UNITED KINGDOM

	2009	2011
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access	2	1
Limits on Content	7	8
Violations of User Rights	14	16
Total	**23**	**25**

POPULATION: 62.2 million
INTERNET PENETRATION: 84 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Free

INTRODUCTION

The United Kingdom has high levels of internet penetration, and online freedom of expression is generally respected. However, both the government and private parties have presented ongoing challenges to free speech rights in connection with antiterrorism efforts, public order, and intellectual property. The biggest controversy in the past year was the adoption of the Digital Economy Act on the last day of the outgoing government in April 2010. The law allows for the blocking of websites as well as the cutting off of user accounts based on claims of intellectual-property rights violations. In a positive development, the newly elected coalition government has promised to review and repeal a number of laws that negatively affect online free expression and privacy.

The United Kingdom has been an early adopter of new information and communication technologies. The University of London was one of the first international nodes of the ARPAnet, the world's first 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 to connect 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.

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 46 percent in 2000 to 76 percent in 2009, rising 6 percentage points between 2008 and 2009 alone.[1] Broadband is almost universally available, with 99.6 percent of all households capable of obtaining ADSL connections and 49 percent able to connect via cable. There is no significant difference in access between urban and rural access. As of December 2009, 73 percent of homes had internet subscriptions, and 96 percent of those used broadband.[2] The Conservative Party, which heads the coalition government elected in May 2010, has promised superfast broadband for all homes by 2017.

Those in the lowest income groups are significantly less likely to have home internet subscriptions. In addition, the share of people over 65 with an internet subscription is half that of all other age groups, but the gap has been narrowing; in the past year, two million more people obtained connections, half of them over age 50.[3]

Mobile-telephone penetration is nearly universal, with second-generation (2G) networks available in 98 percent of households and third-generation (3G) services available in around 87 percent. Some 93 percent of all households have at least one mobile phone, with 75 million in active use. Use of mobile broadband is also increasing, but it is still low at 15 percent of all households, and is most popular among younger users. Prices for telecommunications access, including mobile telephony and broadband, have continued to decline. In fact, between 2003 and 2008, cost of mobile service declined at an average annual rate of 11.8 percent to about 16 pounds (US$25) per month.[4] The price of broadband has declined 33 percent in the past five years to about 13 pounds (US$21) per month while increasing in speed from 0.6Mb to 8.2Mb/sec.[5]

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to governmental control. ISPs are increasingly engaging in traffic shaping or slowdowns of certain services, such as peer-to-peer (P2P) file sharing and streaming television, while mobile providers have begun to cut back previously unlimited access packages for smart phones, reportedly because of concerns about network congestion. The Office of Communications (Ofcom), the country's

[1] Ofcom, *The Consumer Experience 2009: Research Report* (London: Ofcom, December 2009), http://stakeholders.ofcom.org.uk/market-data-research/market-data/consumer-experience-reports/ce09/.
[2] Ibid.
[3] UK Online Measurement Company, "Almost Two Million More Britons Online Than Last Year—Over Half Are Over 50," news release, June 30, 2010, http://dl.dropbox.com/u/4340062/UKOM%20PR%20290610.pdf.
[4] Ofcom, "Mobile Evolution: Ofcom's mobile sector assessment," December 2009, http://stakeholders.ofcom.org.uk/binaries/consultations/msa/statement/MSA_statement.pdf.
[5] Ofcom, "The Communications Market 2010: UK," August 2010, http://www.ofcom.org.uk/static/cmr-10/UKCM-5.92.html.

telecommunications regulator, adopted a voluntary code of practice on broadband speeds in 2008[6] and is currently holding a consultation on the subject.[7]

The United Kingdom provides a competitive market for internet access, with approximately 700 ISPs in operation, but 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.[8] 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. The Internet Services Providers' Association (ISPA) adopted a code of practice in January 1999 under which ISPs voluntarily agree to follow the decisions of the Internet Watch Foundation (IWF) on which content to block.[9] The IWF, a British charity funded by the industry and the European Union (EU), operates hotlines and investigates allegedly unlawful content.[10] It reportedly orders blocking of some 10,000 web pages from around the world every year, and its list contains 500 to 800 live URLs at any given time.[11] Most of the content blocked or taken down includes pornography, particularly involving children, and terrorism.

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 systems.[12] In 2009, the Home Office shelved plans to require all ISPs to implement the IWF blocking list.[13] However, an office of the Treasury Department sent out a memorandum in March 2010 stating that government bodies were prohibited from signing contracts with companies that did not agree to comply with the IWF list.[14]

---

[6] Ofcom, "Voluntary Code of Practice: Broadband Speeds," June 5, 2008, http://www.ofcom.org.uk/telecoms/ioi/copbb/copbb/.

[7] Ofcom, "Traffic Management and 'net neutrality' - A Discussion Document," http://stakeholders.ofcom.org.uk/consultations/net-neutrality/, accessed October 30, 2010.

[8] Ofcom, "The General Authorisation Regime," http://www.ofcom.org.uk/telecoms/ioi/g_a_regime/, accessed March 30, 2009.

[9] Internet Services Providers' Association, "ISPA Code of Practice," http://www.ispa.org.uk/about_us/page_16.html, accessed March 30, 2009.

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

[11] IWF, "IWF Facilitation of the Blocking Initiative," http://www.iwf.org.uk/public/page.148.htm, accessed March 30, 2009.

[12] Chris Williams, "Home Office Backs Down on Net Censorship Laws," *Register*, October 16, 2009, http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/.

[13] Ibid.

[14] Sean O'Neill, "Government Ban on Internet Firms That Do Not Block Child Sex Sites," *Times*, March 10, 2010, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7055882.ece; Office of Government

The IWF's blocking and removal actions are not transparent, the blocking criteria lack clarity, and the internal appeals process is inadequate. There is no judicial or governmental oversight. The organization has issued several controversial blocking decisions in recent times. In December 2008, the IWF blocked a Wikipedia page devoted to a 1976 album by the rock band Scorpions due to an image of a nude young girl on its cover, leaving many British users temporarily unable to edit any Wikipedia content.[15] The IWF subsequently revoked its decision after protests from the Wikimedia Foundation.[16] In January 2009, the IWF blocked access to controversial images in the Internet Archive's Wayback Machine, but technical faults in ISPs' implementation of the decision resulted in inability of some users to access any of the 85 billion pages stored, including archives of the British Broadcasting Corporation (BBC) and Parliament.[17]

The Terrorism Act of 2006 allows for the takedown of terrorist material hosted in the United Kingdom.[18] ISPs reportedly take down material voluntarily when contacted by the authorities, though there are no statistics available on the practice.[19]

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. In a notable case in 2010, bloggers used Twitter to defeat a court's "super-injunction" forbidding the *Guardian* newspaper from publishing an article on the company Trafigura's dumping of toxic waste in Ivory Coast.[20] The injunction was broad enough to apply even to parliamentary debates. Bloggers also played a key role in reviewing evidence in the libel case brought against author Simon Singh by the British Chiropractic Association.[21]

Commerce, "Procurement Policy Note—Blocking Access to Web Pages Depicting Child Sexual Abuse," March 5, 2010, http://www.ogc.gov.uk/documents/PPN_05_10_Blocking_illegal_sites.pdf.

[15] "Wikipedia Child Image Censored," British Broadcasting Corporation (BBC), December 8, 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm; Antony Savvas, "Wikipedia Founder Considers Action Against IWF over Scorpions Image Ban," ComputerWeekly.com, December 9, 2008, http://www.computerweekly.com/Articles/2008/12/09/233807/Wikipedia-founder-considers-action-against-IWF-over-Scorpions-image.htm.

[16] Steven Musil, "Internet Watchdog U-Turns on Wikipedia Ban," ZDNet UK, December 10, 2008, http://www.zdnet.co.uk/news/networking/2008/12/10/internet-watchdog-u-turns-on-wikipedia-ban-39574751/.

[17] Cade Metz, "IWF Confirms Wayback Machine Porn Blacklisting," *Register*, January 14, 2009, http://www.theregister.co.uk/2009/01/14/iwf_details_archive_blacklisting/.

[18] Terrorism Act 2006 (c. 11), §3, available at Office of Public Sector Information, http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_1.

[19] Chris Williams, "Terrorism Chiefs Don't Know What They've Censored Online," *Register*, November 12, 2009, http://www.theregister.co.uk/2009/11/12/west_terror/.

[20] Steve Bell, "Trafigura Drops Bid to Gag Guardian over MP's Question," *Guardian*, October 13, 2003, http://www.guardian.co.uk/world/cartoon/2009/oct/14/trafigura-gag-steve-bell-cartoon.

[21] Robert Dougans and David Allen Green, "Virtual Veracity," *The Lawyer*, July 5, 2010, http://www.thelawyer.com/virtual-veracity/1004911.article.

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 Digital Economy Act was adopted in April 2010,[22] during the final parliamentary "wash-up" session—featuring limited debate—prior to Parliament's dissolution for national elections. The law gives the government the power to impose rules requiring ISPs to take "technical measures" against users who are reported (but not proven in a court or independent hearing) to be infringing copyright. The technical measures can include limiting their access speed, blocking their access to sites, and suspending their internet service altogether. ISPs will be required to track users accused of infringements, and copyright holders can apply for a court order to obtain the identification of users. Web sites that are found to have or likely to have "substantial" violations of copyright can be blocked by a court order. Ofcom has already begun developing the regulations for the law, initially only to apply to the larger ISPs.[23] There is significant concern that this will also have the effect of limiting public access though libraries, pubs, hotels, and other locations. The ISPs British Telecom and TalkTalk have begun a legal challenge of the law.[24]

The threat of libel suits has 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.[25] 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.[26] This often results in hosting companies 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 overseas litigants with little or no

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

[23] Ofcom, "Online Infringement of Copyright and the Digital Economy Act 2010," May 28, 2010, http://stakeholders.ofcom.org.uk/consultations/copyright-infringement/.

[24] "ISPs Take Digital Economy Act to the Courts," Out-Law.com, July 8, 2010, http://www.out-law.com/default.aspx?page=11211.

[25] 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#.

[26] 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.

connection to the country exploit the ubiquity of online content to invoke plaintiff-friendly English libel laws against their critics.[27]

In the past year there has been considerable debate over the scope of the libel laws, and the current government, like its predecessor, has promised to review and amend them to better protect freedom of expression. A bill introduced in the House of Lords by Lord Lester specifically includes greater protections for ISPs to limit their liability for user-generated content.[28] The government has committed to introduce its own reform bill in 2011.

In an effort to combat terrorism, the government has taken 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 the subject, were detained in 2008 under the Terrorism Act of 2000 for downloading material deemed to be terrorist in nature. In another case, a man was convicted in 2010 under the Communications Act of 2003 for using the Twitter microblogging service to express dismay at the closing of the local airport and writing that he would blow up the airport if it did not reopen within a week, which an airport manager—reading the message several days later—considered to be a threat.[29] London's Metropolitan Police Service has begun asking cybercafe owners to voluntarily monitor their users' activities as part of the antiterrorism effort, and to put up posters warning patrons not to access "inappropriate or offensive content."

Laws such as the Obscene Publications Act and the Protection of Children Act (extended in 2009) restrict possession or access to sexually oriented materials. In 2009, a man was prosecuted under the Obscene Publications Act for writing and posting online a violent sex fantasy involving the pop band Girls Aloud; the case, which ended in acquittal, had been prompted by an IWF complaint to the police.[30] Kent police in April 2010 initiated the first prosecution of a person under the law for an online chat-room conversation. The outcome of the case is expected to set an important precedent on application of the obscenity law to internet communications.[31]

There is continued concern about surveillance, as authorities have increasingly used or misused the powers granted under the Regulation of Investigatory Powers Act (RIPA).[32] The law covers the interception of communications; the acquisition of communications data,

[27] "Writ Large," *Economist*, January 8, 2009, http://www.economist.com/world/international/displaystory.cfm?story_id=12903058.
[28] Defamation Bill 2010, available at Index on Censorship, http://www.indexoncensorship.org/wp-content/uploads/2010/05/draft-bill-lester-libel.pdf.
[29] David Allen Green, "Paul Chambers: A Disgraceful and Illiberal Judgment," *Jack of Kent*, May 11, 2010, http://jackofkent.blogspot.com/2010/05/paul-chambers-disgraceful-and-illiberal.html.
[30] "Man Cleared over Girls Aloud Blog," BBC, June 29, 2009, http://news.bbc.co.uk/2/hi/uk_news/england/tyne/8124059.stm.
[31] Jane Fae Ozimek, "Mucky Private Chat Could Be Illegal Soon," *Register*, May 18, 2010, http://www.theregister.co.uk/2010/05/18/text_law_extension/.
[32] See generally the Explanatory Notes to Regulation of Investigatory Powers Act at http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000023_en_1, accessed January 2009.

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 nearly 500 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 2009, there were 525,130 requests for communications data from telephone companies (including mobile-phone service providers) and ISPs.[33] In the past few years, there have been numerous cases in which RIPA powers have been used to investigate minor violations, such as sending children to school in the wrong school district or illegal trash dumping.[34] The law has also been used against journalists to obtain their phone records and identify their sources. This has prompted orders to scale back its use.[35]

In 2009, regulations to implement the EU Data Retention Directive were adopted.[36] Under the directive, providers must retain communications data on all users for 12 months, including mobile-phone location and e-mail logs. ISPs also continue to "voluntarily" store web-access logs. Government agencies access this information through the procedures in RIPA. The Interception Modernisation Programme (IMP), a proposal to expand surveillance through deep packet inspection (DPI) and create a 2 billion pound (US$3.2 billion) central database of all communications, was hotly debated in 2009 but failed to move forward as a bill under the old government.[37] The new coalition government promised to limit the scale of surveillance conducted in the country. However, it quietly announced in late 2010 its intent to preserve the ability of various law enforcement agencies to "obtain communication data and to intercept communication within the appropriate legal framework."[38]

There has been significant public discussion surrounding the secret use of DPI by ISPs including British Telecom and Virgin in cooperation with the advertising company Phorm.[39]

---

[33] Sir Paul Kennedy, "Report of the Interception of Communications Commissioner for 2009," July 27, 2010, http://www.official-documents.gov.uk/document/hc1011/hc03/0341/0341.pdf, accessed February 15, 2011.
[34] Steve Doughty, "Councils Deploy Snooping Powers 200 Times a Week," *Daily Mail*, November 12, 2009, http://www.dailymail.co.uk/news/article-1227102/Councils-deploy-snooping-powers-200-times-week.html.
[35] Ian Grant, "UK Tightens Ripa Surveillance Rules," ComputerWeekly.com, November 4, 2009, http://www.computerweekly.com/Articles/2009/11/04/238423/UK-tightens-Ripa-surveillance-rules.htm.
[36] The Data Retention (EC Directive) Regulations 2009 (SI 2009 No. 859), April 2, 2009.
[37] 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.
[38] Tom Whitehead, "Every email and website to be stored," *Telegraph,* October 20, 2010, http://www.telegraph.co.uk/technology/news/8075563/Every-email-and-website-to-be-stored.html.
[39] Charles Arthur, "Phorm Fires Privacy Row for ISPs," *Guardian*, March 6, 2008, http://www.guardian.co.uk/technology/2008/mar/06/internet.privacy; Ian Grant, "Phorm Answers Critics at 'Town-Hall'

Providers withdrew their support for the initiative after the public outcry, and the European Commission has begun proceedings against the UK government for failing to implement the EU Telecommunications Privacy Directive.[40] Virgin is reportedly still using DPI to monitor users' sharing of copyrighted materials.[41]

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. In 2009, the first two prosecutions under the rule yielded convictions, including that of a mentally unstable man who was not accused of committing a serious underlying crime.[42]

Meeting," ComputerWeekly.com, April 18, 2008, http://www.computerweekly.com/Articles/2008/04/21/230354/Phorm-answers-critics-at-39town-hall39-meeting.htm.

[40] European Commission, "Telecoms: Commission Steps Up UK Legal Action over Privacy and Personal Data Protection," news release, October 19, 2009, http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=5369.

[41] Chris Williams, "Virgin Media to Trial Filesharing Monitoring System," *Register*, November 26, 2009, http://www.theregister.co.uk/2009/11/26/virgin_media_detica/.

[42] Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2008–2009* (London: Stationary Office, July 2009), http://www.official-documents.gov.uk/document/hc0809/hc07/0704/0704.pdf; Chris Williams, "UK Jails Schizophrenic for Refusal to Decrypt Files," *Register*, November 24, 2009, http://www.theregister.co.uk/2009/11/24/ripa_jfl/.