United Kingdom

The United Kingdom (U.K.) has a notable libertarian tradition, manifested by, among other things, solid guarantees of freedom of expression, freedom of information, and protection of privacy. Nonetheless, over the last few years the country has witnessed a quick shift toward increased surveillance and police measures in both online and physical space. Combating terrorism and preventing child abuse have been widely used by state agencies and private commercial actors (e.g., Internet service providers) to justify the implementation of interception of communications and direct filtering measures in the country, which have drawn growing criticism.

Background

The U.K., consisting of England, Wales, Scotland, and Northern Ireland, is a constitutional monarchy currently headed by Queen Elizabeth II.[1] Previously a colonial power, the U.K. emerged from the World Wars as a leading global financial center and Western democracy.[2] As the country is a member of the European Union (EU), the bloc's law takes precedence over national law, with U.K. courts required to recognize the jurisdiction of the European Court of Justice (ECJ) in matters of EU law.

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political	•				
Social	•				
Conflict and security	•				
Internet tools	•				

Other Factors	Low	Medium	High	Not Applicable
Transparency				•
Consistency				•

KEY INDICATORS	
GDP per capita, PPP (constant 2005 international dollars)	33,717
Life expectancy at birth (years)	79
Literacy rate (percent of people age 15+)	99
Human development index (out of 179)	21
Rule of law (out of 211)	15
Voice and accountability (out of 209)	13
Democracy index (out of 167)	21 (Full democracy)
Digital opportunity index (out of 181)	10
Internet users (percent of population)	79.6

Source by indicator: World Bank 2009a, World Bank 2009a, World Bank 2009a, UNDP 2008, World Bank 2009b, World Bank 2009b, Economist Intelligence Unit 2008, ITU 2007, ITU 2008.

The U.K. has a vast media network, led by the British Broadcasting Corporation (BBC), a publicly funded institution,[3] with a mandate to remain independent.[4] Other media institutions in the U.K. also enjoy journalistic freedom and represent a broad spectrum of political ideas.[5] Despite the officially recognized journalistic freedom, there have been reports of journalists being jailed or detained for divulging state secrets.[6] The U.K. is a strong supporter of fundamental human rights and freedoms, including freedom of expression.[7] However, recent developments in U.K. antiterrorism laws, in particular the Terrorism Act (2000) and subsequent legislation in 2005 and 2006, have drawn harsh criticism. Advocacy groups claim that new provisions focused on expanding police powers and allowing communication providers to retain personal data for the purpose of ''protecting national security or preventing or detecting crime that relates to national security''[8] are contrary to basic human rights principles.[9]

Internet in the United Kingdom

Residents of the U.K. currently form the fifth-largest broadband subscriber population in the world.[10] In the U.K., 61 percent of households had Internet access in 2007, with 84 percent of those having a broadband connection.[11] The sector regulator reports that broadband technology is available for practically every U.K. citizen to connect to the Internet.[12] In 2006, 63 percent of adults in the U.K. were estimated to have accessed the Internet within a three-month period.[13] Internet usage is more widespread among the younger generations, with over 90 percent of people aged 16 to 24 accessing the Internet in a three-month period, and only 24 percent of those aged over 65 accessing it during the same period.[14] Most of the users access the Internet from their home location (87 percent).[15] As a result of affordability and enhanced market competition, mobile penetration is very high.[16] However, the percentage of people accessing the Internet with their handsets is surprisingly small (only 3 percent in 2007).[17]

In 2007, there were around 700 Internet service providers (ISPs) in the U.K.[18] Of the broadband providers, however, Virgin Media and BT (formerly British Telecom) provided services for half of the market;[19] along with the three next largest providers, they comprise 84 percent of the market.[20] Broadband service has expanded so significantly in the last four years that it is now more affordable than dial-up service.[21] Currently, no restrictions exist on the amount of information a user can send and receive when subscribing to broadband service, but it is recognized that network management might be required in the future.[22]

In December 2008, the majority of ISPs in the U.K. agreed to better inform their customers about Internet connection speeds. This scheme, which would benefit approximately 95 percent of the U.K.'s Internet users, was adopted in response to consumer confusion about advertisements that promised broadband speeds that were largely unattainable.[23]

Legal and Regulatory Frameworks

The telecommunications industries are regulated by the Office of Communications (Ofcom).[24] Ofcom's mandate includes, among other duties, the protection of audiences against harmful material, unfairness, and infringements of privacy.[25] Broadcasting in the U.K. is regulated by the Department for Culture, Media, and Sport (DCMS).[26]

As a member state of the European Union, the U.K. has integrated the bloc's communication directives into its national law. The European Parliament has recently voted on the new proposals by the European Commission (EC) to reform the telecommunications regulations with the idea of promoting competition on a pan-European level and taking further steps to preserve information security, including controlling spam, spyware, and other malicious software.[27] Updated regulations are expected to be integrated into national legislation starting in 2010.

In 2000, the EU adopted a proposal concerning, inter alia, the dissemination of child pornography on the Internet.[28] The notes to the proposal explicitly state that service providers normally will not be held liable for any dissemination, caching, or hosting of child pornography, though they are held liable if they commit illegal acts that benefit the service provider.[29] This is consistent with broader EU law which states that ISPs acting as ''mere conduits'' of information are not liable for any illegal information transmitted.[30] European Union law specifically provides that ISPs are under no obligation to monitor the information they transmit, but they must be able to provide information on its transmission given an appropriate request from the government.[31]

Though U.K. authorities do not oblige ISPs to monitor the information being transmitted, at least one major ISP, BT, filters child pornography materials.[32] However, BT stresses that they do not affirmatively search for sites to block, but rather act only upon reports by users and information provided by the Internet Watch Foundation

(IWF).[33] The implementation of this filtering practice is known as ''CleanFeed.''[34] The IWF, a nonprofit organization based in the U.K. that works with the U.K. government, compiles a list of Web sites it deems illegal and transmits this information to BT and other ISPs.[35] The list compiled by the IWF usually contains 800–1,200 unique and live URLs.[36] In addition to filtering content for child sexual abuse, the IWF also detects and attempts to take down Web sites hosted in the U.K. that promote racial hatred,[37] which are illegal under the Public Order Act 1986.[38]

In 2006, Home Office Minister Vernon Croaker announced that from 2008 onward he expected that all ISPs would block access to child pornography using a ''CleanFeed'' style system.[39] The announcement also suggested that if the filtering was not done by ISPs on a voluntary basis, Parliament would consider legislative enforcement.[40] At that time, the largest ISPs in Britain, which together provided over 90 percent of all broadband access, all used some sort of filtering system.[41]

The U.K. commissioned a report on child safety on the Internet that was released in March 2008 (the Byron Report).[42] This report recognized that it would not be possible to remove fully all obscene material from the Internet and that any effective control would have to be adopted voluntarily by ISPs.[43] It stated that there was a strong case to block illegal material such as child pornography, though it also recommended that no attempts be made to filter illegal material at the network level.[44] The U.K. government has agreed to implement all the recommendations contained in the Byron Report.[45]

In December 2008, a number of British ISPs blocked a Wikipedia page displaying an image of an album cover from 1976 that portrayed a naked teenage girl. The ISPs made the decision after receiving a warning from the IWF claiming the image may be illegal. Wikipedia users complained that the ISPs blocked not only the image but the entire article; they also noted that the ISPs did not apply the block systematically, as access to commercial sites, such as Amazon.com, that sold the album and displayed its cover image, was still available.[46] Furthermore, the block temporarily prevented users on the affected ISPs from editing Wikipedia.[47] Several days after the block was imposed, the IWF reviewed the case and decided to remove the article from their list of offensive sites, citing the negative effects of the block and the wide availability of the image on other sites.[48]

United Kingdom law requires that information that glorifies or incites terrorism be censored.[49] According to section 3 of the Terrorism Act (2006), once provided with a notice that a Web site may contain terrorism-related content, an ISP may be liable for the content if it does not take every reasonably expected step to block access to the content.[50]

Filtering technologies such as the ''CleanFeed'' system are criticized for not publicizing the list of filtered Web sites, which could lead to abuses.[51] In addition, because

ISPs and the IWF are not public institutions, they are not subject to judicial review.[52] Instead, the IWF offers an internal appeal procedure.[53]

Internet Surveillance

The U.K., together with the United States, was ranked as one of the worst offenders against individual privacy rights in the democratic world by Privacy International for 2007.[54]

Among areas of great concern are the estimated 4 million CCTV cameras installed in practically every corner of Britons' social life.[55] Based on the EU Data Retention Directive but at times exceeding its scope, the data retention scheme in the U.K. took a significant step forward. There are ''hundreds of thousands'' of requests from state agencies to communications providers for traffic data.[56]

In the U.K., the Information Commissioner's Office (ICO) is an independent authority with the goal of promoting access to official information and protecting personal information. It is also responsible for enforcing the Data Protection Act 1998 (DPA).[57] The commissioner has a broad mandate but only minimal enforcement powers.[58] A new act has been proposed to amend the DPA and give the ICO the authority to impose fines for deliberate data protection breaches.[59] The ICO reports to Parliament and is sponsored by the Ministry of Justice.[60] Recently, concerns have arisen over ISPs tracking user activity to customize viewed ads.[61] The commissioner himself warned in 2004 that the U.K. was in danger of becoming a ''surveillance society.'' This concern was reiterated in the House of Lords' February 2009 report entitled ''Surveillance: Citizens and the State.''[62] However, after a review of the situation the ICO noted that as long as users are ''informed when a cookie is placed on their computer, given clear and comprehensive information about the purpose of the storage and given the ability to refuse it being placed on the system . . . there does not appear to be any detriment to users,'' and that the developing companies are not in violation of the Data Protection Act 1998.[63]

The U.K. government's power to collect communications data is primarily addressed in the Regulation of Investigatory Powers Act 2000 (RIPA).[64] Warrants to approve the collection of communication content are issued by the Secretary of State upon proof that the intrusion is necessary and proportionate when balanced with individuals' privacy interests.[65] The Secretary of State has broad powers that are loosely regulated.[66] The collection of noncontent data, including subscriber information, traffic, and location data, can be authorized without a warrant by various public officials.[67]

As for other electronic surveillance, the Foundation for Information Policy Research notes that even before the events of September 11, 2001, the U.K. was utilizing sophisticated systems for electronic surveillance against crime. The foundation warns that

further ''safeguards and democratic oversight'' are needed.[68] On May 21, 2008, *The Guardian* warned of the possibility of a database that records every telephone call, e-mail, and Web site visit made in Britain.[69] On June 9, 2008, the ICO released a statement recognizing the necessity to consider the impact of the development of such tools on individuals' privacy and the need to minimize unnecessary intrusion. It further recommends that ''every possible step ... be taken to ensure public trust in the way that personal information is collected and stored.''[70] Although plans for the database to collect all user information were canceled, the Home Secretary has requested that communications firms record contact between customers, including e-mails, phone calls, and Internet use, as well as visits to social networking sites.[71]

In a different area, expectations of commercial gain due to online advertising have led some of the most important operators in the country (BT, Talk Talk, and Virgin) to use different applications to track the browsing history of their customers. In April 2009, the EU expressed its intent to commence legal actions against the U.K. for allowing this Web-tracking practice, which, according to the EU, would violate privacy laws.

ONI Testing Results

The OpenNet Initiative comprehensively tested three ISPs in the United Kingdom: Easynet,[72] Be,[73] and BT,[74] and did not find any evidence of filtering; however, the U.K. openly blocks child pornography Web sites (which ONI does not test) and has allegedly blocked other sites containing ''illegal material.''[75]

Conclusion

Protecting freedom of expression and encouraging tolerance to diverse viewpoints, the U.K. is one of the pioneers in nurturing politically sensitive debates and promoting the use of new technology. Freedom of expression and protection of privacy over the Internet is guaranteed in the law. Nevertheless, motivated by national security concerns, the state has provided for vast surveillance measures over online communications. Moreover, certain filtering and tracking practices do take place. Such practices are sometimes encouraged by the state but most often voluntarily implemented by private operators. The U.K. government, however, has to ensure that blocking practices do not lead to abuse in the absence of external and independent control.

Notes

1. *BBC News*, ''Country Profile: United Kingdom,'' http://news.bbc.co.uk/2/hi/europe/country_profiles/1038758.stm.

2. Central Intelligence Agency, ''The World Factbook: United Kingdom,'' https://www.cia.gov/library/publications/the-world-factbook/geos/uk.html.

3. BBC, ''About the BBC: How the BBC Is Run,'' http://www.bbc.co.uk/info/running/.

4. BBC Trust, ''About the Trust,'' http://www.bbc.co.uk/bbctrust/about/index.html.

5. *BBC News*, ''Country Profile: United Kingdom,'' http://news.bbc.co.uk/2/hi/europe/country_profiles/1038758.stm.

6. Reporters Without Borders, ''United Kingdom,'' http://www.rsf.org/article.php3?id_article=25478&Valider=OK.

7. Amnesty International, ''UK—Amnesty International Report 2008,'' http://www.amnesty.org/en/region/uk/report-2008.

8. Privacy International, ''United Kingdom of Great Britain and Northern Ireland,'' 2007, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559479.

9. Ibid.

10. Om Malik, ''Broadband Subscribers, 300 Million Strong,'' *GigaOm*, June 22, 2007, http://gigaom.com/2007/06/22/broadband-subscribers-300-million-strong/.

11. National Statistics Online, ''Internet Access: 65% of Households Had Access in 2008,'' August 26, 2008, http://www.statistics.gov.uk/cci/nugget.asp?id=8.

12. Ofcom, ''The Consumer Experience—Research Report 07,'' http://www.ofcom.org.uk/research/tce/ce07/.

13. National Statistics, ''Internet Access 2007: Households and Individuals,'' http://www.statistics.gov.uk/pdfdir/inta0807.pdf.

14. Ibid.

15. Ibid.

16. Central Intelligence Agency, ''The World Factbook: United Kingdom,'' https://www.cia.gov/library/publications/the-world-factbook/geos/uk.html.

17. National Statistics, ''Internet Access 2007: Households and Individuals,'' http://www.statistics.gov.uk/pdfdir/inta0807.pdf.

18. Ofcom, ''The Consumer Experience—Research Report 07,'' http://www.ofcom.org.uk/research/tce/ce07/.

19. Ibid.

20. Ibid.

21. Ibid.

22. Ibid.

23. *BBC News*, ''Net Speed Rules Come into Force,'' December 4, 2008, http://news.bbc.co.uk/2/hi/technology/7764489.stm.

24. Ofcom, ''Statutory Duties and Regulatory Principles,'' http://www.ofcom.org.uk/about/sdrp/.

25. Ibid.

26. BBC, ''About the BBC: How the BBC Is Run,'' http://www.bbc.co.uk/info/running/.

27. European Commission, ''eCommunications: Reforming the Current Telecom Rules,'' http://ec.europa.eu/information_society/policy/ecomm/tomorrow/index_en.htm.

28. Activities of the European Union, Summaries of Legislation, ''Combating Trafficking in Human Beings, the Sexual Exploitation of Children and Child Pornography,'' December 20, 2006, http://europa.eu/legislation_summaries/employment_and_social_policy/equality_between_men_and_women/l33089b_en.htm.

29. Ibid.

30. Council Directive 2000/31, art. 12, 2000 O.J. (L 178) 1 (EC).

31. Ibid. at art. 15.

32. *Fronterra*, ''Facing Up to ... Extreme Abuse of the Internet,'' May 2004, http://www.btplc.com/Societyandenvironment/Ourapproach/CSRresources/Hottopics/Abuseoftheinternet/Abuseoftheinternet.pdf; BT, ''The Historical Development of BT,'' http://www.btplc.com/Thegroup/BTsHistory/History.htm.

33. *Fronterra*, ''Facing Up to ... Extreme Abuse of the Internet,'' May 2004, http://www.btplc.com/Societyandenvironment/Ourapproach/CSRresources/Hottopics/Abuseoftheinternet/Abuseoftheinternet.pdf.

34. IWF/BT Project CleanFeed, ''Extreme Pornography Websites,'' http://www.iwf.org.uk/government/page.101.220.htm.

35. Internet Watch Foundation (IWF), http://www.iwf.org.uk/.

36. Internet Watch Foundation, ''IWF URL list,'' http://www.iwf.org.uk/public/page.148.htm.

37. Internet Watch Foundation, ''Role and Remit,'' http://www.iwf.org.uk/public/page.35.htm.

38. Public Order Act, chapter 64, section 4, Fear or Provocation of Violence.

39. 446 Parl. Deb., H.C. (6th ser.) (2006) 709W.

40. Ibid.

41. Ibid.

42. Tanya Byron, ''Safer Children in a Digital World: The Report of the Byron Review,'' March 2008, http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf.

43. Ibid.

44. Ibid.

45. Press Release, Department for Culture, Media, and Sport and Department for Children, Schools, and Families [U.K.], ''Government Commits to Delivering Byron Recommendations,'' March 27, 2008, http://www.culture.gov.uk/reference_library/media_releases/5061.aspx/.

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

47. Barry Collins, ''Brits Blocked from Wikipedia over Child Porn Photo,'' *PC Pro*, December 8, 2008, http://www.pcpro.co.uk/news/241440/brits-blocked-from-wikipedia-over-child-porn-photo.html.

48. ISPreview, ''Internet Watch Foundation U-Turns on Wikipedia Block,'' December 10, 2008, http://www.ispreview.co.uk/news/EkkllAlVuVbKzPsVgN.html.

49. Terrorism Act, 2006, c. 11 (U.K.).

50. Ibid. at sec. 3.

51. Lillian Edwards, ''From Child Porn to China, in One Cleanfeed,'' *SCRIPT-ed*, vol. 3, no. 3, 174 (2006), http://www.law.ed.ac.uk/ahrc/script-ed/vol3-3/editorial.pdf.

52. Ibid.

53. Internet Watch Foundation, ''Complaints, Appeals and Correction Procedures,'' http://www.iwf.org.uk/public/page.148.341.htm.

54. Privacy International, ''The 2007 International Privacy Ranking,'' http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597.

55. *BBC News*, ''Warning over 'Surveillance State,''' February 6, 2009, http://news.bbc.co.uk/1/hi/uk_politics/7872425.stm.

56. Privacy International, ''The 2007 International Privacy Ranking.''

57. Data Protection Act 1998, http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1.

58. The Information Commissioner is appointed by Her Majesty by Letters Patent; House of Lords report, ''Surveillance: Citizens and the State,'' February 6, 2009, http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf.

59. Section 55A was inserted into the DPA by Section 144 of the Criminal Justice and Immigration Act (CJIA) 2008, not yet in force. As reported in ''Response to the Data Sharing Review Report,'' http://www.justice.gov.uk/docs/response-data-sharing-review.pdf.

60. Information Commissioner's Office, ''About the ICO,'' http://www.ico.gov.uk/about_us.aspx.

61. Cahal Milmo, ''Internet's Founder Attacks Scheme to Monitor Web Usage,'' *The Independent*, March 18, 2008, http://www.independent.co.uk/life-style/gadgets-and-tech/news/internets-founder-attacks-scheme-to-monitor-web-usage-797133.html.

62. House of Lords report, ''Surveillance: Citizens and the State,'' February 6, 2009, http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf.

63. Information Commissioner's Office, ''Phorm—Website and Open Internet Exchange,'' April 18, 2008, http://www.whatdotheyknow.com/request/10456/response/30346/attach/2/Phorm%20the%20ICO%20view%2018%20April%2008%20v1.3.doc.doc.

64. Regulation of Investigatory Powers Act 2000, Chapter 23, http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; for ECHR compliance, see ''Editorial,'' Crim. L.R. 2000, Nov, 877–878, http://www.homeoffice.gov.uk/documents/cons-2003-access-comms-data. Part II covers surveillance, differentiating ''directive'' from ''intrusive'' surveillance.

65. Regulation of Investigatory Powers Act 2000, Chapter 23.

66. Ibid.

67. Various offices, ranks, or positions within the public authorities are ''persons designated'' by the Secretary of State in Part I Chapter II of RIPA.

68. Foundation for Information Policy Research, http://www.fipr.org.

69. Bobbie Johnson, ''Plan to Record All Calls and Emails Alarms Watchdogs,'' *The Guardian*, May 21, 2008, http://www.guardian.co.uk/technology/2008/may/21/freedomofinformation.civilliberties.

70. ICO, ''Statement on Home Affairs Committee,'' June 9, 2008, http://www.ico.gov.uk/upload/documents/pressreleases/2008/statement_home_affairs_committee.pdf.

71. Dominic Casciani, ''Plan to Monitor All Internet Use,'' *BBC News*, April 27, 2009, http://news.bbc.co.uk/2/hi/uk_news/politics/8020039.stm.

72. Easynet, http://www.easynet.com/gb/en/.

73. Be, https://www.bethere.co.uk/.

74. BT UK, http://www.bt.com/.

75. Internet Watch Foundation, ''IWF Facilitation of the Blocking Initiative,'' http://www.iwf.org.uk/public/page.148.htm.