UNITED KINGDOM

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	1	1
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	16	16
Total (0-100)	**25**	**25**

* 0=most free, 100=least free

POPULATION: 63 million
INTERNET PENETRATION 2011: 82 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

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 email in 1976. Academic institutions began connecting to the network in the mid-1980s. Internet service providers (ISPs) began appearing in the late 1980s, and more general commercial access was available by the early 1990s.

The United Kingdom has high levels of internet penetration, and online freedom of expression is generally respected. In the past year, however, substantial debate emerged about placing limits on social media sites such as Twitter and Facebook following the London riots in 2011, which prompted Prime Minister David Cameron and other officials to suggest that there should be a way of disabling these services when they are being used to promote violence. After an immediate public outcry, the government backed away from making any concrete proposals to this effect. The government has also taken proactive measures to combat copyright violations through the blocking of websites and penalties for alleged offenders. Moreover, public concern over surveillance has continued to grow, particularly after the Communications Capabilities Development Programme was reintroduced in May 2012, which if implemented would require ICT service providers to retain data on phone calls, emails, text messages and 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.[1]

In a positive development, the government introduced a bill to revise the Defamation Act,[2] which would provide greater protections for ISPs, limit their liability for user-generated content, and place limits on "libel tourism." Additionally, new 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.

OBSTACLES TO ACCESS

Access to internet in the United Kingdom is widespread, and there are few practical barriers, even in rural and disadvantaged areas. The share of homes with computers has increased from 52 percent in 2001 to 78 percent in 2011,[3] and internet penetration stood at 82 percent in 2011.[4] Broadband is almost universally available, with nearly 100 percent of all households capable of obtaining ADSL connections and 48 percent able to connect via cable. The government in December 2010 committed to ensuring "superfast" broadband of at least 24 Mbps for 90 percent of households by 2015.[5] The Broadband Delivery Programme is providing £830 million (US$1.32 billion) in funding for the project.

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 an internet subscription is significantly lower than that of all other age groups, but the gap has been narrowing rapidly.

Mobile telephone penetration is also universal, with a penetration rate of over 130 percent in 2011.[6] Second-generation (2G) networks are available in 99.9 percent of households while third-generation (3G) services are available in 98.9 percent. Mobile broadband is also increasing and is now used by 17 percent of all households, while 11 percent of households

[1] 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.
[2] 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.
[3] Ofcom, *The Consumer Experience 2011: Research Report* (London: Ofcom, December 2011), http://stakeholders.ofcom.org.uk/binaries/research/consumer-experience/tce-11/research_report_of511a.pdf.
[4] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[5] Department for Innovation, Business and Skills (BIS), *Britain's Superfast Broadband Future*, December 2010. http://www.culture.gov.uk/images/publications/britainsSuperfastBroadbandFuture.pdf.
[6] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

use mobile broadband as their main internet connection. Prices for telecommunications access, including mobile telephony and broadband, have continued to decline. Between 2008 and 2011, the average cost of all mobile service packages declined 27 percent to under £9 pounds (US$14) per month for a basic package and £33 for (US$52) for an advanced package that includes internet.[7] The price of broadband declined 33 percent in the past five years to about 14 pounds (US$22) per month while increasing in speed from 1.6 Mbps to an average of 15.5 Mbps.[8]

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 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.[9] It held a consultation on the subject in 2010[10] and released a report in 2011 that called for a self-regulatory approach to network neutrality focusing on information disclosure rather than enforceable rules.[11] It described blocking of services and sites by ISPs as "highly undesirable" but said that market forces will address possible problems. In March 2011, the major ISPs pledged to a "Voluntary industry code of practice on traffic management transparency for broadband services,"[12] which will make the traffic management practices of various ISPs more transparent and accessible to consumers.

There was significant controversy about placing limits on social media sites such as Twitter and Facebook following the London riots in 2011. It was alleged that the sites were used to organize the disorder, prompting Prime Minister David Cameron and other public officials to suggest that there should be a way of preventing people from using these sites in similar situations.[13] The government, however, backed away from the statement after public and industry protests, and no specific steps were ever taken that would restrict use of social media.

---

[7] Ofcom, *The Consumer Experience 2011: Research Report*.
[8] Ibid.
[9] 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/.
[10] Ofcom, "Traffic Management and 'net neutrality,' A Discussion Document," June 24, 2010, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/.
[11] Ofcom, "Ofcom's approach to net neutrality," November 11, 2011, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/.
[12] Broadband Stakeholder Group, "Broadband providers launch new traffic management transparency code," March 15, 2012, http://www.broadbanduk.org/content/view/479/7/.
[13] "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.

Nominet, the main domain registrar in the United Kingdom, is currently consulting on a new policy regarding the suspension of web domains at the request of law enforcement bodies.[14] The registrar has already suspended thousands of domains without a court order after receiving complaints from the police and other bodies for alleged criminal violations.[15] Nominet is also being told that failure to remove the domains may result in them being found criminally liable. Under an appeals process, 12 orders have been appealed with three overturned. Civil rights groups and ISPs are demanding that court orders should be required under the new policy.[16]

The United Kingdom provides a competitive market for internet access, with approximately 700 ISPs in operation; however, 95 percent of users are served by five major companies. 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.[17] 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 filtering or blocking of internet content. Nevertheless, there have been increasing demands in recent years to expand the blocking and filtering of content related to violations of intellectual property and sites that promote extremism and terrorism, as well as measures to strengthen parental controls and prevent children from viewing adult-oriented sites.

The Internet Watch Foundation (IWF), a British charity funded by ISPs and the European Union (EU), operates hotlines and investigates allegedly unlawful content related to child sexual abuse and criminally obscene materials.[18] Previously, it had also received reports on materials inciting racial hatred, but that has been moved to TrueVision, a new police-run

[14] "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 August 20, 2012, http://www.nominet.org.uk/policy/issuegroups/current/domainsassociatedwithcrime/.

[15] 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: it's good to talk," Open Rights Group (blog), May 20, 2011, http://www.theoneclickgroup.co.uk/news.php?id=6261.

[16] 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.

[17] Ofcom, "The General Authorisation Regime," accessed March 31, 2011, http://www.ofcom.org.uk/telecoms/ioi/g_a_regime/.

[18] The Internet Watch Foundation (IWF) website is located at http://www.iwf.org.uk/.

website.[19] The Internet Services Providers' Association (ISPA) adopted a code of practice in January 1999 under which ISPs voluntarily agree to follow the watch list provided by the IWF on which content to remove and block.[20] Additionally, laws such as the Protection of Children Act are used to prosecute individuals suspected of accessing or circulating child pornography.

The CleanFeed filtering system, developed by British Telecom and the IWF, blocks access to any images or websites listed in the IWF database. It is estimated that 98.9 percent of all UK traffic is filtered using CleanFeed or other, less-sophisticated filtering systems.[21] In 2009, the Home Office shelved plans to require all ISPs to implement the IWF blocking list,[22] but in 2010 it adopted rules that prohibit government bodies from procuring services from ISPs that do not use the list.[23] On several occasions, due to technical difficulties on the ISP level, blocking decisions designated to prevent access to harmful content also disabled users from temporarily accessing popular sites such Wikipedia.[24] Most recently, in 2011, the IWF identified for blocking a single URL at the popular cloud server site Fileserve, but due to technical problems, British Telecom and Virgin subscribers were prevented from using the entire service for several days.[25]

There has also been increased public debate about imposing measures that would more effectively prevent children from accessing adult-oriented material on the internet. 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.[26] The four largest ISPs announced in October 2011 that they were offering systems allowing users to filter "adult" materials at the ISP level and they issued a code of practice aimed at educating consumers about parental controls.[27] There has been considerable public discussion, including parliamentary meetings, over whether the system should be turned on by default, requiring users to request the ability to access adult materials, but the government has declined to endorse that policy. Instead, the government launched the ParentPort website in

[19] 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/news/post/302-incitement-to-racial-hatred-removed-from-iwfs-remit.
[20] Internet Services Providers' Association, "ISPA Code of Practice," accessed August 20, 2012, http://www.ispa.org.uk/about-us/ispa-code-of-practice/.
[21] 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/.
[22] Ibid.
[23] 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.
[24] "Wikipedia Child Image Censored," BBC News, December 8, 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm.
[25] "UK ISP Block of Fileserve Site Blamed on Internet Watch Foundation Filter," ISPreview, November 19, 2011.
[26] "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.
[27] "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.

October 2011 to receive complaints about materials "unsuitable for children" across all forms of media.[28]

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 where courts have ordered websites, such as Newzbin and the Pirate Bay, to be blocked for copyright infringement[29] and to have their domain names seized[30] based on the Copyright Act and other laws. The High Court has ordered the ISPs to use the CleanFeed system to block the URLs to the sites. The Department for Culture, Media and Sport (DCMS) has also been meeting with ISPs and rights holders to develop a code of practice for a "rapid judicial procedure" to block "substantially infringing websites."[31]

In addition, the government has increased its efforts to limit access to "extremist" materials on the internet.[32] 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 terrorism, or urges people to commit or help with terrorism.[33] ISPs reportedly take down material voluntarily when contacted by the authorities, though there are no statistics available on the practice and it appears to be unregulated and informal.[34] A new Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials, and as of 2011, the unit reported that it had successfully taken down material in 156 cases.[35] The government released a revised Prevent Anti-Terrorism Strategy in 2011, which calls for blocking access to "extremist" materials in schools and public libraries and more efforts to remove "harmful content" from the internet.[36] The report also states that commercial filtering companies have agreed to include terrorist-related materials in their filtering systems.

[28] Homepage: http://www.parentport.org.uk/.
[29] Twentieth Century Fox Film Corporation and others v. British Telecommunications plc [2011] EWHC 2714 Ch (October 26, 2011).
[30] 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.
[31] "FOI request reveals plans for 'rapid procedure' on web blocking," Out-Law.com, November 17, 2011, http://www.out-law.com/en/articles/2011/november/foi-request-reveals-plans-for-rapid-procedure-on-web-blocking/.
[32] 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/.
[33] Terrorism Act 2006 (c. 11), §3, available at Office of Public Sector Information, http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_1; See, "Reporting extremism and terrorism online," DirectGov, http://www.direct.gov.uk/en/CrimeJusticeandtheLaw/CounterTerrorism/DG_183993.
[34] Chris Williams, "Terrorism Chiefs Don't Know What They've Censored Online," The Register, November 12, 2009, http://www.theregister.co.uk/2009/11/12/west_terror/.
[35] Home Office, "Prevent Strategy," June 2011, http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/prevent-strategy-review?view=Binary.
[36] Ibid

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, the group, 38 Degrees, has over one million members who use social media to campaign successfully on issues, such as saving national forests from being sold off.[37] However, as noted above, there have been discussions about whether it is appropriate to limit access to social media if necessary to prevent violence. The Attorney General also said in June 2011 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.[38]

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.

The intersection of intellectual property and freedom of expression is currently one of the most hotly debated issues. After much controversy, the Digital Economy Act (DEA) was adopted in April 2010,[39] giving the government the power to impose rules requiring ISPs to monitor their users and take "technical measures" against users who are reported (but not proven in a court or independent hearing) to be infringing copyright. These measures include limiting access speeds and cutting off access altogether. The ISPs, British Telecom and TalkTalk, together with free expression and consumer groups filed a legal challenge of the law in 2010.[40] However, the High Court rejected most of the challenge in April 2011 with only a cursory regard to freedom of expression,[41] and the decision was upheld by the

[37] See, "Victory! Government to scrap plans to sell our forests," 38 Degrees (blog), February 17, 2011, http://blog.38degrees.org.uk/2011/02/17/victory-government-to-scrap-plans-to-sell-our-forests/.
[38] 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.
[39] The Digital Economy Act 2010 (c. 24), available at Office of Public Sector Information, accessed August 20, 2012, http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1.
[40] "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.
[41] 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); Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012]

Court of Appeal in March 2012.[42] The DEA also stipulates that websites found to have or likely to have "substantial" violations of copyright can be blocked by a court order.

Ofcom is currently working on an Obligations Code—which will specify when and how ISPs will issue warning notices to their customers who are thought to be illegally accessing copyright-protected material—to implement the law. The present draft allows customers to challenge any such allegation, but they will have to pay a £20 ($US 32) fee for each appeal. In an interesting development, the High Court in March 2012 ruled that the use of internet protocol (IP) addresses was an unreliable way of identifying violators. The ruling also described as "objectionable" the letters that the company was planning to send to people accused of intellectual property violations, which had included threats to cut off service and demands for excessive payments.[43]

A new initiative to revise the Communications Act of 2003 is expected to be announced in late 2012, which will likely result in substantial changes to the 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.[44] The government is currently holding a consultation to implement some of the recommendations of the review.

The threat of libel suits continues to have a significant chilling effect on both content producers and ISPs. English libel law is expansive in its restrictions on allegedly libelous material and places a heavy financial and evidentiary burden on defendants.[45] The United Kingdom has implemented the EU 2002 E-Commerce Directive, which states that hosts can be held liable if they are found to have had knowledge of illicit material, including defamatory content, but failed to remove it.[46] This often results in hosting companies

EWHC 268 (Ch) (20 February 2012); Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 1152 (Ch) (02 May 2012).

[42] British Telecommunications Plc, R (on the application of) v. BPI (British Recorded Music Industry) Ltd & Ors [2012] EWCA Civ 232 (March 06, 2012).

[43] Golden Eye (International) Ltd & Anor v Telefonica UK Ltd [2012] EWHC 723 (Ch) (March 26, 2012); "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/.

[44] 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/2011/07/Consumer-Focus-Parody-briefing.pdf.

[45] 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://libelreform.org/our-report#.

[46] 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*

quickly taking down material when asked, with little inquiry as to the legality of the demand. There is also concern over "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.[47] Recently, the High Court has narrowed the application of the law, in one case ruling that Google does not qualify as a publisher for its blog-hosting service, even though it has received notification of allegedly infringing materials.[48] Moreover, there has been an increased use of libel law for offending Twitter posts, some resulting in substantial damages.[49]

In 2011, the government introduced a bill to revise the Defamation Act,[50] which will provide greater protections for ISPs by limiting their liability for user-generated content and also restrict libel tourism. However, it might also require authors of anonymous posts to identify themselves for the ISPs to be protected.[51] The bill is expected to be enacted in late 2012 or 2013.

In addition to questions surrounding intellectual property enforcement, the government has taken strong measures against users who post or download information perceived as a security treat. For example, two students, one of whom was taking a course on terrorism, were detained in 2008 under the Terrorism Act of 2000 for downloading material deemed to be terrorist in nature.

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, a man was convicted in 2010 under the Communications Act for using 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.[52] The High Court overruled his conviction in July 2012, finding that the statement did not

[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.

[47] "Libel Tourism: Writ Large," The Economist, January 8, 2009, http://www.economist.com/world/international/displaystory.cfm?story_id=12903058.

[48] Tamiz v Google Inc [2012] EWHC 449 (QB).

[49] Cairns v Modi [2012] EWHC 756 (QB) (March 26, 2012); See also, Gervase de Wilde, "Case Law: Cairns v Modi – Defendant found liable for Twitter comments," Inforrm Blog, March 28, 2012, http://inforrm.wordpress.com/2012/03/28/case-law-cairns-v-modi-defendant-found-liable-for-twitter-comments-gervase-de-wilde/.

[50] 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.

[51] See, Ministry of Justice, "The Government's Response to the Report of the Joint Committee on the Draft Defamation Bill," February 2012, 77-88, http://www.justice.gov.uk/downloads/publications/policy/moj/government-response-draft-defamation-bill.pdf.

[52] 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.

represent a credible threat.[53] There have also been a series of arrests of individuals in the past year for the posting of allegedly racist materials,[54] including a man sentenced to 56 days in prison in March 2012 for posting racially-biased statements on Twitter about a footballer who had fallen gravely ill on the field.[55]

There is continued concern about surveillance as authorities have increasingly used or misused the powers granted under the Regulation of Investigatory Powers Act (RIPA).[56] 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. It requires that communications providers maintain interception capabilities, including systems to record internet traffic on a large scale.

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 communications require approval from the home secretary or another secretary of state. 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.[57] 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.[58]

The Protection of Freedoms Act, a major promise of the government, was formally approved on May 1 2012. The act sets up new rules in a variety of areas including retention of DNA, fingerprints of school children, and surveillance cameras. On cyber-related issues, it amends RIPA to require a magistrate's approval for access to communications data by local authorities, thereby limiting their surveillance powers.[59]

---

[53] Chambers v Director of Public Prosecutions [2012] EWHC 2157 (QB), July 27, 2012.
[54] See, Martin Wainwright, "Man who racially abused Stan Collymore on Twitter spared prison," Guardian, March 21, 2012, http://www.guardian.co.uk/technology/2012/mar/21/man-racially-abused-collymore-twitter-spared-prison; "Teenagers given final warnings over racist tweets aimed at Sammy Ameobi," Guardian, February 7, 2012, http://www.guardian.co.uk/football/2012/feb/07/teenagers-warning-racist-tweets-sammy-ameobi.
[55] Steven Morris, "Student jailed for racist Fabrice Muamba tweets," Guardian, March 27, 2012. http://www.guardian.co.uk/uk/2012/mar/27/student-jailed-fabrice-muamba-tweets.
[56] See generally, the Explanatory Notes to Regulation of Investigatory Powers Act, accessed January 2009, http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000023_en_1.
[57] 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.
[58] "Snooping errors twice led to wrongful detention, watchdog reveals," Guardian, July 13, 2012.
[59] Protection of Freedoms Bill (HL Bill 99), http://www.publications.parliament.uk/pa/bills/lbill/2010-2012/0099/lbill_2010-20120099_en_1.htm.

In 2009, regulations to implement the EU Data Retention Directive were adopted.[60] Under the directive, providers must retain communications data on all users for 12 months, including mobile phone location and email logs. ISPs also continue to "voluntarily" store web-access logs, and government agencies access this information through the procedures in RIPA. In May 2012, the government announced the Communications Capabilities Development Programme (CCDP), a proposal that if implemented would require ICT service providers to retain data on phone calls, emails, text messages, and communications on social-networking sites in order to combat terrorism and organized crime.[61] The CCDP would also expand the real time surveillance capabilities of the security services and require ISPs to monitor users.[62] Under the previous government, the program was hotly debated in 2009 but failed to move forward as a bill.[63]

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 ruled in 2008 that self-incrimination protections do not apply.[64] 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 two convictions for refusal to disclose.[65]

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 police websites,[66] government bodies, and newspapers.[67] In addition, police have launched two major investigations as a spin off of the phone hacking investigation—Operation Tuleta

[60] The Data Retention (EC Directive) Regulations 2009 (SI 2009 No. 859), April 2, 2009.
[61] 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.
[62] "Queen's Speech: Communications Data Bill", SCL, May 9, 2012; See also, Robert Booth, "Government plans increased email and social network surveillance," The Guardian, April 1, 2012. http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance.
[63] London School of Economics Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (London: London School of Economics and Political Science, June 2009), http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf.
[64] S & Anor, R v [2008] EWCA Crim 2177 (October 09, 2008).
[65] 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/.
[66] "Soca website taken down after LulzSec 'DDoS attack,'" BBC News, June 20, 2011; "Attack takes Soca crime agency website down," BBC News, May 3, 2012.
[67] "Hacked Sun site greatly exaggerates Murdoch's death," The Register, July 18, 2011.

and Operation Kalmyk—into whether News International illegally hacked the emails of various persons,[68] resulting in a number of arrests.

[68] "Leveson Inquiry: Police reveal 'likely' victim numbers," BBC News, February 6, 2012, http://www.bbc.co.uk/news/uk-16905465.