UNITED KINGDOM

	2012	2013
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	15
Total (0-100)	**23†**	**23**

* 0=most free, 100=least free

POPULATION: 63.2 million
INTERNET PENETRATION 2012: 87 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- In an effort to protect children from harmful content, filtering on mobile phones is enabled by default and has resulted in instances of over-blocking. In contrast, ISPs did not block politically orientated content on household connections (see **LIMITS ON CONTENT**).
- Revisions to the Defamation Act provided greater legal protections for intermediaries and reduced the scope for "libel tourism" (see **LIMITS ON CONTENT** and **VIOLATIONS OF USER RIGHTS**).
- The Protection of Freedoms Act of 2012 created new requirements to obtain judicial approval prior to accessing online surveillance data, although revelations surrounding the GCHQ's Tempora program have since brought many of these protections into doubt (see **VIOLATIONS OF USER RIGHTS**).
- Several web users were prosecuted or fined for breaking court injunctions, violating the privacy of crime victims, and committing libel using social networks (see **VIOLATIONS OF USER RIGHTS**).

EDITOR'S NOTE ON RECENT DEVELOPMENTS

The following chapter covers developments in the United Kingdom from May 1, 2012 to April 30, 2013. However, beginning in June 2013, British daily newspaper the Guardian *published a series of revelations on secret surveillance practices by the British General Communications Headquarters (GCHQ) and American National Security Agency (NSA). Under the GCHQ's "Tempora" program, British authorities had entered into secret agreements with telecoms giants to install intercept probes on undersea cables landing on British shores. The content of this data was then filtered and stored, typically for three days, in order for GCHQ agents to comb through it for counterterrorism and law enforcement. User "metadata" was stored in a GCHQ facility for 30 days. Furthermore, details emerged surrounding close collaboration between the NSA and the GCHQ, including payments of at least £100 million ($155 million) from the former to the latter. Since UK and U.S. laws place protections on the monitoring of citizens, UK agencies were able to pass on information related to American citizens—and vice versa—thereby bypassing legal restrictions.*

Given that this surveillance has been ongoing for a number of years—including during the period covered by this report—Freedom House has decided to include it in this edition of Freedom on the Net (see Violations of User Rights).

INTRODUCTION

The United Kingdom was an early adopter of new information and communication technologies (ICTs). The University of London was one of the first international nodes of the ARPAnet, the world's introductory operational packet switching network that later came to compose the global internet, and the Queen sent her first ceremonial e-mail in 1976. Academic institutions began connecting to the network in the mid-1980s. By the beginning of the next decade, internet service providers (ISPs) emerged as more general commercial access became available.

The United Kingdom has high levels of internet penetration and online freedom of expression is generally respected. During the past year, however, there has been an attempt by ministers to introduce a new framework for monitoring and collecting online communications as part of the Draft Communications Data Bill.[1] In addition, there has been widespread concern that government proposals to improve journalism co-regulation would result in new liability risks applying to blogs.[2] While ongoing concerns about web filtering and blocking have continued, particularly on mobile platforms, greater public concern has focused on surveillance of communications, particularly after the June 2013 revelations of mass surveillance of web use, e-mail, and mobile traffic data. The Communications Capabilities Development Programme was reintroduced in May 2012, which, if implemented, would require providers to retain data on phone calls, e-mails, text messages and

† The 2012 rating for the UK was adjusted on the basis of updated scoring guidelines to best convey changes over time.
[1] See, Draft Communications Data Bill, http://www.parliament.uk/draft-communications-bill/.
[2] Michael Savage, "Bloggers fear they could be savaged by press watchdog," The Times, March 20, 2013, http://www.thetimes.co.uk/tto/news/medianews/article3717799.ece.

communications on social-networking sites, in addition to expanding the real time surveillance capabilities of the security services in order to combat terrorism and organized crime.[3] However, following the recent leaks by former NSA contractor Edward Snowden, it appeared that the existing surveillance operations were already testing the boundaries of what was permissible.

In a positive development, the government passed a bill to revise the Defamation Act, which provides greater protections for ISPs through limiting their liability for user-generated content, as well as reducing "libel tourism."[4] Additionally, the Protection of Freedoms Act of 2012 sets forth a requirement for local authorities to obtain a magistrate's approval for access to communications data, thereby placing limits on their surveillance powers.[5] The draft Communications Data Bill keeps this requirement.[6]

OBSTACLES TO ACCESS

Access to the internet has become essential to citizenship and social inclusion in the United Kingdom. The share of homes with connected devices has increased from 53 percent in 2002 to 82 percent in 2012,[7] and internet penetration grew from 70 in 2007 to 87 percent in 2012.[8] In December 2010, the government committed to promoting universal access to basic broadband, but progress to that goal remains stalled.[9] The government set a further objective of ensuring "superfast" broadband for 90 percent of households by 2015.[10] The Broadband Delivery UK program has made available £830 million ($1.32 billion) in funding for the project.[11] Although there remain significant numbers of people who for financial or literacy reasons are unable or disinclined to subscribe, broadband is widely available, with nearly 100 percent of all households within range of ADSL connections and 45 percent within reach of fiber optic cable.[12] Superfast connections are, for the most part, only available in major urban centers and not in rural areas.

Even where access is available, use and participation does not necessarily follow. In 2012, 22 percent of the UK adult population did not use the internet at home.[13] Research by the British

[3] David Barrett, "Phone and email records to be stored in new spy plan," The Telegraph, February 18, 2012, http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.
[4] See, Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), http://services.parliament.uk/bills/2012-13/defamation.html.
[5] Protection of Freedoms Act 2012, http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted.
[6] Draft Communications Data Bill, http://www.parliament.uk/draft-communications-bill/.
[7] Ofcom, *The Consumer Experience of 2012: Research Report* (London: Ofcom, January 2013), http://stakeholders.ofcom.org.uk/binaries/research/consumer-experience/tce-12/Consumer_Experience_Researc1.pdf.
[8] "Individuals Using the Internet," International Telecommunication Union, 2000-2012, accessed August 7, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[9] See, Department for Culture, Media and Sport, *Proposed Changes to Siting Requirements for Broadband Cabinets and Overhead Lines to Facilitate the Deployment of Superfast Broadband Networks*, January 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/89449/CONDOC_fixed_bb.pdf.
[10] Ibid.
[11] Department for Culture, Media and Sport, *Next Phase of Superfast Broadband Plans Announced*, December 2010. https://www.gov.uk/government/news/next-phase-of-superfast-broadband-plans-announced--4.
[12] Ofcom, *The Consumer Experience of 2012: Research Report*.
[13] Consumer Communications Panel, "Bridging the Gap: Sustaining Online Engagement," May 2012, http://www.communicationsconsumerpanel.org.uk/smartweb/research/bridging-the-gap:-sustaining-online-engagement.

Communications Consumer Panel found that citizens with internet access may choose not to participate if they lack technical understanding, lack adequate equipment, or are reluctant to submit personal data.[14] Those in the lowest income groups are significantly less likely to have home internet subscriptions, and the gap has remained the same for the past several years. The share of people over 65 with broadband access is significantly lower than that of all other age groups, but the gap has been narrowing rapidly.[15]

Mobile telephone penetration is also universal, with a penetration rate of over 130 percent in 2012.[16] Second-generation (2G) and third-generation (3G) networks are available in over 99 percent of all households. Overall household use of mobile broadband decreased from 17 percent to 12 percent in 2012, and 6 percent of households use mobile broadband as their main internet connection. From 2011 to 2012, the average cost of all mobile service packages increased 7 percent to just over £9 pounds ($14) per month for a basic package and £43 for ($66) for an advanced package that includes internet.[17] The price of broadband declined 13 percent in the past four years to about £16 ($24) per month[18] while increasing in speed from 3.6 Mbps to an average of 12.0 Mbps.[19]

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to government control. ISPs regularly engage in traffic shaping or slowdowns of certain services, such as peer-to-peer (P2P) file sharing and television streaming, while mobile providers have cut back on previously unlimited access packages for smart phones, reportedly because of concerns about network congestion. The Office of Communications (Ofcom), the country's telecommunications regulator, adopted a voluntary code of practice on broadband speeds in 2008, which it updated in 2010.[20] After holding a consultation on the subject,[21] Ofcom released a report in 2011 that called for a self-regulatory approach to network neutrality focusing on information disclosure rather than enforceable rules.[22] It described blocking of services and sites by ISPs as "highly undesirable" but said that market forces will address possible problems. In July 2012, the major ISPs published a "Voluntary code of practice in support of the open internet."[23] 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.

Nominet, the domain registrar in the United Kingdom that manages access to newly introduced

[14] Ibid.
[15] Ofcom, *The Consumer Experience of 2012: Research Report*.
[16] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2012, accessed August 7, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[17] Ofcom, *The Consumer Experience of 2012: Research Report*.
[18] Ibid.
[19] Ofcom, "Overview of UK Broadband Speeds," March 14, 2013.
[20] Ofcom, "2010 Voluntary Code of Practice: Broadband Speeds," July 27, 2010, http://stakeholders.ofcom.org.uk/telecoms/codes-of-practice/broadband-speeds-cop-2010/code-of-practice/.
[21] Ofcom, "Traffic Management and 'net neutrality,' A Discussion Document," June 24, 2010, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/.
[22] Ofcom, "Ofcom's approach to net neutrality," November 11, 2011, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/.
[23] 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/.

.uk, .wales, and .cymru domains, consulted on a new policy regarding the suspension of web domains at the request of law enforcement bodies.[24] The registrar had suspended thousands of domains without a court order after receiving complaints from the police and other bodies for alleged criminal and civil violations.[25] Nominet was told that failure to remove the domains may result in them being found criminally liable. Civil rights groups and ISPs expressed concerned about a lack of due process and have demanded that court orders be required under any new policy.[26]

The UK provides a competitive market for internet access, and prices for communications services compare favorably with those in other countries.[27] Through local loop unbundling, a large number of companies provide internet access on infrastructure provided mainly by British Telecom (BT) and Virgin. BT, as the sole choice for many consumers, is dominant in the provision of wholesale access. This is likely to continue with the rise of "fiber to the cabinet" and "fiber to the home" services, which currently amount to around 40 percent of subscriptions. Four major ISPs—BT, Virgin, TalkTalk, and Sky—control around 87 percent of the total market.[28] ISPs are not subject to licensing but must comply with the general conditions set by Ofcom, such as having a recognized code of practice and being a member of an alternative dispute-resolution scheme.[29] Ofcom's duties include regulating competition among communications industries, including telecommunications and wireless communications services. It is generally viewed as fair and independent in its oversight.

LIMITS ON CONTENT

There is no general law authorizing internet censorship in the UK. At the same time, the UK does operate a filtering system to block unlawful content, such as child pornography. Additionally, laws such as the Protection of Children Act are used to prosecute individuals suspected of accessing or circulating content relating to child abuse.[30] Over the past years, these filtering tools have expanded to include the blocking of content related to intellectual property violations and sites that promote extremism and terrorism. Most recently, there have also been new developments to strengthen parental controls in order to prevent children from viewing adult-oriented sites. These measures

[24] "UK police may be given domain name-suspension powers," Out-Law.com, September 5, 2011. http://www.out-law.com/en/articles/2011/september/uk-police-may-be-given-domain-name-suspension-powers/; Nominet, "Dealing with domain names used in connection with criminal activity," accessed May 21, 2013, http://www.nominet.org.uk/how-participate/policy-development/current-policy-discussions-and-consultations/dealing-domain-names.

[25] According to Open Rights Group, Nominet has said that the takedowns are for "counterfeit goods sites (83%), phishing (9.6%), drugs (6.3%) and fraud (0.8%)"; Jim Killock, "Domain seizures," Open Rights Group (blog), May 20, 2011, http://www.openrightsgroup.org/blog/2011/domain-seizures.

[26] Nominet, "Nominet direct.uk Consultation: Response Analysis," accessed May 21, 2013, http://www.nominet.org.uk/sites/default/files/NomensaAnalysisFinal.pdf; Jim Killock, "ISPA, LINX and ORG insist on Court Orders for domain suspensions," Open Rights Group (blog), November 23, 2011, http://www.openrightsgroup.org/blog/2011/ispa,-linx-and-org-insist-on-court-orders-for-domain-suspensions.

[27] Ofcom, *The Consumer Experience of 2012: Research Report*.

[28] Ofcom, "The Communications Market 2012," July 18, 2012, pp. 313, available at http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/UK_5.pdf.

[29] Ofcom, "General Conditions of Entitlement," accessed May 21, 2013, http://stakeholders.ofcom.org.uk/telecoms/ga-scheme/general-conditions/.

[30] See, Protection of Children Act 2009, http://www.legislation.gov.uk/ukpga/1999/14/contents.

have been most controversial in the realm of mobile devices, where filtering criteria can be subjective and often result in the blocking of content that poses little threat to those under the age of 18. Since these child filters are turned on by default, many mobile users navigate a web in which some legitimate websites, such as those belonging to political groups or civil society organizations, are blocked.

Under a voluntary code of practice adopted by the Internet Services Providers' Association (ISPA) in January 1999, British ISPs block sites flagged as harmful by the Internet Watch Foundation (IWF), a British charity funded by ISPs and the European Union (EU).[31] The IWF generates a blacklist of unlawful content through a citizen hotline and investigations into allegedly criminal content.[32] Previously, the IWF also received reports on materials inciting hatred, but that has since been moved to TrueVision, a new police-run website.[33] The CleanFeed filtering system, developed by BT and the IWF, blocks access to any images or websites listed in the IWF database. While ISPs are not required to implement the IWF blocking list,[34] the overwhelming majority of ISPs do so. Furthermore, in 2010 the Home Office adopted rules that prohibit government bodies from procuring services from ISPs that do not use the list.[35] Consumer awareness of CleanFeed remains very low and the list of blocked sites remains secret in order to deter access to unlawful materials.

In addition to child pornography and hate sites, the government has also taken a proactive approach in limiting access to websites that have been found in violation of copyright protections. There have been a number of cases in which courts have ordered websites, such as Newzbin and the Pirate Bay, to be blocked for copyright infringement[36] and to have their domain names seized based on the Copyright, Designs and Patents Act and other laws.[37] The CleanFeed system has been adapted to enable ISPs to enforce the blocks and the list of URLs is steadily growing.[38] The Digital Economy Act (DEA) of 2010 stipulates that websites found to have "substantial" violations of copyright can be blocked by a court order. However, a review mandated by the government and conducted by Ofcom determined that those particular blocking provisions are unlikely to be effective.[39]

---

[31] Internet Services Providers' Association, "ISPA Code of Practice," accessed August 20, 2012, http://www.ispa.org.uk/about-us/ispa-code-of-practice/.
[32] The Internet Watch Foundation (IWF) website is located at http://www.iwf.org.uk/.
[33] Homepage: 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.
[34] Chris 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/.
[35] 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.
[36] 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).
[37] 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.
[38] The UK's High Court has also ordered ISPs to block Kickass Torrents, H33T, and Fenopy, http://www.bbc.co.uk/news/technology-21601609.
[39] Ofcom, "'Site Blocking' to reduce online copyright infringement," May 27, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78095/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf.

A new initiative to revise the Communications Act of 2003 is expected to be announced later in 2013, which may result in substantial changes to these and other provisions that were adopted through the DEA. The government also initiated a review of intellectual property law in 2011, releasing a report which recommended significant changes to the law, including an explicit exemption for parody, which only partially exists in case law now.[40] The government endorsed the review's conclusions and has consulted on and passed laws to implement its recommendations.[41] In March 2013, the Intellectual Property Office also launched a mediation service to assist in resolving intellectual property disputes.[42] (See "Violation of User Rights" for more information on laws related to the prosecution of users).

In addition, the government has increased its efforts to limit access to "extremist" materials on the internet.[43] The Terrorism Act of 2006 allows for the takedown of terrorist material hosted in the United Kingdom if it "glorifies or praises" terrorism, is information that could be useful to conducting terrorism, or urges people to commit or help with terrorism.[44] ISPs reportedly take down material when contacted by the authorities, though statistics released by ISPs appear to be unverifiable and informal.[45] A new Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials, and as of March 2013, the unit reported that it had successfully taken down 4,000 URLs that breach UK terrorism legislation.[46] The government released a revised Prevent Anti-Terrorism Strategy in 2011, which calls for limiting access to "extremist" materials in schools and public libraries and more efforts to remove "harmful content" from the internet.[47] The strategy also involves "sharing unlawful websites for inclusion in commercial filtering products."[48]

There has also been increased public debate about imposing measures that would more effectively prevent children from accessing adult-oriented material on the internet. The four largest ISPs announced in 2011 that they were offering systems allowing users to filter "adult" materials at the

[40] Intellectual Property Office, "Digital Opportunity: A review of Intellectual Property and Growth," May 2011, http://www.ipo.gov.uk/ipreview; See also, "Parody, pastiche & caricature Enabling social and commercial innovation in UK copyright law," Consumer Focus, July 2011, http://www.consumerfocus.org.uk/files/2012/11/Consumer-Focus-Parody-briefing.pdf.

[41] See, Intellectual Property Office, "Implementing the Hargreaves review", accessed May 25, 2013, http://www.ipo.gov.uk/types/hargreaves.htm.

[42] Intellectual Property Office, "Mediation of Intellectual Property Disputes and IPO Mediation Service," March 2013, http://www.ipo.gov.uk/ipenforce/ipenforce-dispute/ipenforce-mediation.htm.

[43] 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/.

[44] Terrorism Act 2006 (c. 11), §3, available at Office of Public Sector Information, http://www.legislation.gov.uk/ukpga/2006/11/contents; See, "Reporting extremism and terrorism online," DirectGov, http://www.direct.gov.uk/en/CrimeJusticeandtheLaw/CounterTerrorism/DG_183993.

[45] See, e.g., Google Transparency Report, Removal Requests, accessed May 27, 2013, http://www.google.com/transparencyreport/removals/government/.

[46] Home Office, "CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report," March 2013, https://www.gov.uk/government/publications/contest-annual-report-2012.

[47] Home Office, "Prevent Strategy," June 2011, http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/prevent-strategy-review?view=Binary.

[48] Home Office, "CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report."

ISP level and issued a code of practice aimed at educating consumers about parental controls.[49] In June 2011, the Department of Education sponsored a review, which recommended that ISPs provide an "active choice" to parents to limit children's access to adult materials.[50] While the government opposed the use of default filtering, it asked ISPs to encourage their subscribers to make an active choice to switch on parental controls if children are in the household.[51] By the end of 2013, the four major ISPs will also implement a system that automatically e-mails account holders when those parental controls are changed.[52] Regulators also launched the ParentPort website 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 house to use parental controls.[53]

With the rapid rise of mobile access to the internet, the issue of mobile filtering has become increasingly controversial. 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 such as payment details. Blocked content includes pornography, so-called "hate sites," and in some cases, web forums that could potentially allow minors to interact with older users.[54] 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.[55] In turn, the Independent Mobile Classification Body (IMCB), appointed by the MBG, sets the criteria for which websites are deemed to be unsuitable for children under the age of 18. However, the process has been criticized by the Open Rights Group (ORG) as subjective, insufficiently transparent, and generally problematic.

The ORG, in collaboration with the London School of Economics (LSE) Media Policy Project, created the website "Blocked.org.uk" to allow users to report cases of "over-blocking," in which mobile phone providers blocked access to content that poses little or no threat to child welfare, including civil society and political websites. The ORG-LSE report found that websites as diverse as Tor, eHow.com, the French digital rights advocacy group "La Quadrature du Net," a website critical of alleged BBC bias, and a community website for the town of St. Margarets in Middlesex were all blocked. The website of the British National Party, an extreme right-wing political organization, was also blocked. It was classified as a "hate site" by O2, the only provider that

[49] "Code of Practice on Parental Controls—BT, TalkTalk, Virgin Media and Sky," Virgin Media, October 28, 2011, http://mediacentre.virginmedia.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1245.
[50] "Update on the implementation of 'Letting Children be Children,'" Department for Education, April 26, 2012, http://www.education.gov.uk/childrenandyoungpeople/healthandwellbeing/b0074315/bailey-review.
[51] Department of Education, "The Government's response to the consultation on parental internet controls," December 2012, http://www.education.gov.uk/ukccis/news/a00218633/parental-internet-controls-consultation.
[52] See, United Kingdom Council for Child Internet Safety, "Executive Board Notes February 2013," accessed May 24, 2013, http://www.education.gov.uk/ukccis/about/b0076378/executive-board.
[53] Homepage: http://www.parentport.org.uk/.
[54] See a report published by LSE/ Open Rights Group http://www.openrightsgroup.org/assets/files/pdfs/MobileCensorship-webwl.pdf and a discussion here: http://blogs.lse.ac.uk/mediapolicyproject/2012/05/17/response-to-mobile-censorship-report-mobile-fixed-internet-are-different/
[55] "Who We Are," Mobile Phone Group, accessed September 3, 2013, http://www.mobilebroadbandgroup.com/whoweare.htm.

operates a "URL checker" page to look-up how a given website is classified.[56] The owners and operators of websites are not notified that they have been blocked and it is not clear from mobile providers what process they must go through to request to be unblocked.[57]

Similarly, the filtering system for fixed-line connections has encountered its own faults. On several occasions, due to technical difficulties at the ISP level, blocking decisions designed to prevent access to harmful content also temporarily disabled users from accessing popular sites such as Wikipedia.[58] In 2011, the IWF identified a single URL at the popular cloud server site Fileserve to be blocked; however, due to technical problems, BT and Virgin subscribers were prevented from using the entire service for several days.[59]

Finally, under the EU 2002 E-Commerce Directive, hosts can be held liable if they are found to have had knowledge of illicit material, including defamatory content, but have failed to remove it.[60] This caused hosting companies to quickly take down material when asked, with little inquiry as to the legitimacy of the demand.[61] In April 2013, the government updated the Defamation Act, which now provides greater protections for ISPs by limiting their liability for user-generated content.[62] (For more on UK libel law and the issue of libel tourism, please see "Violation of User Rights.")

Following the revelation of phone hacking practices by journalists and news organizations, the government launched an inquiry into press ethics.[63] The government is currently seeking to promote a stronger scheme for self-regulation that encompasses traditional news platforms as well as news websites. To encourage participation, publishers that join a self-regulatory body receive greater protection from punitive damages.[64] 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. There are exceptions to punitive damages exposure for certain types of publishers, including broadcasters, personal blogs, and special interest publications. While barriers to entry in news markets remain theoretically very low, the reality is that recent years have seen a consolidation of online news into a smaller number of providers, with large providers such as News

[56] 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.
[57] Peter Bradwell, Gemma Craggs, Alessandra Cappuccini, and Joana Kamenova, *Mobile Internet censorship: What's happening and what we can do about it,* Open Rights Group and the LSE Media Policy Project, May 2012, available at http://www.openrightsgroup.org/assets/files/pdfs/MobileCensorship-webwl.pdf.
[58] "Wikipedia Child Image Censored," BBC News, December 8, 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm.
[59] "UK ISP Block of Fileserve Site Blamed on Internet Watch Foundation Filter," ISPreview, November 19, 2011.
[60] Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013). 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 just 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.
[61] Saskia Walzel, "European Commission Consults on Notice and Takedown," Media Policy Project (blog), August 24, 2012, http://blogs.lse.ac.uk/mediapolicyproject/2012/08/24/european-commission-consults-on-notice-and-takedown/.
[62] See, Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), http://services.parliament.uk/bills/2012-13/defamation.html.
[63] The Report into the Culture, Practice and Ethics of the Press, November 29, 2012, http://www.levesoninquiry.org.uk/about/the-report/.
[64] See, Section 41, Crime and Courts Act 2013, http://www.legislation.gov.uk/ukpga/2013/22/contents/enacted.

International and Associated Newspapers, as well as the publicly-owned BBC, garnering more control over online news markets.[65] Evidence taken from the Leveson Inquiry revealed that there were close links between these news providers and government actors.

Users in the United Kingdom continue to enjoy wide access to free or low-cost blogging services, allowing them to express their views on the internet. 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[66] and 38 Degrees have millions of members who use social media to campaign successfully on issues.[67] An online petition against UK libel laws received over 60,000 signatures, including support from numerous high profile public figures. "The Libel Reform Campaign," the 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 April 2013.[68]

However, there have been discussions about whether it is appropriate to limit access to social media if necessary to prevent violence. Following the London riots in 2011, Prime Minister David Cameron and other public officials suggested a need to prevent individuals from using social media sites such as Twitter and Facebook for the purposes of organizing public disorder. The government backed away from the statement after public and industry protests, and no specific steps were ever taken that would restrict use of social media.[69]

VIOLATIONS OF USER RIGHTS

The United Kingdom has no written constitution or comprehensive bill of rights. The European Convention on Human Rights is incorporated into UK law through the Human Rights Act of 1998, and British courts have increasingly recognized freedom of expression and other human rights. Over the past year, a new graduated response scheme was introduced by Ofcom in a bid to combat online piracy. Changes to the Defamation Act have also resulted in more protections for intermediaries and defendants, while seeking to reduce libel tourism. Despite these increasing protections, several users were fined for a range of posts on social media, an issue which the public prosecutor has looked to re-examine. In total, there were 653 criminal charges filed against Twitter and Facebook users in England and Wales during 2012.[70] Finally, leaked documents concerning the Tempora program and UK collaboration with U.S. intelligence agencies have brought new

[65] See the Open Society Foundation Mapping Digital Media UK Report http://www.opensocietyfoundations.org/reports/mapping-digital-media-united-kingdom.
[66] See, http://www.avaaz.org/.
[67] See, "Current Campaigns," 38 Degrees (blog), accessed May 27, 2013, http://www.38degrees.org.uk/campaigns.
[68] See, "The Libel Reform Campaign," http://www.libelreform.org/index.php, accessed June 24, 2013.
[69] "PM statement on disorder in England," The official site of the British Prime Minister's Office, August 11, 2011, http://www.number10.gov.uk/news/pm-statement-on-disorder-in-england/; "England riots: Government mulls social media controls," BBC News, August 11, 2011. http://www.bbc.co.uk/news/technology-14493497.
[70] Brian Wheeler, "Twitter users: A guide to the law," BBC News Magazine, February 26, 2013, http://www.bbc.co.uk/news/magazine-20782257.

information to light on the government's widespread surveillance of ICTs for counterterrorism and law enforcement purposes. Privacy groups have criticized the measures as disproportionate and lacking legal oversight.

After much controversy, the Digital Economy Act (DEA) was adopted in April 2010.[71] 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. If surveys and data indicate that this does not result in an overall reduction of infringement in the UK, the DEA provides for a second phase that allows the government to authorize "technical measures," such as limiting access speeds and cutting off access altogether. The ISPs BT and TalkTalk, together with free expression and consumer groups, filed a legal challenge to the DEA in 2010.[72] However, the High Court rejected most of the challenge in April 2011[73] and the decision was upheld by the Court of Appeal in March 2012.[74]

In June 2012, communications regulator Ofcom published an Obligations Code, which specifies when and how ISPs will issue warning notices to their customers who are thought to be illegally accessing copyright-protected material.[75] The code provides for a graduated response, where ISPs must monitor IP addresses and send notifications to users of possible copyright infringement. After a user receives three notifications in a year, copyright owners may request users' personal details and initiate legal action against them. The code allows customers to appeal any such allegation for a £20 ($31) fee. The cost has been criticized as unjust,[76] particularly given the courts' skepticism about the reliability of identifying infringers using IP addresses.[77]

Ofcom clarified in June 2012 that only those ISPs providing service to over 400,000 broadband-enabled lines are required to implement the graduated response scheme explained above.[78] Therefore, most libraries and providers of wireless hotspots would not be obligated to monitor and notify users. Additionally, the "technical measures" phase of the DEA cannot be initiated until the

[71] The Digital Economy Act 2010 (c. 24), available at Office of Public Sector Information, accessed May 25, 2013, http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1.

[72] "ISPs Take Digital Economy Act to the Courts," Out-Law.com, July 8, 2010, http://www.out-law.com/default.aspx?page=11211; "Skeleton Argument on Behalf of Consumer Focus and ARTICLE 19," ARTICLE 19, March 10, 2011. http://www.article19.org/data/files/pdfs/submissions/skeleton-argument-on-behalf-of-consumer-focus-and-article-19.pdf.

[73] British Telecommunications Plc & Anor, R (on the application of) v. The Secretary of State for Business, Innovation and Skills [2011] EWHC 1021 (Admin) (April 20, 2011). See also, Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 268 (Ch) (February 20, 2012); Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 1152 (Ch) (May 2, 2012).

[74] British Telecommunications Plc, R (on the application of) v. BPI (British Recorded Music Industry) Ltd & Ors [2012] EWCA Civ 232 (March 6, 2012).

[75] 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/.

[76] "O2 disclosure ruling could impact on workings of imminent new anti-piracy code, campaigners say," Out-Law.com, March 29, 2012, http://www.out-law.com/en/articles/2012/march1/o2-disclosure-ruling-could-impact-on-workings-of-imminent-new-anti-piracy-code-campaigners-say/.

[77] See, Golden Eye (International) Ltd & Anor v. Telefonica UK Ltd [2012] EWHC 23 (Ch) (March 26, 2012).

[78] Ofcom, "Online Infringement of Copyright and the Digital Economy Act 2010.

Obligations Code is in force for 12 months.[79] Delays in implementation of the Code have made it unlikely that ISPs will be required to take these measures earlier than 2015.[80]

In recent years, threats of libel suits were causing significant chilling effects on both content producers and ISPs, particularly due to the heavy financial and evidentiary burden on defendants.[81] This worsened due to an increase in "libel tourism," a practice in which foreign litigants with little or no connection to the country exploit the ubiquity of online content to invoke plaintiff-friendly English libel laws against their critics.[82] In a positive sign, updates to the Defamation Act passed in April 2013[83] place restrictions on libel tourism by requiring claimants to show that, of all the places in which the statement has been published, England and Wales are clearly the most appropriate places in which to bring legal action.[84] The act also codifies defenses of "truth," "honest opinion," and "publication on matters of public interest."

Nonetheless, there has also been an increased use of libel law for offending Twitter posts, with some cases resulting in substantial damages. In April 2013, it was reported that a British woman was being sued by a Qatari company for defamatory tweets. The dispute arose after the woman took to Twitter to complain of an outstanding payment of £146 ($226), and later £25 ($39), for services rendered. If found guilty, the woman could be ordered to pay up to £120,000 ($186,000) in libel damages.[85]

In addition to questions surrounding intellectual property enforcement and libel, the government has taken strong measures against users who post or download information perceived as a security threat. General laws such as the Public Order Act and the 2003 Communications Act are increasingly being used to charge individuals with crimes for posting threatening or harassing materials on the internet. For example, Paul Chambers had been convicted in 2010 under Section 127 of the Communications Act of 2003, which prohibits sending "by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character."[86] Chambers had used Twitter to express dismay at the closing of the local airport, jokingly writing that he would blow up the airport if it did not reopen within a week.[87] The High Court overruled his conviction in July 2012, finding that the statement was not one of a menacing character.[88]

---

[79] The Digital Economy Act 2010 (c. 24), section 10(2).
[80] 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.
[81] Section 1, Defamation Act 1996; see Jo Glanville and 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://bit.ly/8bC7BX.
[82] "Libel Tourism: Writ Large," The Economist, January 8, 2009, http://www.economist.com/world/international/displaystory.cfm?story_id=12903058.
[83] See, Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), http://services.parliament.uk/bills/2012-13/defamation.html.
[84] Defamation Act 2013 (c. 26).
[85] "Lesley Kemp faces libel suit over Twitter comments," BBC News, April 22, 2013, http://bbc.in/14CqEnO.
[86] Section 127, Communications Act 2003, http://www.legislation.gov.uk/ukpga/2003/21/section/127.
[87] David Allen Green, "Paul Chambers: A Disgraceful and Illiberal Judgment," Jack of Kent (blog), May 11, 2010, http://jackofkent.blogspot.com/2010/05/paul-chambers-disgraceful-and-illiberal.html.
[88] Chambers v Director of Public Prosecutions [2012] EWHC 2157 (QB), July 27, 2012.

In December 2012, the Director of Public Prosecutions launched a three-month consultation on guidelines for prosecuting cases involving communications sent via social media. The proposed 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.[89] In contrast, communications that are offensive, indecent, obscene, or false, are unlikely to be subject to prosecution.[90] Article 19, a human rights organization that focuses on promoting freedom of expression, welcomed the guidelines but cautioned that they could still leave room for abuse of prosecutorial discretion.[91]

Speaking in June 2011, the Attorney General stated that social media users who violate court injunctions, such as those that aim to prevent the publication of information about pending court cases in which one of the parties is not named, could face criminal charges for contempt of court.[92] For example, legal proceedings were reportedly launched in February 2013 against several online users for publishing photos of a convicted killer, despite a court injunction to ban the publication of anything which could reveal the killer's identity.[93] In a similar case from late 2012, nine users were each ordered to pay a fine of £624 ($967) for revealing the identity of a rape victim over social networks. According to the 1992 Sexual Offences Act, victims and alleged victims of rape have a right to anonymity.[94] Social media users can also face punishments from their employers for statements made online. A police officer was forced to resign after posting a series of tweets celebrating the death of the late prime minister Margaret Thatcher.[95]

There is continued concern about surveillance as authorities have increasingly used or misused the powers granted under the Regulation of Investigatory Powers Act (RIPA).[96] The law covers the interception of communications; the acquisition of communications data, including billing data; intrusive surveillance, such as on residential premises or in private vehicles; covert 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. A Secretary of State may also require that communications providers maintain interception capabilities, including systems to record internet traffic on a large scale. Under current rules, RIPA allows national government agencies and over 400 local bodies to access communication records for a variety of reasons, from national security to tax collection. Orders for interception and access to the content of

[89] "Interim guidelines on prosecuting cases involving communications sent via social media," Director of Public Prosecutions, December 19, 2012, http://www.cps.gov.uk/consultations/social_media_consultation.html.
[90] "Interim guidelines on prosecuting cases involving communications sent via social media," Director of Public Prosecutions.
[91] Article 19, "UK: Social media guidelines for prosecutors welcomed but practical application remains to be seen," Dec. 19, 2012, http://www.article19.org/resources.php/resource/3569/en/uk:-social-media-guidelines-for-prosecutors-welcomed-but-practical-application-remains-to-be-seen.
[92] Tara Conlan, "Twitter users who breach injunctions risk legal action, warns attorney general," Guardian, June 7, 2011, http://www.guardian.co.uk/media/2011/jun/07/twitter-users-injunctions-legal-action.
[93] Brian Wheeler, "Twitter users: A guide to the law," BBC News Magazine, February 26, 2013, http://www.bbc.co.uk/news/magazine-20782257.
[94] Press Association, "Ched Evans Rape Case: Twitter Users Who Named Victim Fined £624 Each in Landmark Case," November 5, 2012, Huffington Post UK, http://www.huffingtonpost.co.uk/2012/11/05/ched-evans-twitter-users-fined_n_2077186.html.
[95] "Thatcher: Policeman Quits Over Tweets," Sky News, April 12, 2013, http://news.sky.com/story/1077308/thatcher-policeman-quits-over-tweets.
[96] See generally, the Explanatory Notes to Regulation of Investigatory Powers Act, accessed January 2009, http://www.legislation.gov.uk/ukpga/2000/23/notes/contents.

communications require approval from a Secretary of State, such as the Home Secretary or Foreign Secretary. In 2011, there were 494,078 requests for communications data from telephone companies (including mobile phone service providers) and ISPs—a decrease of 11 percent from the previous year.[97] According to the Interception Commissioner, there were nearly 900 instances where records were incorrectly obtained by authorities and two persons were incorrectly detained based on mistakes in the communications data.[98]

According to amendments to RIPA that were introduced through the Protection of Freedoms Act, local authorities must acquire the approval of a magistrate in order to access communications data.[99] The act, approved on May 1, 2012, seemingly imposed important limits on surveillance powers. However, from June 2013 onwards, details have emerged over the secret surveillance practices of the Government Communications Headquarters (GCHQ), often in collaboration with the National Security Agency (NSA) of the United States. These revelations indicate that a significant amount of surveillance is currently taking place outside of this particular legal framework.

Through a series of leaks obtained by the *Guardian* newspaper, it was revealed that the GCHQ has been conducting a secret surveillance project, codenamed "Tempora," since the fall of 2011. A part of the GCHQ's larger "Mastering the Internet" program, Tempora was launched to create an "internet buffer" consisting of massive amounts of user data obtained from undersea fiber-optic cables landing in the UK. Under Tempora, the content of communications—phone calls, e-mails, social networking posts, private messages, and more—can be stored for three days while it is processed by intelligence agents; metadata is stored for 30 days. The intercept probes—referred to in GCHQ documents as "special source exploitation"—reportedly gave the agency access to 200 fiber-optic cables by 2012, each carrying a load of 10 Gbps of data. An obscure clause within RIPA served as the legal basis for this practice. Under the provision, this sort of broad surveillance may be signed off by the foreign secretary or home secretary if communications data is arriving from or departing to foreign soil. [100] However, since the UK's fiber-optic network often provides for domestic traffic to be routed through international cables before returning to the island, the provision allows for the GCHQ to conduct widespread surveillance over most, if not all of UK citizens.[101]

Furthermore, by collaborating with their U.S. government partners, the GCHQ is able to bypass legal protections coded in RIPA in order to obtain information on British citizens from the NSA's PRISM program, which gave the NSA access to the private communications of foreign nationals

[97] Rt Hon Sir Paul Kennedy, "2011 Annual Report of the Interception of Communications Commissioner," House of Commons, June 13, 2012, http://www.intelligencecommissioners.com/docs/0496.pdf.
[98] Ibid; Alan Travis, "Snooping errors twice led to wrongful detention, watchdog reveals," Guardian, July 13, 2012, http://www.guardian.co.uk/uk/2012/jul/13/snooping-errors-wrongful-detention-watchdog.
[99] Protection of Freedoms Act, http://www.legislation.gov.uk/ukpga/2012/9/enacted.
[100] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and 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.
[101] 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.

through secret information sharing agreements with major U.S. internet companies. At the same time, the arrangement allowed the GCHQ to pass on information to the NSA regarding U.S. citizens, thereby bypassing American restrictions on domestic surveillance. Indeed, according to leaked internal documents, the GCHQ facility in Cheltenham reportedly "produces larger amounts of metadata collection than the NSA."[102] In another internal document, the GCHQ praised its intelligence collecting and information sharing efforts, stating that the NSA was "delighted by our unique contributions against the [unsuccessful] Times Square and Detroit bombers."[103] Documents also revealed that the U.S. government has provided at least £100 million ($155 million) in funding to the GCHQ over the past few years, leading some observers to conclude that the U.S. government was essentially paying to use information obtained by the UK government.[104] Privacy advocates, such as Privacy International, have criticized the programs as "blanket surveillance," lacking judicial oversight and disproportionately affecting the rights guaranteed in Article 8 of the European Convention of Human Rights.[105]

In 2009, regulations to implement the EU Data Retention Directive were adopted.[106] Under the directive, providers must retain communications data on all users for 12 months, including mobile phone location and e-mail logs, but excluding the content of the communications. ISPs can also continue to "voluntarily" store web-access logs and government agencies may access this information through the procedures in RIPA.[107] In May 2012, the government announced the Communications Capabilities Development Programme (CCDP), a proposal to require ICT service providers to retain data on phone calls, e-mails, text messages, and communications on social-networking sites in order to combat terrorism and organized crime.[108] This was incorporated into a draft Communications Data Bill, which if passed would also expand the real-time surveillance capabilities of the security services and require ISPs to monitor users.[109] Progress on the bill has stalled, however, and on April 25, 2013, Deputy Prime Minister Nick Clegg announced that the bill was unlikely to be implemented during the current government.[110] According to the *Guardian*, British telecommunications giants BT and Vodafone Cable, as well as several other international companies, have been collaborating with the GCHQ under secret agreements to tap into

[102] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and James Ball, "Mastering the internet: how GCHQ set out to spy on the world wide web, " The Guardian, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet?INTCMP=SRCH.
[103] Nick Hopkins, Julian Borger, Luke Harding, "GCHQ: inside the top secret world of Britain's biggest spy agency," The Guardian, August 1, 2013, http://www.theguardian.com/world/interactive/2013/aug/01/gchq-spy-agency-nsa-edward-snowden#part-six.
[104] Nick Hopkins and 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.
[105] 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.
[106] The Data Retention (EC Directive) Regulations 2009 (SI 2009 No. 859), April 2, 2009, http://www.legislation.gov.uk/ukdsi/2009/9780111473894.
[107] See, The Retention of Communications Data (Code of Practice) Order 2003, http://www.legislation.gov.uk/uksi/2003/3175/made.
[108] David Barrett, "Phone and email records to be stored in new spy plan," The Telegraph, February 18, 2012, http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.
[109] See, Draft Communications Data Bill, http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/.
[110] Kelly Fiveash, "Nick Clegg: Snooper's Charter 'isn't going to happen,'" The Register, April 25, 2013, http://bit.ly/10eLMYz.

transatlantic cables. The companies have responded to the allegations by stating that they are obliged to hand over user data under UK and European Union law.[111]

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. The Court of Appeal held in 2008 that such disclosure would not necessarily violate the privilege against self-incrimination.[112] There has been increasing use of the provision to obtain court orders to force disclosure of keys. Between April 2011 and March 2012, there were 33 court orders for decryption, 14 people charged with refusing to disclose their keys, and 2 convictions for refusal to disclose.[113]

There have been numerous cyber-hacking incidents in the UK in the previous year. Apart from intrusions for fraud and other criminal purposes, activist hacking groups have targeted both commercial[114] and government bodies[115] In addition, police have launched two major investigations—Operation Tuleta and Operation Kalmyk—into whether News International illegally hacked the e-mails of various persons, resulting in a number of arrests.[116]

[111] 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?INTCMP=SRCH.
[112] S & Anor, R v [2008] EWCA Crim 2177 (October 09, 2008).
[113] Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012* (London: Stationary Office, July 2012), http://www.official-documents.gov.uk/document/hc1213/hc04/0498/0498.pdf; Chris Williams, "UK Jails Schizophrenic for Refusal to Decrypt Files," The Register, November 24, 2009, http://www.theregister.co.uk/2009/11/24/ripa_jfl/.
[114] 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/.
[115] 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.
[116] See, The Report into the Culture, Practices and Ethics of the Press, Volume I, Part E, Chapter 5, November 29, 2012, http://www.levesoninquiry.org.uk/about/the-report/; "Leveson Inquiry: Police reveal 'likely' victim numbers," BBC News, February 6, 2012, http://www.bbc.co.uk/news/uk-16905465.