Freedom House

United Kingdom

	2013	2014
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)	15	16
TOTAL* (0-100)	**23**	**24**

* 0=most free, 100=least free

Population:	64.1 million
Internet Penetration 2013:	90 percent
Social Media/ICT Apps Blocked:	No
Political/Social Content Blocked:	No
Bloggers/ICT Users Arrested:	No
Press Freedom 2014 Status:	Free

Key Developments: May 2013 – May 2014

- Filtering mechanisms, particularly child-protection filters enabled on all household and mobile connections by default, inadvertently blocked legitimate online content (see **Limits on Content**).
- The Defamation Act, which came into effect on 1 January 2014, introduced greater legal protections for intermediaries and reduced the scope for "libel tourism," while proposed amendments to the Contempt of Court Act may introduce similar protections for intermediaries in relation to contempt of court (see **Limits on Content** and **Violations of User Rights**).
- New guidelines published by the Director of Public Prosecutions in June 2013 sought to limit offenses for which social media users may face criminal charges. Users faced civil penalties for libel cases, while at least two individuals were imprisoned for violent threats made on Facebook and Twitter (see **Violations of User Rights**).
- In April 2014, the European Court of Justice determined that EU rules on the mass retention of user data by ISPs violated fundamental privacy and data protection rights. UK privacy groups criticized parliament for rushing through "emergency" legislation to maintain the practice in July, while failing to hold a public debate on the wider issue of surveillance (see **Violations of User Rights**).
- Police asked a Twitter user to delete a non-threatening tweet about the UK Independence Party (UKIP); separately, intelligence agents raided the offices of the *Guardian* and ordered the destruction of hard drives after the newspaper published leaked documents about government surveillance (see **Violations of User Rights**).

Introduction

The United Kingdom (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 result of the growing popularity of smartphones and the increasing availability of superfast networks, which have maximum advertised speeds of 30 Mbit/s or more. But a growth in technological capacities has simultaneously allowed expanded surveillance, leading to growing fears of abuse by police and intelligence agents.

Leaks by former National Security Agency (NSA) contractor Edward Snowden, published in the *Guardian*, revealed the extent of digital surveillance by the Government Communications Headquarters (GCHQ), a British intelligence-gathering agency. Leaked documents outlined programs and tactics used by GCHQ and its international partners over the past several years, raising questions about the reliability of any previous measures of users' online freedoms in the UK. The fact that these tactics were apparently lawful led to concerns about proportionality, and whether existing legislation on surveillance was intended to be applied in digital contexts.

As in past years, the increasing use of technological methods to restrict access to certain content continued to be controversial. The outsourcing and privatizing of blocking and filtering services raised questions about transparency and overblocking, which may have significant effects on users' online freedoms. There have also been indications that internet users may not fully comprehend their rights and responsibilities in the online world, leading to more prosecutions for online activity.

On a more positive note, changes to the Defamation Act, which came into effect on 1 January 2014, have resulted in more protections for intermediaries and defendants. Proposals for revisions to the Contempt of Court Act were also introduced to deal with the effects of online reporting of the administration of justice. Attempts to curtail online copyright infringements in the form of the Digital Economy Act, which had been criticized for their possible impact on net freedoms, have stalled. While some legislation is therefore being updated and promulgated to protect online freedom, the UK's legislative landscape may need to be revisited to safeguard users' online freedoms in the era of mass surveillance.

Obstacles to Access

Access to the internet has become essential to citizenship and social inclusion in the UK.[1] ICT infrastructure in the country is generally of a strong standard, allowing high levels of access. Over the past year, substantial investments in superfast broadband have also 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. Policies and regulation in the country tend to favor access, although recent revelations regarding extensive government surveillance practices may impact how citizens choose to access the internet.

1 Ofcom, *Internet Citizens 2013: Research Report* (London: Ofcom), November 5, 2013, http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/Internet-Citizens-Report.pdf.

Internet penetration has grown from 78.39 percent in 2008 to 89.84 percent at the end of 2013,[2] with more than 80 percent of adults having household internet access.[3] In the past year, the share of homes with fixed and mobile broadband has grown to 77 percent,[4] with 26.7 percent of UK households having superfast broadband. Nearly 100 percent of all households are within range of ADSL connections and 48 percent of households are within reach of cable. In June 2013 the government completed a consultation that reinforced the need for a supportive policy and regulatory environment for investment in broadband infrastructure,[5] and pledged a further GBP 530 million (US$ 850 million) to help make superfast broadband available in rural communities. The government also set a target that 95 percent of the population would have access to superfast broadband by 2017, and by March 2014, 509,000 rural premises had such access.[6] This builds on the previous phase in which the Broadband Delivery UK program made GBP 830 million (US$ 1.32 billion) available for broadband expansion.[7] The extension of fast broadband to all areas remains a priority and steady progress to this end continues.[8]

Mobile telephone penetration is extensive, with a reported penetration rate of 123.7 percent at the end of 2013.[9] In 2014, 61 percent of all UK adults claimed to own a smartphone, leading to a substantial growth of internet use on mobile phones.[10] 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 6 million subscriptions and over 70 percent of UK premises being able to access outdoor 4G coverage from at least one network. Second-generation (2G) and third-generation (3G) networks are available in over 99 percent of all households. Only four percent of households use mobile broadband as their main internet connection, and overall household use of mobile broadband has decreased over the past two years, from 17 percent in 2011 to 8 percent in March 2014.[11]

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,

2 "Individuals Using the Internet," International Telecommunication Union, 2000-2012, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

3 Ofcom, *The Communications Market* 2014 (London: Ofcom), August 7, 2014, http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr14/uk/. P 261.

4 Ofcom, *The Communications Market* 2014 (London: Ofcom), August 7, 2014, http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr14/uk/. P 261.

5 Department for Culture, Media and Sport (DCMS), *Proposed Changes to Siting Requirements for Broadband Cabinets and Overhead Lines to Facilitate the Deployment of Superfast Broadband Networks* (London: DCMS), June 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205746/Fixed_Broadband_Consultation_Summary_of_Responses_final.pdf.

6 Ofcom, *The Communications Market* 2014, p 309.

7 DCMS, "Next Phase of Superfast Broadband Plans Announced," December, 2010, https://www.gov.uk/government/news/next-phase-of-superfast-broadband-plans-announced--4.

8 For local area progress in broadband provision, see DCMS, *Table of local broadband projects*, November 2013, https://docs.google.com/spreadsheet/ccc?key=0Ah3sVRjT82kKdEltX0lJNjNVWWhNbjBnNGwxeHhqMHc#gid=0.

9 International Telecommunication Union (ITU), "United Kingdom Profile," 2013, http://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx

10 Ofcom, *The Communications Market* 2014.

11 The Oxford Internet Survey p52 http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.pdf.

with the gap between socio-economic 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 by 11 percentage points since 2008.[12] Of the UK households that do not have access to the internet, the majority have no intention to get connected.[13]

The average broadband speed in 2014 was 17.8 Mbps,[14] continuing a trend of rising speeds and growing satisfaction among consumers served by faster fiber-based services.[15] 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 57 percent of adults said they used data services on their mobile phones, an eight percent increase from 2013.[16] More than a quarter of all fixed broadband connections are superfast, an increase of 58 percent from 2013.[17] Superfast connections are increasingly deployed beyond the major urban centers and the price of such connections is decreasing.[18]

The UK provides a competitive market for internet access, and prices for communications services compare favorably with those in other countries.[19] Average fixed internet spending has continued to increase as result of a growth in broadband take-up and switching to superfast services.[20] While 4G services were initially more expensive than non-4G services, the difference is shrinking, and in some cases disappearing.[21] The price basket for superfast broadband has declined by eight percent to just over GBP 8 (US$ 13) per month,[22] while fixed broadband prices increased by one percent in real terms to GBP 16.35 (US$ 26) a month in 2012.[23] The price of a basket of mobile services fell by 3.5 percent in 2013, and is around GBP 14.30 (US$ 23.10). The difference between superfast and standard services is between GBP 5 (US$ 8) and GBP 10 (US$ 16) per month.[24]

Four major ISPs, British Telecom (BT), Virgin Media, TalkTalk, and Sky, control 87 percent of the total market.[25] 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 access. By 2013, unbundled telephone lines reached 9 million homes.[26] Virgin has the highest share of superfast broadband subscribers (56 percent); BT has a 35 percent share, but is dominant in the provision of wholesale access.[27]

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

13 Ofcom, *The Communications Market* 2014, p 262.

14 Ofcom, *The Communications Market 2014*.

15 Ofcom, *The Communications Market 2014*, table 5.71.

16 Ofcom, *The Communications Market* 2014, p 346.

17 Ofcom, *The Communications Market* 2014, p 346, p 13.

18 Ofcom, *The Communications Market* 2014, p 346.

19 Ofcom, *The Consumer Experience of 2013: Research Report*.

20 Ofcom, *The Communications Market* 2014, p 32.

21 Ofcom, *The Communications Market* 2014, p 307.

22 Ofcom, *The Communications Market* 2014, p 307.

23 Ofcom, *The Communications Market 2013*.

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

25 Ofcom, *The Communications Market 2013*.

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

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

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 an alternative dispute-resolution scheme.[28] The government also 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,[29] while mobile providers have cut back on previously unlimited access packages for smartphones, reportedly because of concerns about network congestion. 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.[30] It described the blocking of services and sites by ISPs as "highly undesirable" but said that market forces will address potential problems.[31]

In July 2012, major ISPs published a "Voluntary Code of Practice in Support of the Open Internet".[32] 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.[33]

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 be restricting offensive or otherwise inappropriate words or expressions in domain name registrations.[34] The Nominet Board agreed to make all of the recommended changes.[35] The amended policy specifically aims to address limits on content in respect of serious sexual offences.[36]

Limits on Content

While there is no general law authorizing internet censorship in the UK, filtering mechanisms do operate with the aim of blocking criminal content such as child sexual abuse, sites that promote extremism and terrorism, and copyright-infringing materials. Filtering tools have also expanded to strengthen parental controls over the viewing of adult-oriented sites by children. These child

28 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.

29 Such as peer-to-peer (P2P) file sharing and television streaming.

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

31 Developments at European Union (EU) level may, in the future, also have an impact on net neutrality provisions in the UK. See http://ec.europa.eu/digital-agenda/en/eu-actions.

32 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/.

33 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.

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

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

36 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.

protection measures have been particularly controversial in the realm of mobile devices, where filtering criteria have often resulted in overblocking. A lack of transparency regarding sites blocked through court orders, as well as the increasing outsourcing and privatizing of filtering services, have also raised concerns.

The Internet Watch Foundation (IWF), a registered UK charity, aims to prevent access to child sexual abuse and criminally obscene adult content.[37] The IWF compiles a blacklist of URLs containing images of child sexual abuse using a citizen's hotline and investigations by IWF analysts,[38] in accordance with the Sexual Offences Definitive Guideline published by the Sentencing Council under the Ministry of Justice.[39] In cases where such content is hosted within the UK, therefore constituting a criminal offense, the IWF coordinates with the police and local hosting companies in order to have it removed. A similar system is in place for websites that depict child sexual abuse through non-photographic means, such as computer-generated images, as well as for websites containing criminally obscene adult content.[40]

For child sexual abuse content that is hosted overseas and outside the jurisdiction of British courts, the IWF contacts international hotlines and foreign police authorities in order to have the content eventually removed from servers in the host country. However, in order to prevent British users from accessing the content in the meantime, British ISPs block access to the websites listed in the IWF blacklist using the CleanFeed filtering system, developed by the IWF and BT. Non-photographic child sexual abuse images and criminally obscene adult images do not fall under the remit of the IWF when hosted abroad.[41]

Similar processes for the investigation of online materials inciting hatred were transferred from the IWF to TrueVision, a site that is managed by the police, in 2011.[42]

In November 2013, Prime Minister David Cameron welcomed the introduction of new algorithmic filters by Google and Microsoft that prevent searches for child abuse imagery, and warned that if such measures were unsuccessful, legislative intervention could follow. As many as 100,000 search terms for illegal material are programmed to return no results.[43] Laws such as the Protection of Children Act are used to prosecute individuals suspected of accessing or circulating content relating to child abuse.[44] According to some reports,[45] the task of creating certain filters has been outsourced to foreign companies, raising concerns about evading transparency and reporting requirements

37 The IWF is a British charity funded by ISPs and the EU.

38 The Internet Watch Foundation (IWF) site is located at http://www.iwf.org.uk/.

39 For the latest guidelines, effective April 1, 2014, please visit https://www.iwf.org.uk/assets/media/hotline/Sentencing%20Councils%20Sexual%20Offences%20Definitive%20Guideline%20April%202014.pdf.

40 See "Remit, Vision and Mission" Internet Watch Foundation, https://www.iwf.org.uk/about-iwf/remit-vision-and-mission.

41 TJ McIntyre, "Child Absue images and Cleanfeeds: Assessing Internet Blocking Systems," 2011, available at http://www.academia.edu/771272/Child_Abuse_Images_and_Cleanfeeds_Assessing_Internet_Blocking_Systems.

42 The TrueVision site is located at http://www.report-it.org.uk/home. See IWF, "Incitement to racial hatred removed from IWF's remit," April 11, 2011, http://www.iwf.org.uk/about-iwf/newss/post/302-incitement-to-racial-hatred-removed-from-iwfs-remit.

43 "Google and Microsoft agree steps to block abuse images," *BBC News*, November 18, 2013, http://www.bbc.co.uk/news/uk-24980765.

44 Accessible: http://www.legislation.gov.uk/ukpga/1999/14/contents.

45 See, e.g., Tim Cushing, "UK's Anti-Porn Filtering Being Handled By A Chinese Company," *TechDirt*, July 26, 2013, http://www.techdirt.com/articles/20130725/20042323953/uks-anti-porn-filtering-being-handled-chinese-company.shtml.

under the Freedom of Information Act, particularly regarding how these filters work and why certain sites may be blocked without a court order.[46]

The government has increased its efforts to limit access to materials defined as "extremist" on the internet.[47] The Terrorism Act allows for the removal of terrorist material hosted online in the UK if it "glorifies or praises" terrorism, if it is information that could be useful to conducting terrorism, or if it urges people to commit or support terrorism.[48] A Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials, and the unit reported that it had removed more than 29,000 locally-hosted 'pieces' that breach UK terrorism legislation by April 2014.[49] The government claims to have taken down some 15,000 instances of "jihadist propaganda" since December 2013 in the continuing fight to deny religious extremists in Iraq and Syria with tools to recruit British citizens.[50] The government released a revised "Prevent Anti-Terrorism Strategy" in 2011, which also calls for limiting access to "extremist" materials in schools and public libraries and increasing efforts to remove "harmful content" from the internet.[51] 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.[52]

In addition to child sexual abuse, sites that incite hatred (or "hate sites"), and extremist sites, the government has also taken a proactive approach to restricting sites that have been found in violation of copyright protections. The UK High Court has continued to block sites based on copyright infringement, [53] although it recently held that merely publishing a link to copyright infringing material, rather than hosting the material online, does not amount to a copyright infringement.[54] This approach has since been confirmed by the Court of Justice of the European Union.[55] There have been a number of cases in which courts have ordered sites, such as Newzbin

46 Accessible: http://www.legislation.gov.uk/ukpga/2000/36/contents; See Steve Wood, "Ensuring transparency isn't the cost of outsourcing," *Information Commissioner's Office* (blog), March 5, 2014, http://iconewsblog.wordpress.com/2014/03/05/ensuring-transparency-isnt-the-cost-of-outsourcing-05032014/.

47 See Home Affairs Committee, "MPs urge internet providers to tackle on-line extremism," February 6, 2012, http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/news/120206-rvr-rpt-publication/.

48 Terrorism Act 2006 (c. 11), §3, http://www.legislation.gov.uk/ukpga/2006/11/contents; See "Reporting extremism and terrorism online," *DirectGov*, https://reporting.direct.gov.uk/.

49 Home Office, *CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report* (London: Home Office CM8583), March 26, 2013, https://www.gov.uk/government/publications/contest-annual-report-2012; Open Rights Group, "Counter Terrorism Internal Referral Unit," https://wiki.openrightsgroup.org/wiki/Counter_Terrorism_Internet_Referral_Unit

50 Patrick Wintour, "Government reveals scale of online fight against jihadists," *The Guardian*, June 23, 2014, http://www.theguardian.com/world/2014/jun/23/jihadist-propaganda-government-youtube-british-muslims-isis.

51 Home Office, *Prevent Strategy* (London: Home Office CM8092), June 2011, http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/prevent-strategy-review?view=Binary.

52 Home Office, *CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report*.

53 "Linking to infringing material may not on its own be an act of copyright infringement, says UK judge," *Out-Law*, November 22, 2013, http://www.out-law.com/en/articles/2013/november/linking-to-infringing-material-may-not-on-its-own-be-an-act-of-copyright-infringement-says-uk-judge/

54 *Paramount Home Entertainment International Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2013] EWHC 3479 (Ch) (November 13, 2013), http://www.bailii.org/ew/cases/EWHC/Ch/2013/3479.html.

55 *Nils Svensson and others v Retriever Sverige AB* Case C-466/12 (February 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text&docid=147847&pageIndex=0&doclang=en&mode=req&dir&occ=first&part=1&cid=395; See Court of Justice of the European Union, "Press release No 20/14," February 20, 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-02/cp140020en.pdf.

and the Pirate Bay, to be blocked for copyright infringement,[56] and to have their domain names seized based on the Copyright, Designs, and Patents Act,[57] and other legislation.[58] The CleanFeed system has been adapted to enable ISPs to enforce the blocks, and the list of blocked URLs is growing.[59] The Digital Economy Act (DEA) also stipulates that sites found to have "substantial" violations of copyright can be blocked by a court order. However, an Ofcom review determined that such copyright-related blocking provisions, contained in Sections 17 and 18 of the DEA, are unlikely to be effective and should rather be used in conjunction with other measures. Under these Sections, the Secretary of State for Culture, Media and Sport is able to create regulations to allow "blocking injunctions" by the courts in order to force ISPs to block access to pirated copyright content.[60] Despite the ostensible transparency of the legal system, obtaining copies of the copyright injunctions has proved challenging.[61] The non-profit Open Rights Group (ORG) has consequently called for more transparency about what sites are blocked by court injunctions.[62]

Under the EU 2002 E-Commerce Directive, hosts can be held liable if they are found to have had knowledge of illicit material, including libelous content, but have failed to remove it.[63] This has caused hosting companies to promptly take down material when asked, with little inquiry as to the legitimacy of the demand.[64] 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.[65] (See "Violation of User Rights")

The blocking policy is instituted in line with a voluntary code of practice adopted by the Internet Services Providers' Association.[66] While British ISPs are not required by law to implement the IWF

56 Cf. *EMI Records (Ireland) Ltd and others v UPC Communications Ireland Ltd and others* [2013] IEHC 274 (June 12, 2013), *Dramatico Entertainment Ltd and others v. British Sky Broadcasting Ltd and others* [2012] EWHC 1152 (Ch) (May 2, 2012); *Twentieth Century Fox Film Corporation and others v. British Telecommunications plc* [2011] EWHC 2714 (Ch) (October 26, 2011).

57 Accessible: http://www.legislation.gov.uk/ukpga/1988/48/contents.

58 Matt Warman, "Serious Organised Crime Agency closes down rnbxclusive.com filesharing website," *The Telegraph*, February 15, 2012, http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.

59 The UK's High Court has also ordered ISPs to block Kickass Torrents, H33T, and Fenopy. See David Lee, "Court orders UK ISPs to block more piracy sites," *BBC News*, February 28, 2013, http://www.bbc.co.uk/news/technology-21601609.

60 Ofcom, '*Site Blocking' to reduce online copyright infringement* (London: Ofcom), May 27, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78095/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf.

61 Judith Townend, "Court short of basic Information," *The Guardian*, March 5, 2012, http://www.theguardian.com/law/2012/mar/05/court-case-lists-open-justice.

62 Andy, "Steps towards uncovering the UK's piracy site blackout," *TorrentFreak*, July 19, 2013, http://torrentfreak.com/steps-towards-uncovering-the-uks-piracy-site-blackout-130719/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Torrentfreak+%28Torrentfreak%29&utm_content=FeedBurner.

63 Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013), http://www.legislation.gov.uk/uksi/2002/2013/made. See *Metropolitan International Schools Ltd v. (1) Designtechnica Corporation (2) Google UK Ltd & (3) Google Inc* [2009] EWHC 1765 (QB) (search engine not liable for excerpts); *Bunt v. Tilly* [2006] EWHC 407 (QB) (ISP not liable if it only provides connection); *Twentieth Century Fox Film Corporation v. Newzbin* [2010] EWHC 608 (Ch) (company that provides indexing of copyrighted files liable); *Kaschke v. Gray & Anor* [2010] EWHC 690 (QB) (host that moderates user comments liable). See also Electronic Commerce Directive (Hatred against Persons on Religious Grounds or the Grounds of Sexual Orientation) Regulations.

64 Saskia Walzel, "European Commission Consults on Notice and Takedown," *LSE Media Policy Project* (blog), August 24, 2012, http://blogs.lse.ac.uk/mediapolicyproject/2012/08/24/european-commission-consults-on-notice-and-takedown/.

65 Defamation Act 2013, accessible: http://www.legislation.gov.uk/ukpga/2013/26/contents; See also Iain Wilson & Max Campbell, "Defamation Act 2013: A Summary and Overview", *Inforrm* (blog), January 21, 2014, https://inforrm.wordpress.com/2014/01/21/defamation-act-2013-a-summary-of-the-act-iain-wilson-and-max-campbell/.

66 Adopted in January 1999. See Internet Services Providers' Association, "ISPA Code of Practice," July 3, 2007, http://www.ispa.org.uk/about-us/ispa-code-of-practice/.

blocking list,[67] the Home Office adopted rules in 2010 that prohibit government bodies from procuring services from ISPs that fail to use the list.[68] Consumer awareness of CleanFeed is low, and the list of blocked sites remains secret in order to deter access to unlawful materials. In January 2014, a human rights audit of the IWF recommended the introduction of an independent judicial review of IWF's operations.[69]

Public debate about the imposition of measures that would more effectively prevent children from accessing adult-oriented material on the internet increased in the past year. In November 2013, Sky, TalkTalk, BT, and Virgin pledged to form a new joint venture to lead an awareness campaign around child safety with a marketing expenditure in excess of GBP 25 million (US$ 40 million).[70] The group launched the InternetMatters.org portal in May 2014 to provide parents with advice for making decisions around children's online safety. Media regulators also launched the ParentPort site in October 2011 to receive complaints about materials "unsuitable for children" across all forms of media and to provide a resource for parents for tips on parental controls.[71]

With the rapid rise of mobile internet access, mobile filtering has also become increasingly prevalent. Due to concerns over the unsupervised use of data-enabled mobile phones by children under the age of 18, mobile internet subscriptions are sold to customers with child filters enabled by default and, depending on the provider, require either the disabling of the filters or a deliberate "opt-in" to adult content. Customers can verify their age and remove the filters by contacting their provider with proof of age. Blocked content includes pornography, hate sites, and in some cases, web forums that could potentially allow minors to interact with older users.[72] The practice is conducted in accordance with a 2004 code of conduct established by the Mobile Broadband Group (MBG), consisting of the providers Vodafone, Three, EE, and O2.[73] The code of conduct, last updated in July 2013, covers commercial and internet content, illegal content, malicious communications and customer education.[74] In September 2013 the Independent Mobile Classification Body (IMCB), originally appointed by the MBG to establish the criteria for which sites are deemed to be unsuitable for children under the age of 18, was replaced by the British Board of Film Classification (BBFC) to categorize content and calibrate internet filters.[75] However, the process has been criticized for being subjective, insufficiently transparent, and generally problematic.[76]

67 Christopher Williams, "Home Office Backs Down on Net Censorship Laws," *The Register*, October 16, 2009, http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/.

68 Ben Leach, "Ban for internet providers failing to block child sex sites," *The Daily Telegraph*, March 10, 2010, http://www.telegraph.co.uk/technology/facebook/7411020/Ban-for-internet-providers-failing-to-block-child-sex-sites.html.

69 See https://www.iwf.org.uk/accountability/human-rights-audit.

70 Samuel Gibbs, "UK's top tech executives meet for summit against online child abuse", *The Guardian*, November 18, 2013, http://www.theguardian.com/technology/2013/nov/18/uk-top-tech-executives-online-child-abuse.

71 The Parentport site is located at: http://www.parentport.org.uk/.

72 See LSE Media Policy Project/ Open Rights Group, *Mobile Internet censorship: What's happening and what we can do about it* (May 2012), http://www.openrightsgroup.org/assets/files/pdfs/MobileCensorship-webwl.pdf; See also Claire Milne, "Response to Mobile Censorship Report: Mobile & Fixed Internet are Different", *LSE Media Policy Project* (blog), May 17,2012, http://blogs.lse.ac.uk/mediapolicyproject/2012/05/17/response-to-mobile-censorship-report-mobile-fixed-internet-are-different/.

73 "Who We Are," Mobile Phone Group, http://www.mobilebroadbandgroup.com/whoweare.htm.

74 MBG. *Culture, Media and Sport Select Committee inquiry into online safety. Written evidence submitted by the Mobile Broadband Group*, September 30, 2013. Available from: www.mobilebroadbandgroup.com/faq.

75 MPG, "Social responsibility," www.mobilebroadbandgroup.com/social.htm.

76 Peter Bradwell, "Reporting 'over-blocking' to mobile operators," *Open Rights Group*, May 28, 2012, http://www.openrightsgroup.org/blog/2012/reporting-over-blocking-to-mobile-operators; LSE Media Policy Project/ Open Rights Group, *Mobile Internet censorship: What's happening and what we can do about it.*

The efficacy of such child-protection filtering measures for both mobiles and household access has been questioned. They are easy to circumvent,[77] and can affect legitimate content.[78] On several occasions due to technical difficulties at the ISP level, blocking decisions designed to prevent access to harmful content temporarily disabled users from accessing popular sites such as Wikipedia.[79] The ORG has created the site "Blocked.org.uk" to allow users to report overblocking of content that poses little or no threat to child welfare, including sites on sexual education, drug awareness, and pages run by civil society and political parties. A report by the ORG and the London School of Economics (LSE), published in 2012, found that sites as diverse as Tor, eHow, and that of the British National Party, an extreme right-wing political organization, had been temporarily blocked. The latter was classified as a "hate site" by O2, apparently the only provider that operates a "URL checker" page that allows users to ascertain how a particular site has been classified.[80] The owners and operators of sites are not notified that their sites have been blocked, with the ORG reporting 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.[81]

Barriers to entry in news markets remain theoretically very low, recent years have seen a consolidation of online news providers, with large companies garnering more control over online news markets.[82] Evidence submitted to a judicial inquiry on press practices led by Lord Justice Leveson in 2011 and 2012 revealed close links between these news providers and government actors.[83] As a result of findings published in the Leveson Report in 2012, the larger media houses established the Independent Press Standards Organization, the first regulator for publishers in the country, while another initiative, the Impress Project, also aims to cater for smaller and online publishers on a voluntary basis. Publishers may receive greater protection from punitive damages through joining a regulator. The Crime and Courts Act establishes a higher risk of costs and fines for all newsgatherers, including bloggers, if they refuse to self-regulate.[84] Publishers that decline to join, including news blogs, remain exposed to punitive damages if the publication features multiple authors and is subject to editorial control.[85] There are, however, exceptions to costs and punitive damages exposure for certain types of publishers, including broadcasters, personal blogs, and special interest publications.

77 David Smith, "'Go Away Cameron' Chrome extension nullifies PM's porn blockade," *Tech Radar*, December 22, 2013, http://www.techradar.com/news/internet/-go-away-cameron-chrome-extension-nullifies-pm-s-porn-blockade-1210457.

78 Kate Solomon, "Porn filters are blocking legitimate sex education sites, to no one's surprise," *Tech Radar*, December 19, 2013, http://www.techradar.com/news/internet/porn-filters-are-blocking-legitimate-sex-education-sites-to-no-one-s-surprise-1209408.

79 "Wikipedia Child Image Censored," *BBC News*, December 8, 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm.

80 Tom Brewster, "O2 Blocks BNP Website as 'Hate Site'," *Tech Week Europe*, May 18, 2012, http://www.techweekeurope.co.uk/news/o2-blocks-bnp-website-as-hate-site-78653.

81 ORG, "Ten recommendations to ISPs for dealing with over-blocking, " (December 19, 2013); https://www.openrightsgroup.org/blog/2013/ukccis-overblocking.

82 See Open Society Foundations, *Mapping Digital Media: United Kingdom* (Open Society Foundations: London), December 9, 2011, http://www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-united-kingdom-20110701.pdf.

83 Brian H. Leveson, *The Report into the Culture, Practice and Ethics of the Press*, November 29, 2012, https://www.gov.uk/government/publications/leveson-inquiry-report-into-the-culture-practices-and-ethics-of-the-press.

84 See, Crime and Courts Act 2013, accessible: http://www.legislation.gov.uk/ukpga/2013/22/contents/enacted; Media Standards Trust, *The Independent Press Standards Organisation (IPSO): An assessment* (November 2013), http://mediastandardstrust.org/wp-content/uploads/downloads/2013/11/MST-IPSO-Analysis-15-11-13.pdf.

85 See Section 41, Crime and Courts Act 2013, accessible: http://www.legislation.gov.uk/ukpga/2013/22/contents/enacted.

Leveson also recommended that the Information Commissioner's Office (ICO), an independent body that reports to parliament, should publish guidelines as to how the press should be allowed to process personal data in terms of the Data Protection Act, including data obtained, stored and transferred online.[86] In a draft guidance published in January 2014, the ICO recognized that the definition of "journalism" should be interpreted broadly to include citizen bloggers.[87] Thus citizen journalists making use of the internet may potentially avail themselves of the journalism defense in this legislation to avoid being held liable for misconduct related to data processing.

Users in the UK continue to enjoy wide access to free or low-cost blogging services, allowing them to express their views on the internet. YouTube, Facebook, Twitter and other international blog-hosting services are freely available but subject to the filters mentioned above. Users and nongovernmental organizations also employ various forms of online communication to organize political activities, protests, and campaigns. Civil society organizations maintain a significant presence online and have used internet platforms to promote various causes. For example, organizations such as Avaaz,[88] Change.org,[89] and 38 Degrees have millions of members who use social media to campaign successfully on issues.[90] The Libel Reform Campaign, a joint project by the Index on Censorship, English PEN, and Sense About Science, successfully campaigned for changes in the libel laws that were introduced in 2014.[91]

Violations of User Rights

While the UK has no written constitution or bill of rights, the European Convention on Human Rights (ECHR) has been incorporated into UK law through the Human Rights Act,[92] and British courts have recognized the importance of freedom of expression and other human rights. Some positive steps have been taken with the aim of protecting user rights. Changes to the Defamation Act have resulted in more protections for intermediaries and defendants.[93] However, extensive surveillance measures employed by government agencies cast a shadow over the strength and efficacy of protections of user rights in the UK. In addition, this year saw many indications that users may still lack an understanding of their legal obligations when publishing material online, particularly on social media. This is potentially worrying as citizens may be prosecuted for offenses related to copyright, libel, hate speech, incitement to violence, and contempt of court.

86 Brian H. Leveson, *The Report into the Culture, Practice and Ethics of the Press;* Data Protection Act 1998, accessible: http://www.legislation.gov.uk/ukpga/1998/29/contents.

87 ICO, *Data Protection and Journalism: A Guide for the Media* (Draft version 4.0), 23 January 2014, http://ico.org.uk/about_us/consultations/~/media/documents/library/Data_Protection/Research_and_reports/data-protection-and-journalism-a-guide-for-the-media-draft.pdf.

88 See http://www.avaaz.org/.

89 See http://www.change.org/.

90 See "Current Campaigns," *38 Degrees*, http://www.38degrees.org.uk/campaigns.

91 See The Libel Reform Campaign, http://www.libelreform.org/.

92 European Convention on Human Rights (ECHR) 1953; accessible: http://www.echr.coe.int/Documents/Convention_ENG.pdf; Human Rights Act, accessible: http://www.legislation.gov.uk/ukpga/1998/42/contents.

93 See Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), accessible: http://services.parliament.uk/bills/2012-13/defamation.html.

ISPs and users may be punished for copyright-related offenses under the Digital Economy Act (DEA) of 2010.[94] Among other things, the DEA grants the government the power to impose rules on ISPs, such as monitoring and notifying their users after they receive information or reports containing evidence of infringement, even if these allegations are not proven in a court or independent hearing. On September 11, 2013, Ofcom published research showing that almost a quarter of downloads in the UK infringe copyright.[95] A report published in the same month by the LSE Media Policy Project challenged the notion that creative industries are suffering revenue decline as result of copyright infringements.[96] In light of the possible social, cultural, and political impact of punitive measures against citizens, as well as the risk that incentives for innovation and growth will be weakened, the LSE report stressed the need to re-evaluate the DEA.

Over the past year, some users have been prosecuted for copyright-related offenses, with the Federation Against Copyright Theft (FACT) reporting the arrest and fining of various individuals.[97] In March 2014, FACT also launched an Infringing Website List (IWL) in conjunction with the City of London Police to prevent illegal websites operating globally from benefitting from advertising. The IWL retains a list of copyright infringing sites for advertisers to refrain from placing advertisements on such pages.[98] Furthermore, Sections 17 and 18 of the DEA allow for the possibility of the government authorizing "technical measures" against users, such as limiting access speeds or cutting off access altogether, in the fight against piracy.[99] However, following an Ofcom review,[100] the government acknowledged that it would be impracticable to enforce these Sections.[101] In fact, a Draft Deregulation Bill was published in July 2013 that contained a provision to repeal Sections 17 and 18 of the DEA.[102] The provision remained in a revised draft introduced in January 2014.[103] The bill is yet to be finalized.

In June 2012, Ofcom published an Obligations Code that specifies when and how ISPs may issue warning notices to their customers who are thought to be illegally accessing copyright-infringing

94 Accessible: http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1.

95 Ofcom, "Online Copyright Infringement Tracker Wave 4," September 11, 2013, http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/oci-wave4/; "Ofcom: Piracy accounts for one in four downloads," *BBC News*, June 6, 2013, http://www.bbc.co.uk/news/technology-24055245.

96 Bart Cammaerts, Robin Mansell & Bingchun Meng, *Copyright & Creation: A Case for Promoting Inclusive Online Sharing*, LSE Media Policy Project (Policy brief), September 2013, http://www.lse.ac.uk/media@lse/documents/MPP/LSE-MPP-Policy-Brief-9-Copyright-and-Creation.pdf.

97 IP Crime Group, "IP Crime Highlight Report 2013/14," www.gov.uk/government/uploads/system/uploads/attachment_data/file/318338/IP_crime_highlight_report.PDF, p 9.

98 FACT, "FACT supporting the City of London Police call on advertising and brand sectors to help tackle cyber crime," www.fact-uk.org.uk/fact-supporting-the-city-of-london-police-call-on-advertising-and-brand-sectors-to-help-tackle-cyber-crime/.

99 Irina Baraliuc, Sari Depreeuw & Serge Gutwirth, "Copyright enforcement in the digital age: a post-ACTA view on the balancing of fundamental rights," *International Journal of Law & Information Technology*, vol. 21 (March 2013).

100 Ofcom, '*Site Blocking' to reduce online copyright infringement* (London: Ofcom), May 27, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78095/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf.

101 DCMS, *Next Steps for Implementation of the Digital Economy Act*, August 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78090/Next-steps-for-implementation-of-the-Digital-Economy-Act.pdf.

102 See clause 26, accessible: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/210035/130701_CM_8642_Draft_Deregulation_Bill.pdf.

103 UK Parliament, "Deregulation Bill," January 23, 2014, www.publications.parliament.uk/pa/bills/cbill/2013-2014/0162/en/14162en.htm.

material.[104] The code provides for a graduated (or "three strikes") response, whereby ISPs must monitor IP addresses and send notifications to infringing users. After a user receives three notifications in a year, copyright owners may request users' personal details and initiate legal action against them. Only ISPs providing services to over 400,000 broadband-enabled lines are required to implement the graduated response scheme,[105] therefore exempting libraries and providers of wireless hotspots. Additionally, the "technical measures" phase of the DEA cannot be initiated until the Obligations Code is in force for 12 months.[106] The code and relevant costs must be approved by both houses of parliament. Delays in the implementation of the code have made it unlikely that ISPs will be required to take these measures earlier than late 2015.[107]

In June 2013, the Director of Public Prosecutions published final guidelines for prosecuting cases involving communications sent via social media. The guidelines include robust prosecution of communications that may be perceived as credible threats, specifically target an individual or individuals, or amount to a breach of a court order.[108] By contrast, communications that are offensive, indecent, obscene, or false, are unlikely to be subject to prosecution.[109]

The guidelines have been applied in at least one incident to protect victims of abuse or trolling on social media platforms. In late 2013, campaigners for the retention of a female figure's image on UK banknotes became the subjects of extensive harassment online. Some of the abusers were identified, and in February 2014 a man was charged under section 127 of the Communications Act for his involvement via Twitter,[110] and later sentenced to 18 weeks in jail.[111] In the same month, a UK citizen who set up fake Facebook accounts to 'troll herself' and falsely accuse family members of online abuse was sent to prison for 20 months.[112]

In December 2013, proposed changes to the Contempt of Court Act were published by the UK Law Commission.[113] The changes addressed the challenges new media may pose to existing laws on contempt of court, which pre-date the popular internet, among other concerns.[114] The

104 Ofcom, "Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations," June 26, 2012, http://stakeholders.ofcom.org.uk/consultations/infringement-notice/.

105 Ofcom, "Online Infringement of Copyright and the Digital Economy Act 2010."

106 The Digital Economy Act 2010 (c. 24), section 10(2).

107 "UK piracy warning letters delayed until 2015," *BBC News*, June 6, 20134, http://www.bbc.co.uk/news/technology-22796723; Peter Bradwell, "Even more delays to the Digital Economy Act," *Open Rights Group* (blog), February 4, 2013, http://www.openrightsgroup.org/blog/2013/even-more-delays-to-the-digital-economy-act.

108 Crown Prosecution Service. "Guidelines on prosecuting cases involving communications sent via social media," Director of Public Prosecutions, June 2013, www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media.html.

109 Crown Prosecution Service. "Guidelines on prosecuting cases involving communications sent via social media," Director of Public Prosecutions, June 2013, www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media.html.

110 Communications Act 2003, accessible: http://www.legislation.gov.uk/ukpga/2003/21/contents; Rebecca Camber, "MP's Twitter troll charged after bombarding her with vile messages over campaign to put Jane Austen on the £10 note," *Mail Online*, January 24, 2014, http://www.dailymail.co.uk/news/article-2545019/MPs-Twitter-troll-charged-bombarding-vile-messages-campaign-Jane-Austen-10-note.html#ixzz2vTfEmAO8.

111 Amanda Williams, "Twitter troll who threatened to rape MP Stella Creasy in row over Jane Austen appearing on £10 notes is jailed for 18 weeks," September 29, 2014, http://www.dailymail.co.uk/news/article-2773565/Twitter-troll-threatened-rape-Labour-MP-Stella-Creasy-row-Jane-Austen-appearing-10-notes-jailed-18-weeks.html.

112 Maria Tadeo, "Woman becomes first person to be jailed for 'trolling herself'," *The Independent*, February 5, 2014, http://www.independent.co.uk/news/uk/crime/woman-becomes-first-person-to-be-jailed-for-trolling-herself-9110128.html.

113 Accessible: http://www.legislation.gov.uk/ukpga/1981/49/contents.

114 Law Commission. "Contempt of Court," December 19, 2013, http://lawcommission.justice.gov.uk/areas/contempt.htm.

first of its reports, which focused on juror misconduct and internet publications, made various recommendations for reform, including a defense that would prevent online publishers from having to continuously monitor all of their archived material.[115] It has also been proposed that online publications by new media users fall within the ambit of traditional publication for the purposes of the act—meaning that individuals who tweet, blog, or post content that potentially prejudices the administration of justice could be held liable for contempt of court. Jurors who use the internet to look up information about a case may also face criminal charges, in accordance with the proposals.[116]

Social media users have been investigated or charged for interfering with the administration of justice. In late 2013, detectives said they were investigating celebrity Peaches Geldof, who released the name of two mothers who had allegedly allowed singer Ian Watkins to abuse their babies, although their identities were protected under the Sexual Offenses Act.[117] She later apologized and deleted the tweets.[118] Geldof died in 2014. Legal proceedings were launched in February 2013 against several online users for publishing photos that purportedly depicted Jon Venables. A "contra mundum" court injunction bans the publication of anything that could reveal the new identities, appearances, whereabouts or movements of Venables and Robert Thompson, who as children were convicted of murdering a two-year-old.[119] One received a 14-month suspended sentence and a fine of GBP 3,000 (US$ 4,850) in November 2013 for publishing a photograph on Twitter.[120]

In recent years, threats of libel suits had a significant chilling effect on both content producers and ISPs, particularly due to the substantial financial and evidentiary burden on defendants.[121] This was compounded by an increase in so-called "libel tourism," a practice in which foreign litigants with little or no connection to a specific country use the ubiquity of online content to invoke plaintiff-friendly English libel laws against publishers.[122] Amendments to the Defamation Act, which came into effect on 1 January 2014,[123] have now placed restrictions on libel tourism by requiring claimants to prove that of all the places in which a statement was published, England and Wales is clearly the

115 Law Commission, *Contempt of Court (1): Juror Misconduct and Internet Publications* (No 340) (Law Commission: London), December 19, 2013, http://lawcommission.justice.gov.uk/docs/lc340_contempt_of_court_juror_misconduct.pdf.

116 Alex Bailin QC, "Law Commission Report on Contempt of Court: controversial reforms seek to secure fair trials and freedom of speech," *Inforrm* (blog), December 10, 2013, http://inforrm.wordpress.com/2013/12/10/law-commission-report-on-contempt-of-court-controversial-reforms-seek-to-secure-fair-trials-and-freedom-of-speech-alex-bailin-qc/.

117 Sexual Offences Act1992; Josh Halliday, "Peaches Geldof investigated over tweet naming mothers in Ian Watkins case," *The Guardian*, November 28, 2013, http://www.theguardian.com/society/2013/nov/28/peaches-geldof-tweet-ian-watkins-lostprophets.

118 Matthew Weaver and Josh Halliday, "Peaches Geldof apologises for Ian Watkins sex abuse tweet," The Guardian, November 29, 2013, http://www.theguardian.com/society/2013/nov/29/peaches-geldof-apology-ian-watkins-tweet-lostprophets.

119 "Jon Venables, Law and Media Responsibility," *Inforrm* (blog), March 7, 2010, http://inforrm.wordpress.com/2010/03/07/contra-mundum-injunctions-and-jon-venables/; Brian Wheeler, "Twitter users: A guide to the law," *BBC News Magazine*, February 26, 2013, http://www.bbc.co.uk/news/magazine-20782257.

120 "James Bulger killer picture': James Baines sentenced," *BBC*, November 27, 2013, http://www.bbc.co.uk/news/uk-england-merseyside-25122155.

121 Section 1, Defamation Act 1996, http://www.legislation.gov.uk/ukpga/1996/31/contents; see Jo Glanville & Jonathan Heawood, eds., *Free Speech Is Not for Sale: The Impact of English Libel Law on Freedom of Expression* (London: Index on Censorship/English PEN), 2009, http://libelreform.org/our-report#.

122 Gordon Rayner, "How libel tourism became an 'embarrassment' to Britain's reputation," *The Telegraph*, February 23, 2010, http://www.telegraph.co.uk/news/7301403/How-libel-tourism-became-an-embarrassment-to-Britains-reputation.html.

123 See Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), accessible: http://services.parliament.uk/bills/2012-13/defamation.html.

most appropriate place in which to institute an action.[124] The act also introduces a serious harm threshold which should help protect freedom of expression, and it codifies defenses of truth, honest opinion, and publications on matters that are in the public interest.[125]

Nonetheless, the use of libel prosecutions for offending Twitter posts, a practice dubbed "twibel," has increased. Some cases have resulted in substantial damages.[126] In May 2013, the High Court ruled that Member of Parliament Sally Bercow had wrongfully implicated politician and businessman Lord Alistair McAlpine in a child abuse scandal via a libelous tweet.[127] Bercow apologized, removed the offending material, and settled out of court with McAlpine for GBP 15,000 (US$ 24,000).[128] However, the libelous tweet was also retweeted by some of Bercow's thousands of followers. McAlpine settled out of court with at least one of these followers, comedian Alan Davies,[129] while he also demanded that others who had retweeted Bercow's tweet should donate funds to a charity of his choice.[130] McAlpine died in 2014.

The government has also taken measures against users who publish or download information perceived as a security threat. General laws such as the Public Order Act and the Communications Act are being used to charge individuals with crimes for posting threatening or harassing materials on the internet.[131] In the so-called Twitter joke case in 2010, for example, Paul Chambers was convicted under Section 127 of the Communications Act for jokingly tweeting that he would "blow up" a local airport. The High Court overruled his conviction in July 2012, finding that the tweet was not of menacing character.[132]

There are no public restrictions on the use of encryption technologies. However, under Part 3 of the 2000 Regulation of Investigatory Powers Act (RIPA), it is a crime not to disclose an encryption key upon an order from a senior policeman or a High Court judge.[133] The Court of Appeal held in 2008 that such disclosure would not necessarily violate the privilege against self-incrimination.[134] The provision has been used to obtain court orders to force disclosure of keys. Between April 1, 2013

124 Defamation Act 2013 (c. 26); see John Aglionby, "UK Defamation Act aims to end trivial claims and libel tourism," *Ft.com*, December 31, 2013, http://www.ft.com/cms/s/0/afe77e0c-7204-11e3-bff7-00144feabdc0.html#axzz2vOCvPXlv.

125 "Libel: new Defamation Act will reverse 'chilling effect', ministers claim," *The Guardian*, December 30, 2013, http://www.theguardian.com/law/2013/dec/31/trivial-libel-claims-targeted-new-law.

126 "Lesley Kemp faces libel suit over Twitter comments," *BBC News*, April 22, 2013, http://www.bbc.co.uk/news/uk-england-beds-bucks-herts-22224205.

127 *Lord McAlpine of West Green v Sally Bercow* [2013] EWHC 1342 (QB) (May 24, 2013), http://www.bailii.org/ew/cases/EWHC/QB/2013/1342.html; See Hugh Tomlinson QC, "Case Law: McAlpine v Bercow (No.2), Sally Bercow's tweet was defamatory," *Inforrm* (blog) May 24, 2013, http://inforrm.wordpress.com/2013/05/24/case-law-mcalpine-v-bercow-no-2-sally-bercows-tweet-was-defamatory-hugh-tomlinson-qc/.

128 Patrick Sawer, "Lord McAlpine, Conservative Party fundraiser, dies," *The Telegraph*, January 18, 2014, http://www.telegraph.co.uk/news/politics/conservative/10581372/Lord-McAlpine-Conservative-Party-fundraiser-dies.html.

129 Mark Sweney, "Lord McAlpine settles libel action with Alan Davies over Twitter," *The Guardian*, October 24, 2013, http://www.theguardian.com/media/2013/oct/24/lord-mcalpine-libel-alan-davies.

130 Lisa O'Carroll, "Lord McAlpine to demand charity donations for false Twitter allegations," *The Guardian*, November 20, 2012, http://www.theguardian.com/media/2012/nov/20/lord-mcalpine-false-twitter-allegations.

131 Public Order Act, accessible: http://www.legislation.gov.uk/ukpga/1986/64/contents; Communications Act, accessible: http://www.legislation.gov.uk/ukpga/2003/21/contents.

132 *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (QB) (July 27, 2012), http://www.bailii.org/ew/cases/EWHC/QB/2012/2157.html.

133 2000, accessible: http://www.legislation.gov.uk/ukpga/2000/23/contents.

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

and March 31, 2014, there were 37 court orders for decryption, 11 people charged with refusing to disclose their keys, and 2 convictions for refusal to disclose, with 9 cases still in progress.[135]

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.[136] 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. The international companies, including BT and Vodafone Cable, responded to criticism of the practice by stating that they are obliged to hand over user data under UK and European Union law.[137]

In October 2013, the parliamentary Intelligence and Security Committee launched an inquiry into the extent and scale of mass surveillance undertaken by Britain's spy agencies.[138] The UN also announced an investigation into the surveillance powers of both US and UK intelligence agencies.[139] Internet companies like Facebook, Microsoft, Google, Twitter, and Yahoo submitted a memorandum to the UK parliament Home Affairs Committee calling for greater transparency about government requests for user data.[140]

In February 2014, the *Guardian* revealed the existence of another controversial GCHQ surveillance program codenamed Optic Nerve. The program, which dated from at least 2008, indiscriminately collected bulk still images from Yahoo webcam chats until 2010, including substantial quantities of sexually explicit communications. These images were saved to agency databases regardless of whether individual users were intelligence targets.[141] The report led to renewed calls for a review of surveillance laws and practices.[142]

135 Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2013-2014* (London: Stationary Office), September 4, 2014, https://www.gov.uk/government/publications/annual-report-of-the-chief-surveillance-commissioner-for-2013-to-2014.

136 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.

137 James Ball, Luke Harding & Juliette Garside, "BT and Vodafone among telecoms companies passing details to GCHQ," *The Guardian*, August 2, 2013, http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

138 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.

139 Nick Hopkins & Matthew Taylor, "Edward Snowden revelations prompt UN investigation into surveillance," *The* Guardian, December 2, 2013, http://www.theguardian.com/world/2013/dec/02/edward-snowden-un-investigation-surveillance.

140 Rowena Mason, "Top web firms urge more transparency over UK requests for user data."

141 Spencer Ackerman & James Ball, "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ," *The Guardian*, February 28, 2014, http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

142 "Has GCHC taken a photo from your webcam?" *Big Brother Watch* (blog), February 28, 2014, https://www.bigbrotherwatch.org.uk/home/2014/02/gchq-taken-photo-webcam.html; Glyn Moody, "Finally: Senior UK Politicians Start To Call For Review Of GCHQ's Spying Activities," *TechDirt*, March 5, 2014, http://www.techdirt.com/articles/20140304/03580826422/finally-senior-uk-politicians-start-to-call-review-gchqs-spying-activities.shtml.

Various legislative measures authorize surveillance,[143] including RIPA.[144] 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 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.[145]

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.[146] However, since the UK's fiber-optic network often routes domestic traffic through international cables, this provision essentially legitimizes the GCHQ's ability to conduct widespread surveillance over most, if not all UK citizens.[147]

At the same time, the arrangement allows GCHQ to pass on information to its US counterparts in the NSA regarding US citizens, thereby bypassing American restrictions on domestic surveillance. Documents revealed that the US 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.[148]

In the last year, 514,608 requests for communications data were submitted by public authorities as a whole, down from 570,135 in 2012, while 2,760 lawful intercept warrants were issued, a 19 percent decrease from 2012.[149] The Interception Communications Commissioner undertook a detailed investigation of statutory functions performed by his office—namely overseeing interception requests—after criticism following Snowden's revelations, and is investigating whether this number of applications amounts to a "significant institutional overuse" of interception agencies' power. In 2013, 970 communications data errors were reported, leading to 6 separate incidents in which law enforcement agencies acted upon inaccurate data. While the majority of the errors had no serious consequences, in seven of these cases, this led to what the commissioner called "very significant consequences" for involved citizens. The commissioner also expressed his belief that GCHQ and other interception agencies and departments he oversees "do so lawfully, conscientiously, effectively and in the national interest."

143 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.

144 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.

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

146 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.

147 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.

148 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.

149 Rt Hon Sir Anthony May, *2013 Annual Report of the Interception of Communications Commissioner* (London: House of Commons), April 8, 2014, http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.

While the UK government has similarly asserted that its surveillance programs are lawful,[150] the GCHQ surveillance leaks have led to concerns about how proportionate and justified these methods are. There have also been questions about whether RIPA, which was drafted almost 15 years ago, was ever intended for the purposes to which it is being put,[151] and whether reports such as those produced by the interception commissioner are sufficiently transparent.[152] Privacy advocates have criticized the tactics as "blanket surveillance," lacking judicial oversight and undermining the rights guaranteed in Article 8 of the ECHR.[153] Some commentators said the British public appeared somewhat apathetic about the revelations.[154]

In terms of data protection mechanisms, regulations to implement the 2006 EU Data Retention Directive were adopted in 2009.[155] 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.[156] In April 2014, however, the European Court of Justice struck down the EU directive as a serious breach of fundamental rights such as privacy.[157] 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.[158] The UK Data Retention and Investigatory Powers Act requires telecommunication companies to retain users' metadata for up to 12 months. Academics, journalists, and privacy advocates criticized the legislation for maintaining powers that were struck down by the European court.[159] The new act was framed as a temporary fix and will expire at the end of 2016.

In some limited cases, the government uses extrajudicial means to intimidate or pressure users into taking down content. For instance, police reportedly went to the house of a blogger to ask that he

150 See Associated Press, "William Hague defends US-UK spy links," *The Guardian*, June 26, 2013, http://www.theguardian.com/politics/2013/jun/26/hague-defends-us-uk-spy.

151 Robert Pritchard, "The Snowden Leaks: The Need to Update Our Legislation on Data and Security," *RUSI*, October 31, 2013, https://www.rusi.org/analysis/commentary/ref:C527248CF8F8ED/.

152 Sam Smith, "The hidden reports from the Interception of Communications Commissioner Office," *Privacy International*, November 26, 2013, https://www.privacyinternational.org/blog/the-hidden-reports-from-the-interception-of-communications-commissioner-office; Mark Pack, "The Interception of Communications Commissioner has Failed," *Liberal Democratic Voice*, April 27, 2012, http://www.libdemvoice.org/xx-reasons-the-interception-of-communications-commissioner-28234.html.

153 1953; accessible: http://www.echr.coe.int/Documents/Convention_ENG.pdf; Nick Hopkins, "NSA and GCHQ spy programmes face legal challenge"; Nick Hopkins, "Huge swath of GCHQ mass surveillance is illegal, says top lawyer," *The Guardian*, January 28, 2014, http://www.theguardian.com/uk-news/2014/jan/28/gchq-mass-surveillance-spying-law-lawyer.

154 John Lanchester, "The Snowden files: why the British public should be worried about GCHQ," *The Guardian*, October 3, 2013, http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester; Jonathan Freedland, "Snowden fallout throws in stark relief US and UK notions of liberty," *The Guardian*, December 2, 2013, http://www.theguardian.com/world/2013/dec/02/snowden-fallout-us-uk-liberty-nsa-spying.

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

156 See The Retention of Communications Data (Code of Practice) Order 2003, accessible: http://www.legislation.gov.uk/uksi/2003/3175/made.

157 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.

158 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.

159 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.

remove tweets related to the Eurosceptic UK Independence Party (UKIP), after a counsellor from the party had complained. The blogger, Michael Abberton, is a member of the Green party. The actions reportedly had no legal basis, as the tweets were not abusive or illegal, leading to complaints by Abberton and a member of parliament.[160]

The *Guardian* has been investigated for allegedly damaging the UK's intelligence services and thereby aiding terrorists through its print and online publications of surveillance leaks.[161] The investigation involved police demands to access source material, a police raid of the *Guardian*'s London offices, and the threat of legal action by the government. In July 2013, GCHQ agents oversaw the destruction of hard drives that contained secret files detailing surveillance activity in a bid to prevent reporting of the leaks from London, despite copies of the material existing outside of the country.[162] No justification has been provided for the allegation that the newspaper's actions put British national security at risk.[163] Alan Rusbridger, the *Guardian*'s editor, was called to testify before the governments' Home Affairs Select Committee in December 2013,[164] where he justified the publication of Snowden's leaks as being in the public interest.[165] In August 2013, David Miranda, was detained and questioned for nine hours at London's Heathrow airport while carrying materials belonging to his partner, journalist Glenn Greenwald, who wrote many of the Snowden stories.[166] Various items in his possession were confiscated. The High Court later ruled that his detention was legal under the Terrorism Act.[167]

There have been numerous incidents of cyberattacks in the UK over the past few years. Apart from intrusions for fraud and other criminal purposes, activist hacking groups have targeted both commercial and government bodies.[168] In October 2013, British citizen Lauri Love was arrested for allegedly hacking into US government computers, although he was later released on bail without charge.[169] Whether he will be extradited to the US to face charges remain to be seen.

160 Martin Williams and Mark Tran, "Police ask blogger to remove tweet about UKIP," *The Guardian*, May 12, 2014, http://www.theguardian.com/politics/2014/may/12/police-ask-blogger-remove-legitimate-tweet-ukip.

161 "Snowden leaks 'worst ever loss to British intelligence'," *BBC*, October 11, 2013, http://www.bbc.co.uk/news/uk-24486649;

162 Luke Harding, "Footage released of Guardian editors destroying Snowden hard drives," January 31, 2014, the Guardian, http://www.theguardian.com/uk-news/2014/jan/31/footage-released-guardian-editors-snowden-hard-drives-gchq.

163 "MI5 chief Andrew Parker will not face MPs on Snowden claims," *The Guardian*, December 11, 2013, http://www.theguardian.com/uk-news/2013/dec/11/mi5-andrew-parker-mps-snowden-guardian-nsa-files.

164 Nick Hopkins & Matthew Taylor, "Guardian will not be intimidated over NSA leaks, Alan Rusbridger tells MPs," *The Guardian*, December 3, 2013, http://www.theguardian.com/world/2013/dec/03/guardian-not-intimidated-nsa-leaks-alan-rusbridger-surveillance.

165 "Alan Rusbridger and the home affairs select committee: the key exchanges," *The Guardian*, December 3, 2013, http://www.theguardian.com/world/2013/dec/03/rusbridger-home-affairs-nsa-key-exchanges.

166 Alan Travis, Matthew Taylor, and Patrick Wintor, "David Miranda detention at Heathrow airport was lawful, high court rules," The Guardian, February 19, 2014, http://www.theguardian.com/world/2014/feb/19/david-miranda-detention-lawful-court-glenn-greenwald.

167 *David Miranda v Secretary of State for the Home Department, the Commissioner of Police for the Metropolis and three interveners* ([2014] EWHC 255 (Admin)) (February 20, 2014), https://www.judiciary.gov.uk/Resources/JCO/Documents/Judgments/miranda-v-sofshd.pdf; Rosalind English, "Case Law: David Miranda v Secretary of State, Detention challenge dismissed," *Inforrm* (blog), February 20, 2014, http://inforrm.wordpress.com/2014/02/20/case-law-david-miranda-v-secretary-of-state-detention-challenge-dismissed-rosalind-english/; Terrorism Act, accessible: http://www.legislation.gov.uk/ukpga/2000/11/contents.

168 Rupert Steiner, "City Focus: Hacking Britain – Cyber crime costs UK up to £27bn a year," *This is Money*, February 19, 2013, http://www.thisismoney.co.uk/money/news/article-2280777/CITY-FOCUS-Hacking-Britain--Cyber-crime-costs-UK-27bn-year.html; Josh Halliday, "Anonymous hits UK government websites over Julian Assange row," *The Guardian*, August 21, 2012, http://www.guardian.co.uk/technology/2012/aug/21/anonymous-hits-government-websites-julian-assange.

169 BBC News, "US hacking case Lauri Love released from bail," July 25, 2014. http://www.bbc.com/news/uk-england-suffolk-28486123.