 2014* (London: Ofcom), November 27, 2014, http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/Internet_Citizens_Report_14.pdf, p 1

3 Department for Culture, Media and Sport (DCMS), *2010 to 2015 government policy: broadband investment*, updated May 8, 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-broadband-investment

4 Ofcom, *Internet Citizens 2014*, p.11

Availability and Ease of Access

Internet penetration has grown to 85 percent as of early 2015, with the share of homes with fixed and mobile broadband at 80 percent.[5] Three in ten of all broadband connections are labeled as "superfast," meaning they have an advertised speed of at least 30 Megabits per second (Mbps).[6] Nearly 100 percent of all households are within range of ADSL connections. The government's Rural Broadband Programme has now been incorporated within a larger Superfast Broadband Programme, and funding expanded to GBP 1.7 billion (US$ 2.62 billion) aimed at improving broadband speed and access.[7] As of March 2015, an additional 2,411,395 premises had access to superfast broadband through the scheme, meaning a total of 80 percent of all UK premises had superfast broadband access availability, in line with a target of 95 percent by 2017.[8] So, while broadband access is effectively ubiquitous, steady progress continues towards the aim of superfast broadband in all areas, which is a stated priority.[9]

Mobile telephone penetration is extensive, with a reported penetration rate of 123.58 percent at the end of 2014.[10] In 2014, 66 percent of all UK adults claimed to own a smartphone, reflecting a substantial growth of internet use on mobile phones.[11] The fastest growth in mobile internet use was among people aged 55 to 64, which increased more than five-fold in four years. Fourth-generation (4G) mobile communication technology is now available from all four national mobile network operators, with more than 23 million subscriptions and over 89 percent of UK premises being able to access outdoor 4G coverage from at least one network.[12] Second-generation (2G) and third-generation (3G) networks are available in over 99 percent of all households. At 33 percent, smartphones were the most important device for internet access as of mid-2015, surpassing laptops (30 percent) and tablets (19 percent).[13]

Even where access is available, use and participation does not necessarily follow. Citizens with internet access may choose not to participate if they lack technical understanding or adequate equipment, if they are concerned about privacy online, or if they have no interest in being online. People in the lowest income groups are significantly less likely to have home internet subscriptions, with the gap between socioeconomic groups remaining the same for the past few years. People aged 75 and above are also less likely to use the internet, although internet use by this group has increased since 2008.[14] Of the UK households that do not have access to the internet, the majority have no intention to get connected.[15] There is a no gender gap in internet use.

5 Ofcom, *The Communications Market Report*, August 6, 2015, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr15/CMR_UK_2015.pdf, p.340

6 Ofcom, *The Communications Market Report,* August 6, 2015, p3

7 DCMS, *2010 to 2015 government policy: broadband investment*, Appendix 2

8 DCMS, *2.5 million more UK homes and businesses can now go superfast*, https://www.gov.uk/government/news/25-million-more-uk-homes-and-businesses-can-now-go-superfast

9 For local area progress in broadband provision, see DCMS*, Table of local broadband projects*, October 2014, https://docs.google.com/spreadsheet/ccc?key=0Ah3sVRjT82kKdEltX0lJNjNVWWhNbjBnNGwxeHhqMHc#gid=0

10 International Telecommunication Union , *Mobile-cellular subscriptions 2000-2014*, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspxhttp://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx

11 Ofcom, *The Communications Market Report*, August 6, 2015, p.339

12 Ofcom, *The Communications Market Report*, August 6, 2015, p.1

13 Ofcom, *The Communications Market Report*, August 6, 2015, p.346

14 Ofcom, *The Consumer Experience of 2013: Research Report,* p.22–26

15 Ofcom, *The Communications Market Report*, August 6, 2015, p.352

The average broadband speed in November 2014 was 22.8 Mbps,[16] continuing a trend of rising speeds and growing satisfaction among consumers served by faster fiber-optic based services. The introduction of 4G services for mobile in 2012 has allowed faster data downloads and uploads, streaming of video, and access to other data services. A total of 61 percent of adults said they used data services on their mobile phones, a four percent increase from 2014.[17] The 7.1 million fixed broadband lines providing speeds of 30 Mbps or higher in the UK today account for 30 percent of all fixed broadband lines, compared to 0.2 percent in 2009.[18] Superfast connections are increasingly deployed beyond the major urban centers, and the price of such connections is decreasing.[19]

The UK provides a competitive market for internet access, and prices for communications services compare favorably with those in other countries.[20] Average fixed internet spending has continued to increase as a result of a growth in broadband uptake and the rise of superfast services. While 4G services were initially more expensive than non-4G services, the difference is shrinking, and in some cases disappearing. The price basket of mobile services continues to fall in real terms, specifically by 0.4 percent in 2014, and is around GBP 14.30 (US$ 21.90).[21] The difference between superfast and standard services in 2014 was between GBP 5 (US$7.66) and GBP 10 (US$15.31) per month.[22]

Economic constraints do appear to negatively impact older and poorer users' ability to participate online. While 85 percent of the UK population has access to internet in their homes, as of 2014 only 63 percent of individuals over the age of 65 use the internet, and among those in the lowest socio-economic group, including the unskilled manual labourers and long-term state dependents, only 64 percent self-describe as internet users.[23]

Restrictions on Connectivity

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to direct government control. ISPs regularly engage in traffic shaping or slowdowns of certain services (such as peer-to-peer file sharing and television streaming), and can also be made to block-access to specific sites via court orders. Mobile providers have cut back on previously unlimited access packages for smartphones, reportedly because of concerns about network congestion.

ICT Market

The five major internet service providers (ISPs) are British Telecom (BT) with a 32 percent market share, Sky (22 percent), Virgin Media (20 percent), TalkTalk (14 percent), and EE (4 percent).[24] Through local loop unbundling—where communications providers offer services to households using infrastructure provided mainly by BT and Virgin—a large number of companies provide internet

16 Ofcom, *The Communications Market Report*, August 6, 2015, p.15
17 Ofcom, *The Communications Market Report*, August 6, 2015, p.340
18 Ofcom, *The Communications Market Report*, August 6, 2015, p.15
19 Ofcom, *The Communications Market* 2014, p 346.
20 Ofcom, *The Consumer Experience of 2013: Research Report*.
21 Ofcom, *The Communications Market Report*, August 6, 2015, p.317
22 Ofcom, *The Communications Market 2014*, p 311.
23 http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/Internet_Citizens_Report_14.pdf
24 Ofcom, *The Communications Market Report*, August 6, 2015, p.292

access. By 2013, unbundled telephone lines reached 9 million homes.[25] Virgin has the highest share of superfast broadband subscribers at 56 percent as of 2014; BT has a 35 percent share, but is dominant in the provision of wholesale access.[26] ISPs are not subject to licensing but must comply with general conditions set by the communications regulator, Ofcom, such as having a recognized code of practice and being a member of a recognized alternative dispute-resolution scheme.[27]

The telecommunications provider O2 leads the mobile operator market, with some 22 percent of market, followed by Vodafone (19 percent), Orange (11 percent), and Three (3) (10 percent) according to information from Statista as of 2014.[28]

Regulatory Bodies

Ofcom is the primary regulator, by virtue of the broad definitions of responsibility for "citizens," "consumers," and "communications matters" granted to it under the Communications Act 2003.[29]

In July 2012, major ISPs published a "Voluntary Code of Practice in Support of the Open Internet".[30] The code commits ISPs to transparency and confirms that traffic management practices will not be used to target and degrade the services of a competitor. The code was amended in May 2013 to clarify that signatories could deploy content filtering or provide such tools where appropriate for public Wi-Fi access.[31]

In September 2013, the domain registrar Nominet launched a review of the ".uk" domain registration policy to focus on the extent to which it should restrict offensive or otherwise inappropriate words or expressions in domain name registrations.[32] The Nominet Board agreed to all the recommended changes,[33] which included a post-registration domain name screening to suspend or remove domain names that encourage serious sexual offenses.[34]

In addition, the Internet Watch Foundation (IWF), an independent self-regulatory body funded by the EU and the online industry, provides a UK internet hotline for the public and IT professionals to report criminal online content in a secure and confidential way.[35] A range of other self-regulatory bodies—for example, the Video On Demand Association, a private self-regulatory body with responsibility for regulating video content in keeping with the EU AudioVisual Media Services Directive, the

25 Ofcom, "UK broadband competition reaches new milestone," April 25, 2013, http://media.ofcom.org.uk/2013/04/25/uk-broadband-competition-reaches-new-milestone/.

26 Ofcom, *The Communications Market* 2014, p 311.

27 Ofcom, *Consolidated Version of General Conditions of Entitlement* (London: Ofcom), December 16, 2013, http://stakeholders.ofcom.org.uk/binaries/telecoms/ga/GENERAL_CONDITIONS_AS_AT_26_DECEMBER_2013.pdf.

28 "Market share held by mobile operators in the United Kingdom (UK) as of June 2014," Statista, 2014, http://www.statista.com/statistics/375986/market-share-held-by-mobile-phone-operators-united-kingdom-uk/.

29 Communcations Act 2003, Part 1, Section 3, http://www.legislation.gov.uk/ukpga/2003/21/contents

30 Broadband Stakeholder Group, "ISPs launch Open Internet Code of Practice," July 25, 2012, http://www.broadbanduk.org/2012/07/25/isps-launch-open-internet-code-of-practice/.

31 Broadband Stakeholder Group, "ISPs launch Open Internet Code of Practice," May 2013, http://www.broadbanduk.org/wp-content/uploads/2013/06/BSG-Open-Internet-Code-of-Practice-amended-May-2013.pdf.

32 Nominet is the domain registrar in the United Kingdom, and manages access to newly introduced .uk, .wales, and .cymru domains.

33 Lord Macdonald QC, *Review of .uk Registration Policy*, December 2013, http://www.nominet.org.uk/sites/default/files/Lord%20Macdonald%20Report%20final.pdf.

34 Nominet, "Nominet to update registration policy in light of Lord Macdonald review," 15 January 2014, http://www.nominet.org.uk/news/latest/nominet-update-registration-policy-light-lord-macdonald-review.

35 The Internet Watch Foundation, https://www.iwf.org.uk/

Advertising Standards Authority, and IPSO, which regulates newspaper websites—apply a combination of voluntary ethical codes and co-regulatory rules to internet content. With the exception of the filtering and blocking blacklists dealing with child abuse content (which are agreed upon by the IWF) these bodies eschew pre-publication censorship and operate post publication notice and takedown procedures within the E-Commerce Directive liability framework.

Limits on Content

The United Kingdom has no blanket laws covering internet blocking but various categories of criminal content such as depictions of child sexual abuse, promotion of extremism and terrorism, and copyright infringing materials are blocked by ISPs using filtering tools. Meanwhile parental controls over adult-oriented sites have become the default, requiring adults to opt-out of the filtering technology to access adult material. These measures have been considered controversial as they often result in over-blocking, and a lack of transparency persists regarding the sites blocked.

Blocking and Filtering

The government has thus far taken a proactive approach to restricting sites that have been found in violation of copyright protections, indicating possible further action to curb infringement.[36] The UK High Court blocks sites based on copyright violations, but it recently held that publishing a link to copyright infringing material, rather than actually hosting it, does not amount to an infringement. This approach was confirmed by the Court of Justice of the European Union. There have been a number of cases in which courts have ordered sites, such as Newzbin and The Pirate Bay, to be blocked for infringing copyright, and to have their domain names seized based on legislation like the Copyright, Designs, and Patents Act.

The CleanFeed system has also been expanded so the blocks can be enforced by ISPs. The list of violating websites has been growing continually. The Digital Economy Act (DEA) of 2010 states that a court order can block sites containing "substantial" violations of copyright. However, as a response to an Ofcom review, which determined that such copyright-related blocking provisions, stipulated in Sections 17 and 18 of the DEA, are unlikely to be effective alone and should rather be used in conjunction with other measures, representatives from the UK's creative industries and major Internet Service Providers (ISPs) have come together with the support of government to launch Creative Content UK.[37]

Creative Content UK was launched in Spring 2015, and comprises a major multi-media education awareness campaign, that aims to create wider appreciation of the value and benefits of entertainment content and copyright. The second component is a subscriber alerts program that will be co-managed and co-funded by ISPs and content creators and is due to begin at a later date.[38] The UK's Department for Culture, Media and Sport (DCMS) has indicated that the program will replace the unfavorable anti-piracy regime rushed through under the DEA where the Secretary of State for

36 Sajid Javid's speech at British Phonographic Industry AGM, Department for Culture, Media and Sport, 1 September 2014, http://bit.ly/1atulAP

37 UK ISPs and rights holders' programme to tackle online piracy "imminent", World Intellectual Property review, 12 May 2014, http://bit.ly/1ec7PO9

38 UK CREATIVE INDUSTRIES AND ISPS PARTNER IN MAJOR NEW INITIATIVE TO PROMOTE LEGAL ONLINE ENTERTAINMENT, British Phonographic Industry, 26 June 2015, http://bit.ly/1mqxeAd

Culture, Media and Sport is able to facilitate "blocking injunctions" by the courts in order to force ISPs to block access to pirated copyright content.[39] Nonprofit groups like Open Rights Group (ORG) had criticized regulatory reliance on the DEA approach, as obtaining copies of the copyright injunctions has proved challenging. Consequently, ORG has called for more transparency about what sites are blocked by court injunctions.

UK blocking policy is instituted in accordance with a voluntary code of practice set forth by the Internet Services Providers' Association. British ISPs are not required by law to implement the IWF blocking list, however since 2010, the Home Office has instituted rules prohibiting government bodies from working with ISPs that fail to use the list. Consumer awareness of CleanFeed remains low, with the list of blocked sites kept from the public in an effort to deter access to unlawful materials. In January 2014, a human rights audit of the IWF recommended that an independent judicial review of IWF's operations be conducted.

In November 2013, Google and Microsoft introduced new algorithmic filters that prevent searches for child abuse imagery. Around 100,000 terms for illegal material are programmed to yield no search results. At the same time, laws like the Protection of Children Act are used to prosecute individuals suspected of accessing or distributing content containing sexual abuse of children. According to reports by civil society groups, the filters raise transparency concerns and evade reporting requirements under the Freedom of Information Act, particularly regarding how these filters work and why certain sites may be blocked without court orders.

In the face of rapidly increasing mobile uptake in the UK, mobile filtering has also become increasingly prevalent. Concerns have also grown over the unsupervised use of data-enabled mobile phones by children under the age of 18, which has led to mobile internet subscriptions being sold to customers with child filters enabled by default, and access to adult content requiring users to verify their age to 'opt-in'. The May 2015 elections featured commitments made by the Conservative Party, which won a parliamentary majority, to strengthen internet porn filters.[40] Blocked content categories, which include pornography, hate sites, and in some cases, web forums that could potentially allow minors to interact with older users, are set out in the 2004 code of conduct established by the Mobile Broadband Group (MBG), consisting of the providers Vodafone, Three, EE, and O2. The code of conduct, last updated in July 2013, covers commercial and internet content, illegal content, malicious communications, and customer education. In September 2013 the British Board of Film Classification (BBFC) replaced the Independent Mobile Classification Body (IMCB) in categorizing content and calibrating internet filters. However, the process continues to be criticized for being too subjective and lacking transparency.

In November 2013, Sky, TalkTalk, BT, and Virgin led a joint awareness campaign around child safety, launching the InternetMatters.org portal in May of 2014 with the aim to provide parents with advice regarding children's online safety. The efficacy of these child-protection measures for filtering content on both mobiles and household access has been questioned. They can not only be easily circumvented with minimal effort, but have been known to lead to the over-blocking of legitimate content. For example, due to technical glitches at the ISP level, users were barred from accessing popular sites such as Wikipedia. In response, ORG created the site "Blocked.org.uk" to allow users to report over-blocking of content that poses little or no threat to child welfare, including sites on

39 'ISPs collaborate with music and film industries on voluntary scheme to combat online piracy," SnIPPts, 13 May 2014 http://bit.ly/1KmteCI

40 'Tories promise to enforce age limits on online pornography', *The Guardian*, April 4, 2015, http://bit.ly/1atulAP

sexual education, homosexuality and drug awareness, and pages run by civil society and political parties. The website of the British National Party, an extreme right-wing political organization, was temporarily blocked for being classified by O2's filter system as a "hate site." As O2 is the only large ISP that operates an "URL checker" page that allows users to ascertain how a particular site has been classified, genuine concerns arise around owners and operators of sites not being notified that their sites have been blocked. ORG reports that some cases of sites blocked on mobile networks have taken a month to be resolved, and that site operators often do not know where to report a wrongfully blocked site.

Content Removal

The government has stepped up efforts to curb radicalization on the internet. The Terrorism Act calls for the removal of material hosted online in the UK if it "glorifies or praises" terrorism, could be useful to conducting terrorism, or incites people to carry out or support terrorism. A Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials and take down instances of "jihadist propaganda." The government updated its "Prevent Anti-Terrorism Strategy" in 2015, which calls for limiting access to "extremist" materials online through school and public library networks and increasing efforts to remove "harmful content" from the internet. The strategy involves "sharing unlawful sites for inclusion in commercial filtering products," through the compiling of a list of extremist URLs by the CTIRU that are then blocked by ISPs.[41] (see also, "Blocking and Filtering" above.)

The Internet Watch Foundation (IWF) compiles a blacklist of URLs with visual depictions of child sexual abuse to prevent access to such illegal content. A citizen's hotline combined with investigations by IWF analysts in accordance with the Sexual Offences Definitive Guideline published by the Sentencing Council under the Ministry of Justice is used to discover and evaluate illegal sites. When the content in question is hosted by UK servers, where this constitutes a criminal offense, the IWF coordinates with the police and local hosting companies to remove it. A similar system exists for websites containing child sexual abuse through non-photographic means, such as computer-generated images, as well as for websites with criminally obscene adult content.

For content that is hosted by overseas servers, the IWF coordinates with international hotlines and police authorities to get the offending content taken down in the host country. In the meantime, British users are prevented from accessing content deemed illegal by British ISPs using the CleanFeed filtering system, which was developed by the IWF and BT. Similar processes are in place for the investigation of online materials inciting hatred under the oversight of TrueVision, a site that is managed by the police.

According to the EU 2002 E-Commerce Directive, knowledge of illicit material, including libelous content, on a host website in conjunction with a failure to remove it is prosecutable. This has resulted in hasty takedowns by hosting companies, with little inquiry as to the legitimacy of the takedown notice. In April 2013, the government updated the Defamation Act. The updates came into effect on January 1, 2014, and provide greater protections for ISPs by limiting their liability for user-generated content.

41 "2010 to 2015 government policy: counter-terrorism," Gov.UK, May 8, 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-counter-terrorism/2010-to-2015-government-policy-counter-terrorism.

Although EU rather than UK-specific, the so-called "right to be forgotten" ruling from the European Court of Justice in May 2014, which gave search engines the task of removing links from their search results on the requests of individuals if the stories in question were deemed to be inadequate or irrelevant, has had an impact on the way content is handled in the country. According to Google's Transparency Report on European privacy removal requests,[42] Google had received 35,140 requests by July 2015, requesting the removal or 137,955 URLs from its search results. The rate of compliance was 37.5 percent. News publishers including the BBC[43] and the Telegraph[44] have retaliated by publishing lists of the stories which had been delisted by search engines. In May 2015, it was reported that the Information Commissioner's Office was in talks with Google over 48 cases that it believed the search engine had not resolved effectively.[45]

Media, Diversity, and Content Manipulation

Self-censorship is difficult to measure in the United Kingdom, but not a grave concern. After the January 2015 attack on the French publication Charlie Hebdo some publications refrained from publishing the controversial cartoons of the prophet Muhammad,[46] but these were not government influenced or mandated. Due to the UK's extensive surveillance practices, it is possible that certain online groups feel as though they must self-censor to avoid potential government interference.

In June 2015 the UK's Investigatory Powers Tribunal confirmed that GCHQ had been unlawfully surveilling NGOs, including Amnesty International and Legal Resources Center in South Africa.[47] The tribunal made "no determination" on the claims brought by other NGOs, including Liberty and Privacy International, which could mean either that GCHQ is not surveilling the two NGOs, or that the surveillance has been deemed lawful. Representatives from Amnesty International, Privacy International, and Liberty alluded to the possibility of self-censorship by stating that they could not appropriately do their job under such conditions of surveillance.[48]

Other than surveillance, and the government's role in encouraging the filtering activities described above, there is no explicit evidence relating to the government manipulation of online content. Online media outlets face economic constraints that negatively impact their ability to remain financially sustainable. Publications have struggled to find a profitable system for their online news platforms as ad revenue continues to fall.

The UK telecoms regulatory, Ofcom, adopted a voluntary code of practice on broadband speeds in 2008 and released a report in 2011 that called for a self-regulatory approach to network neutrality.[49] It described the blocking of services and sites by ISPs as "highly undesirable" but said that market

42 Google Transparency report, https://www.google.com/transparencyreport/removals/europeprivacy/ Accessed July 7 2015

43 Neil MacIntosh, List of BBC web pages which have been removed from Google's search results, BBC Internet Blog, June 25 2015 http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379

44 Rhiannon Williams, Telegraph stories affected by EU 'right to be forgotten', *The Telegraph*, July 2 2015 http://www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html

45 Kevin Rawlinson, Google in 'right to be forgotten talks with regulator', *BBC News*, 13 May 2015 http://www.bbc.co.uk/news/technology-32720944

46 http://www.politico.com/blogs/media/2015/01/news-orgs-censor-charlie-hebdo-cartoons-after-attack-200709.html#.VK18tMDFVi5.twitter

47 http://www.theguardian.com/uk-news/2015/jun/22/gchq-surveillance-two-human-rights-groups-illegal-tribunal

48 http://rt.com/uk/271111-gchq-amnesty-international-spy/

49 Ofcom, *Ofcom's approach to net neutrality*, November 11, 2011, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/.

forces will address potential problems.[50] Developments at European Union (EU) level are likely in the future to have an impact on net neutrality provisions in the UK, after agreement has been reached to ban paid prioritization across the EU as part of the Digital Single Market policy package.

There are a wide variety of news platforms available online, with 60 percent of people reporting that they consume news online, and 44 percent reporting that they consume news through apps. Blogs and social media also act as available news sources, but have seen a readership decline by four points to 23 percent. Diverse views are present online, but may not be widely read, as 59 percent obtain their news from the BBC website or app, 18 percent obtain their news through Google, and 17 percent obtain their news through Facebook.[51]

Digital Activism

Online political mobilization continues to grow both in terms of numbers of participants and numbers of campaigns, though the efficacy of online mobilization remains controversial and it is impossible to explain success with reference to online campaigns alone. Petition and advocacy platforms such as 38 Degrees and AVAAZ continued to grow, with AVAAZ claiming around 1.6million "members" in 2015 in the UK. All civil society organizations, charities and political parties now view online as an indispensable part of a wider campaign strategy.

As a result of Privacy International's case against the Investigatory Powers Tribunal (IPT), British citizens are now able to find out if they were illegally spied on by applying directly to the IPT, which is obligated to respond to any complaints and reveal if an individual was illegally monitored.[52] If so, the individual can ask that the data be deleted. Privacy International has made this process even more accessible, by providing a form on its website for applicants, which it will submit on their behalf and fight in any resulting court battles. More than 6,000 people signed up in the first 24 hours after the form was launched, which topped 10,000 in the first two days.[53]

Violations of User Rights

The government has placed significant emphasis on stopping the dissemination of terrorist and hate speech online and on protecting individuals from targeted harassment on social media. While, changes to civil liability laws implemented through the Defamation Act 2013 were meant to relieve content producers and website operators of the burden of ever-looming threats of libel action, the benefits have so far seemed unrealized. Furthermore, users' rights still seem caught in the shadow of extensive surveillance measures used by the government to monitor the flow of information for law enforcement and foreign intelligence purposes. There were several notable legal changes over the past year in these areas.

50 . See http://ec.europa.eu/digital-agenda/en/eu-actions. ; https://ec.europa.eu/commission/2014-2019/ansip/blog/making-eu-work-people-roaming-and-open-internet_en

51 http://stakeholders.ofcom.org.uk/binaries/research/tv-research/news/2014/News_Report_2014.pdf

52 http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa

53 http://www.theguardian.com/technology/2015/mar/03/gchq-tech-giants-fight-for-personal-data

Legal Environment

The UK currently has no constitution or bill of rights, relying instead on the provisions of the European Convention on Human Rights (ECHR), which have been adopted into law via the Human Rights Act 1998. However, in the fall of 2014, Conservative Party officials, including the prime minister, announced their intentions to repeal the Human Rights Act in favor of a UK Bill of Rights in order to give British courts more control over application of human rights principles.[54] Furthermore, following the election of a Conservative government in May 2015, the prime minister reiterated his position that he remains open to withdrawing from the ECHR entirely should parliament not successfully secure the ability to veto decisions of the European Court of Human Rights.[55]

In September 2015, with a new government in office after the general elections that year, the home secretary outlined a proposal for "extremism disruption orders".[56] The orders would allow judicial review of individuals and groups who "spread hate but do not break laws," disallowing them from posting messages to social media without first gaining government approval.[57] While much discussion has centered around combating terrorism, officials have noted that the orders could be used to limit speech of those groups found to disseminate hatred based on gender, sexual orientation, religion, and disabilities. That proposal, supported by the prime minister, also included plans to grant Ofcom, the broadcast and telecommunications regulatory authority, powers to prevent broadcast of "extremist messages," requiring pre-transmission monitoring of content.[58] However, this proposal has met vocal opposition even from within the Conservative Party, including at least four cabinet ministers in the newly elected government.[59]

Beyond targeting extremist and hate speech, the UK has focused on online harassment as well. In February 2015, the Criminal Justice and Courts Act 2015 amended section 1 of the Malicious Communications Act 1988 to quadruple the possible time in prison to two years in the case of targeting individuals with abusive and offensive content online "with the purpose of causing distress or anxiety."[60] The new law, effective in England and Wales only, opened the crown court for more serious offenses, whereas previously only the magistrates' courts may hear such cases.[61] The changes also extended the time limit to bring charges for these offenses to three years from the date of the of-

54 Oliver Wright, "David Cameron to 'scrap' Human Rights Act for new 'British Bill of Rights,'" The Independent, Oct. 1, 2014, http://www.independent.co.uk/news/uk/politics/conservative-party-conference-cameron-announces-plans-to-scrap-human-rights-act-9767435.html.

55 Nicholas Watt, "David Cameron prepared to break with Europe on human rights," The Guardian, June 2, 2015, http://www.theguardian.com/politics/2015/jun/02/david-cameron-prepared-to-break-with-europe-on-human-rights.

56 Alan Travis, "What are Theresa May's new 'extremism disruption orders,'" The Guardian, Sept. 2014, http://www.theguardian.com/politics/2014/sep/30/theresa-may-extremism-disruption-orders.

57 John Bingham, "Sharia law or gay marriage critics would be branded 'extremists' under Tory plans, atheists and Christians warn," The Telegraph, Oct. 31, 2014, http://www.telegraph.co.uk/news/politics/11202290/Sharia-law-or-gay-marriage-critics-would-be-branded-extremists-under-Tory-plans-atheists-and-Christians-warn.html.

58 Rowena Mason and Alan Travis, "David Cameron backs proposal to block extremist messages on TV," The Guardian, May 22, 2015, http://www.theguardian.com/politics/2015/may/22/david-cameron-backs-plans-ofcom-block-extremist-messages-tv-censorship.

59 Alan Travis, "It wasn't just Lib Dems who opposed Theresa May's counter-extremism plans," The Guardian, May 13, 2015, http://www.theguardian.com/world/2015/may/13/theresa-mays-counter-extremism-proposals-are-fraught-with-difficulties.

60 Ministry of Justice and The Rt Hon Chris Grayling MP, "Internet trolls to face 2 years in prison," Gov.uk, Press Release, Oct. 20, 2014, https://www.gov.uk/government/news/internet-trolls-to-face-2-years-in-prison.

61 "Internet trolls face up to two years in jail under new laws," BBC.co.uk, Oct. 19, 2014, http://www.bbc.co.uk/news/uk-29678989.

fense.[62] An act also amended English and Welsh law to criminalize revenge porn."[63] The law, which went into effect on April 13, 2015, makes the offense punishable by up to two years in prison, an increase from six months under provisions in the Malicious Communications Act and the Protection from Harassment Act.[64]

Going further, though, in order to combat such trolling, revenge porn, and other such cyber-bullying, a House of Lords committee recommended in a July 2014 report that websites allowing individuals to post content should be required to establish the actual identity of such individuals beforehand before permitting them to post under a pseudonym or anonymously.[65] Critics argue that such a measure would chill important speech by removing the protections of anonymity from those otherwise afraid to speak.[66] While no specific action on this report's recommendation has been taken, the Defamation Act 2013 offers protection to website operators from private libel suits based on third-party postings only if the alleged victim of defamation can find the user.[67] While the act does not specify what sort of information the website operator must provide to plaintiffs, unauthenticated identity information may be falsified by users and prevent the operator from benefiting from the act's liability protections, thus placing website operators in the position of requiring authenticated identity information or risk civil liability.[68]

The Defamation Act 2013 was intended to reduce the amount of libel travel that has led to a large number of libel suits with only tenuous connection to the UK being brought in its courts, with relevant sections becoming active in January 2014 that require claimants to prove that England and Wales is the most appropriate forum for the action, set a serious harm threshold for claims, and codify certain defenses such as truth and honest opinion. Such "libel tourism" had a chilling effect on the speech of content producers and ISPs in the UK. However, the number of such claims brought in London increased by 60 percent from 2013 to 2014, resulting in the highest figure since 2009.[69] While the reason for the increase is unclear, one cause could be a number of suits seeking the courts' clarification of the meaning and scope of the changes to the Act.[70]

In a positive move, new exceptions to copyright protections came into force in October 2014. The

62 Ministry of Justice and The Rt Hon Chris Grayling MP, "Internet trolls to face 2 years in prison," Gov.uk, Press Release, Oct. 20, 2014, https://www.gov.uk/government/news/internet-trolls-to-face-2-years-in-prison.

63 "'Revenge porn' illegal under new law in England and Wales," BBC.co.uk, Feb. 12, 2015, http://www.bbc.co.uk/news/uk-31429026.

64 Louise Ridley, "Revenge Porn Is Finally Illegal: Who Are The Victims And Perpetrators Of This Growing Phenomenon?," The Huffington Post, March 12, 2015, http://www.huffingtonpost.co.uk/2015/04/12/revenge-porn-law_n_6630730.html.

65 Communications Committee – First Report: Social media and criminal Offences, House of Lords, July 22, 2014, ¶54, http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3704.htm#a14.

66 *E.g.*, Danny O'Brien, UK's Lords and EU Take Aim at Online Anonymity, Electronic Frontier Foundation, 5 Aug. 2014, https://www.eff.org/deeplinks/2014/08/uks-lords-and-eu-take-aim-online-anonymity.

67 Mike Masnick, "Did UK Gov't Already effectively Outlaw Anonymity Online With Its New Defamation Law?," TechDirt, Aug. 11, 2014, https://www.techdirt.com/articles/20140807/17234928145/did-uk-govt-already-effectively-outlaw-anonymity-online-with-its-new-defamation-law.shtml.

68 Eric Goldman, "UK's New Defamation Law May Accelerate The Death of Anonymous User-Generated Content Internationally," Forbes, Sept. 9, 2014, http://www.forbes.com/sites/ericgoldman/2013/05/09/uks-new-defamation-law-may-accelerate-the-death-of-anonymous-user-generated-content-internationally/; Mike Masnick, "Did UK Gov't Already effectively Outlaw Anonymity Online With Its New Defamation Law?," TechDirt, Aug. 11, 2014, https://www.techdirt.com/articles/20140807/17234928145/did-uk-govt-already-effectively-outlaw-anonymity-online-with-its-new-defamation-law.shtml.

69 Judicial Statistics: 2014, Defamation claims increase by 60%, the highest number since 2009, 9 June 2015, Inforrm (blog), https://inforrm.wordpress.com/2015/06/09/judicial-statistics-2014-defamation-claims-increase-by-60-the-highest-figure-since-2009/.

70 "Online platforms face growing risk of defamation claims, says expert," Out-Law.com (blog), June 16, 2015, http://www.out-law.com/en/articles/2015/june/online-platforms-face-growing-risk-of-defamation-claims-says-expert/.

new intellectual property framework included exceptions for making personal copies of protected work for private use, as well as for "parody, caricature and pastiche."[71]

Prosecutions and Detentions for Online Activities

In what seems to have been the first instance in the UK of a revenge porn prosecution, the Crown Prosecution Service (CPS) charged 21-year-old Luke King for disseminating via social media naked photographs of a woman without her permission and making threats to her.[72] The man pleaded guilty and was sentenced in November 2014 to 12 weeks in jail.[73]

The Crown Prosecution Service (CPS) had published amended guidelines in October 2014 instructing that the most serious of harassment offenses should be prosecuted under the Sexual Offences Act 2003, carrying a maximum of 14 years in prison where the intent is to coerce the subjects into sexual activity.[74] In response to a House of Lords inquiry, the CPS also put forth amended guidelines to clarify the application of its existing social media guidelines to other incidents of revenge pornography, which applied existing laws to such offenses.[75]

Prosecutors have also targeted hate speech and incitement to violence based on Islamic extremism. In April 2015, for example, Alaa Esayed, an Iraqi national living in the UK, pleaded guilty to charges of publishing and disseminating terrorist material via Twitter and Instagram from June 2013 to May 2014, resulting in a three-and-a-half year prison sentence.[76] While she argued that the content was not hers but rather "cut and pasted" from messages of others, the court held that its dissemination encouraged the recruitment of young people to travel to foreign countries in order to commit terrorist acts.[77]

Surveillance, Privacy, and Anonymity

Over the past year, several inquiries have studied the UK's surveillance environment and offered recommendations. In October 2013, the parliamentary Intelligence and Security Committee (ISC) launched an inquiry into the extent and scale of mass surveillance undertaken by Britain's spy agencies.[78] The ISC's report entitled "Privacy and Security: A modern and transparent legal framework" was released on March 12, 2015, and offered a review of the "intrusive capabilities available to the

71 "Major reform of intellectual property comes into force," UK Department for Business, Innovation and Skills, September 30, 2014, https://www.gov.uk/government/news/major-reform-of-intellectual-property-comes-into-force.

72 Press Association, "'Revenge porn' offender jailed," Daily Mail, Nov. 14, 2014, http://www.dailymail.co.uk/wires/pa/article-2834847/Revenge-porn-offender-jailed.html.

73 Id.

74 "Guidelines on prosecuting cases involving communications sent via social media," Crown Prosecution Service, amended Oct. 2014, www.parliament.uk/documents/lords-committees/communications/socialmediaoffences/DPPLetter171014.pdf; Owen Bowcott, "Revenge porn could lead to 14-year-sentence, new guidelines clarify," The Guardian, Oct. 7, 2014, www.theguardian.com/law/2014/oct/07/revenge-porn-14-year-sentence-cps-guidelines.

75 "Guidelines on prosecuting cases involving communications sent via social media," Crown Prosecution Service, amended Oct. 2014, www.parliament.uk/documents/lords-committees/communications/socialmediaoffences/DPPLetter171014.pdf.

76 Tom Whitehead, "Woman allegedly posted 45.600 terror messages on Twitter," The Telegraph, Dec. 10, 2014, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11285805/Iraqi-woman-charged-with-allegedly-posting-thousands-of-terror-messages-on-Twitter.html; "'Twitter terrorist' Alaa Esayed jailed for tweets," BBC.co.uk, June 11, 2015, http://www.bbc.co.uk/news/uk-england-london-33097609.

77 Id.

78 Rowena Mason, "Top web firms urge more transparency over UK requests for user data," *The Guardian*, October 18, 2013, http://www.theguardian.com/uk-news/2013/oct/17/uk-gchq-nsa-surveillance-inquiry-snowden.

intelligence agencies." Although finding that bulk interception does not equate to blanket or indiscriminate surveillance, the report highlighted the tension between rights to individual privacy and collective security. The committee concluded that although the country's intelligence agencies do not seek to circumvent the law, the complicated nature of the legal framework and the lack of transparency surrounding it mean that current legislation would be better replaced by a new, single act of parliament.

Similarly, a report released in June 2015 from the Independent Reviewer of Terrorism Legislation, David Anderson, called for a clean slate for government surveillance activities, lamenting the fragmentation and obscurity of current laws. A new law should be both comprehensive in scope and comprehensible in nature, the report said.[79]

There has been considerable concern over the use of the 2000 Regulation of Investigatory Powers Act (RIPA) with regards to the surveillance of journalists and their sources. Protection of journalistic sources was under heated discussion during 2014-15 following two high profile cases of police accessing journalists' communication records with the explicit aim of identifying sources, using RIPA to do so. In September 2014, the London-based Bureau for Investigative Journalism filed an application with the European Court of Human Rights to rule on whether UK legislation properly protects journalists' sources and communications from government scrutiny and mass surveillance.[80] The parliamentary Home Affairs Committee's inquiry into RIPA concluded in December 2014 that RIPA was not fit for purpose and that the legislation governing communications data is in need of complete overhaul.[81]

Surveillance has become a major point of contention in the UK following the revelations by Edward Snowden on the activities of GCHQ and its international counterparts, which were published by the Guardian from June 2013 onwards. Garnering the most attention was a secret and extensive surveillance project, codenamed Tempora, that stored the content of communications—phone calls, emails, social networking posts, private messages, and more—for three days, and stored metadata for thirty days, while it was processed by intelligence agents.[82] Working with telecom companies, GCHQ installed intercept probes at the British landing points of undersea fiber-optic cables, giving the agency access to some 200 cables by 2012, each carrying a load of up to 10 Gbps of data.

Various legislative measures authorize surveillance,[83] including RIPA[84] RIPA includes provisions related to the interception of communications; the acquisition of communications data; intrusive surveillance; secret surveillance in the course of specific operations; the use of covert human intelligence sources like agents, informants, and undercover officers; and access to encrypted data. Under current rules, RIPA allows national agencies and over 400 local bodies to access communication records

79 David Anderson, "A Question of Trust," 11 June 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

80 A summary of the Bureau's application to the European Court of Human Rights https://www.thebureauinvestigates.com/2014/09/14/a-summary-of-the-bureaus-application-to-the-european-court-of-human-rights/

81 Parliament.uk Commons Select Committee http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/news/141206-ripa-rpt-pubn/

82 See *The Guardian*'s interactive site on the Snowden files, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

83 For a general overview of surveillance and the diverse parties involved in the UK, see "Surveillance Road Map: A Shared Approach to the Regulation of Surveillance in the United Kingdom," *ICO*, February 14, 2014, http://ico.org.uk/~/media/documents/library/Corporate/Practical_application/surveillance-road-mapV2.pdf.

84 Accessible: http://www.legislation.gov.uk/ukpga/2000/23/contents; See also, "Explanatory Notes" to RIPA, http://www.legislation.gov.uk/ukpga/2000/23/notes/contents.

for a variety of reasons, ranging from national security to tax collection. The 2012 Protection of Freedoms Act imposed new limits on surveillance powers by requiring local authorities to acquire the approval of a magistrate to access communications data.[85]

A clause within Part I of RIPA supposedly serves as the legal basis for Tempora, allowing the foreign or home secretary to sign off on broad-scale surveillance if communications data is arriving from or departing to foreign soil.[86] However, since the UK's fiber-optic network often routes domestic traffic through international cables, this provision essentially legitimized the GCHQ's ability to conduct widespread surveillance over most, if not all UK citizens.[87]

At the same time, the arrangement allows GCHQ to pass on information to its US counterparts in the NSA regarding U.S. citizens, thereby bypassing American restrictions on domestic surveillance. Documents revealed that the U.S. government has provided at least GBP 100 million (US$ 155 million) in funding to GCHQ over the past few years, leading observers to argue that the U.S. government was paying to use information obtained by the UK government.[88]

In February 2015, the Investigatory Powers Tribunal ruled that the Government Communications Headquarters' (GCHQ) had acted unlawfully in accessing information collected by its U.S. partner, the National Security Agency (NSA), prior to December 2014. The decision was welcomed by UK-based Privacy International and Pakistan-based Bytes For All, two digital rights organizations that have submitted legal challenges to GCHQ practices. However, they remain in disagreement with an earlier ruling that GCHQ practices after December 2014 were not illegal since they were no longer secret, due to the forceful disclosure of information on the UK-U.S. intelligence relationship. The decision marked the first time the tribunal has ruled against any of Britain's three intelligence agencies—GCHQ, MI5, and MI6—that it is entrusted to oversee.[89]

During 2014, 517,236 requests for communications data were submitted by public authorities as a whole (almost 90 percent from police forces and law enforcement agencies), a similar number to the 514,608 received in 2013, while 2,795 lawful intercept warrants were issued, a slight increase from 2760 in 2013.[90] Of these, 68 percent were issued for the purpose of tackling serious crime, and 31 percent for national security concerns.

In terms of data protection mechanisms, regulations to implement the 2006 EU Data Retention Directive were adopted in 2009.[91] Under the regulations, providers had to retain communications data on all users for 18 months, including mobile phone locations and email logs, known as metadata, but excluding the content of the communications.[92] In April 2014, however, the European Court of

85 Protection of Freedoms Act 2012, accessible: http://www.legislation.gov.uk/ukpga/2012/9/enacted.

86 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies & James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

87 Nick Hopkins, "NSA and GCHQ spy programmes face legal challenge," *The Guardian*, July 8, 2013, http://www.theguardian.com/uk-news/2013/jul/08/nsa-gchq-spy-programmes-legal-challenge.

88 Nick Hopkins & Luke Harding, "GCHQ accused of selling its services after revelations of funding by NSA," *The Guardian*, August 2, 2013, http://www.theguardian.com/uk-news/2013/aug/02/gchq-accused-selling-services-nsa.

89 "GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal," Privacy International, February 2, 2015, https://privacyinternational.org/?q=node/482.

90 Rt Hon Sir Anthony May, *2014 Annual Report of the Interception of Communications Commissioner* (London: House of Commons), March 201,5 http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20%28Web%29.pdf

91 The Data Retention (EC Directive) Regulations 2009 (SI 2009 No. 859), April 2, 2009, http://www.legislation.gov.uk/ukdsi/2009/9780111473894.

92 See The Retention of Communications Data (Code of Practice) Order 2003, accessible: http://www.legislation.gov.uk/

Justice struck down the EU directive as a serious breach of fundamental rights such as privacy.[93] Acting on fears that overseas companies would begin to delete data on UK users, thereby threatening counterterrorism work, the government drew up "emergency" legislation on data retention and placed it on a fast-track through parliament in July 2014.[94] The UK Data Retention and Investigatory Powers Act (DRIPA) requires telecommunication companies to retain users' metadata for up to 12 months. Shortly after it was passed, academics, journalists, and privacy advocates criticized the legislation for maintaining powers that were struck down by the European court.[95] The new act was framed as a temporary fix and will expire at the end of 2016. At the time of writing, it was being challenged in court by two MPs, David Davis and Tom Watson, represented by human rights group Liberty, arguing that DRIPA is incompatible with both the UK's Human Rights Act, in particular Article 8, the right to respect for private and family life, and with Articles 7 and 8 of the EU Charter of Fundamental Rights, which call for respect for private and family life and protection of personal data.[96]

There are no public restrictions on the use of encryption technologies. However, under Part 3 of RIPA it is a crime not to disclose an encryption key upon an order from a senior policeman or a High Court judge.[97] The Court of Appeal held in 2008 that such disclosure would not necessarily violate the privilege against self-incrimination.[98] The provision has been used to obtain court orders to force disclosure of keys. Between April 1, 2014 and March 31, 2015, there were 37 court orders for decryption, 29 people charged with refusing to disclose their keys, and 3 convictions for refusal to disclose, with 9 cases still in progress.

Shortly after the terrorist attacks on Paris in January 2015, Prime Minister David Cameron called for a ban on encryption in messaging apps. This was met with criticism from internet freedom and security activists who argued that it would be highly impractical, leaving British communications highly vulnerable,[99] as well as putting an end to e-commerce and introducing excessive filtering.[100] Cameron reaffirmed his commitment to making sure that terrorists were not able to communicate safely via new digital technologies in late June 2015.[101] The UK government plans to put forward a draft investigatory powers bill, dubbed the 'snoopers' charter' by activists, in autumn 2015. It is expected to force tech providers to provide access to encrypted content.

---

uksi/2003/3175/made.

93 Court of Justice of the European Union, "The Court of Justice declares the Data Retention Directive to be invalid," April 8, 2014. curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

94 Andrew Grice, "Emergency data law: David Cameron plots to bring back snoopers' charter," The Independent, July 11, 2014, http://www.independent.co.uk/news/uk/politics/emergency-data-law-government-railroading-through-legislation-on-internet-and-phone-records-9596695.html.

95 Kadhim Shubber, "Everything you need to know about surveillance law DRIP," Wired UK, July 16, 2014, http://www.wired.co.uk/news/archive/2014-07/16/everything-you-need-to-know-about-drip and Alan Travis, "Snooper's charter or justified safeguard? The security bill explained," The Guardian, July 10, 2014, http://www.theguardian.com/politics/2014/jul/10/snoopers-charter-security-bill-explained.

96 Liberty, Campaigning for No Snoopers' Charter, https://www.liberty-human-rights.org.uk/campaigning/no-snoopers-charter, accessed July 7 2015

97 2000, accessible: http://www.legislation.gov.uk/ukpga/2000/23/contents.

98 *R v S & Anor* [2008] EWCA Crim 2177 (October 09, 2008), http://www.bailii.org/ew/cases/EWCA/Crim/2008/2177.html.

99 Cory Doctorow, What David Cameron just proposed would endanger every Briton and destroy the IT industry, *Boingboing*, January 13 2015, http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html

100 James Ball, Cameron wants to ban encryption – he can say goodbye to Digital Britain, Guardian, January 13 2015 http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror

101 Adam Bienkov, David Cameron: Twitter and Facebook privacy is unsustainable http://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable

Intimidation and Violence

There were no reported incidences of overt intimidation or violence against users for their online activities over the coverage period.

Technical Attacks

While there have been incidents of cyberattacks in recent years, nongovernmental organizations, media outlets, or activists are not generally targeted by the government or nonstate actors. However, economically motivated fraud and hacking continue to present a challenge to authorities and the private sector.