Internet Filtering in **Europe**

Introduction

In less than a decade, the Internet in Europe has evolved from a virtually unfettered environment to one in which filtering in most countries, particularly within the European Union (EU), is the norm rather than the exception. Compared with many of the countries in other regions that block Internet content, the rise of filtering in Europe is notable because of its departure from a strong tradition of democratic processes and a commitment to free expression. Filtering takes place in a variety of forms, including the state-ordered takedown of illegal content on domestically hosted Web sites, the blocking of illegal content hosted abroad, and the filtering of results by search engines pertaining to illegal content. As in most countries around the world that engage in filtering, the distinction between voluntary and state-mandated filtering is somewhat blurred in Europe. In many instances filtering by Internet service providers (ISPs), search engines, and content providers in Europe is termed "voluntary" but is carried out with the implicit understanding that cooperation with state authorities will prevent further legislation on the matter.

The scope of illegal content that is filtered in Europe largely is limited to child pornography, racism, and material that promotes hatred and terrorism, although more recently there have been proposals and revisions of laws in some countries that deal with filtering in other areas such as copyright and gambling. Filtering also takes place on account of defamation laws; this practice has been criticized, particularly in the UK, for curtailing lawful online behavior and promoting an overly aggressive notice-and-takedown policy, where ISPs comply by removing content immediately for fear of legal action. ISPs in Europe do not have any general obligation to monitor Internet use and are protected from liability for illegal content by regulations at the European Union (EU) level, but must filter such content once it is brought to their notice. Therefore the degree of filtering in member states depends on the efforts of governments, police, advocacy groups, and the general public in identifying and reporting illegal content.

Efforts over the past decade have been underway to create a set of common policies and practices at the EU-level on Internet regulation. This is viewed as necessary to promote regional competitiveness and commerce, to counter Internet crime and terrorism, and to serve as a platform to share best practices amongst nations. Notable advancements in regulation at the EU level—although not directly in the area of filtering—include the definition of ISP liability toward illegal content and obligations toward data retention.

Regional regulation

A recurring theme throughout this overview will be the overlapping nature of individual country-level law and regionwide regulation. Countering criminal activity on the Internet and promoting the overall competitiveness of the Internet industry have been the primary reasons cited to develop a regional regulatory framework.[1] A regional approach in Europe has its beginnings with a request by the European Council to the European Commission in April 1996 to produce "a summary of problems posed by the rapid development of the Internet" and to assess the need for regulation. The Commission produced a report titled "Illegal and Harmful Content on the Internet" and a Green Paper on "The Protection of Minors and Human Dignity in Audiovisual Services" in response. Based on these documents, "a common framework for self-regulation (of the Internet) at the European level" was drafted, which culminated in an Action Plan on Promoting Safe Use of the Internet. The plan, adopted on January 25, 1999 and operational up to 2002, outlines the basic principles underlying Internet content regulation at the European level.[2] Broadly, undesirable content on the Internet is classified either as "illegal" or "harmful."

The scope of "illegal" content tends to vary between countries, although there are certain issues where there is a greater amount of consensus, such as child pornography, trafficking in human beings, racist material, material promoting terrorism, and all forms of Internet fraud (such as credit card fraud).[3,4] "Harmful" material, as defined in the plan, is that which might offend the values and sentiments of others and could pertain to politics, religion, or racial matters, and could also vary significantly between cultures.

The plan emphasizes the need for action in five broad areas in order to curb illegal and harmful content on the Internet:[5]

1. promoting voluntary industry self-regulation and content monitoring schemes, including the use of hotlines for the public to report illegal or harmful content;
2. providing filtering tools and rating systems that enable parents or teachers to regulate the access of Internet content by children in their care, while allowing adults access to legal content;
3. raising awareness about services offered by industry among users to allow them to leverage the Internet more fully;
4. exploring the legal implications of promoting the safer use of the Internet; and
5. encouraging international cooperation in the area of regulation.

Europe also maintains a regional policy that is generous in limiting ISP liability under the Electronic Commerce Directive, 2000/31/EC. Article 12, the "mere conduit" exception provision, absolves ISPs from liability for information transmitted over their networks as long as they did not initiate the message, select or modify the information, or select the intended recipients. The exemption also extends to the "automatic, intermediate and transient" storage of information, provided it is for a "reasonable period." The latter is left to be specified by member states. Article 13 deals with caching—granting exemption from liability for the "automatic, intermediate and tem-

porary storage of information" that is carried for the exclusive purpose of making onward transmission more efficient. Article 14 addresses the liability associated with hosting content, stating that ISPs "will not be liable for hosting information, provided they do not have actual knowledge that the activity is illegal and, upon obtaining such knowledge, act quickly to remove it."[6] Finally, Article 15 precludes ISPs from any general obligation to monitor content or data transmitted or stored through their services. Further, ISPs are not required to actively seek facts that might indicate illegal activity.[7] These provisions granting ISPs substantial immunity from liability over illegal content are consistent with the law and practice of many other countries around the world that seek to expand Internet use and promote freedom of expression.

Social filtering

Action to regulate obscene content started with individual countries and the implementation of voluntary ISP-level filtering programs. The landmark model of large-scale voluntary ISP filtering in Europe originated in the UK.[8] BT, Britain's largest ISP, serving about a third of the country's home Internet users, launched Project Cleanfeed in June 2004[9] in consultation with the British Home Office. Under the auspices of this project, BT filters Internet content based on a blacklist of Web sites hosted anywhere in the world that contain images of child abuse as defined by the amended Protection of Children Act, 1978.[10] The list is compiled by the Internet Watch Foundation (IWF), a not-for-profit organization, in consultation with government, industry, the police, and the public. IWF provides the list to its members, which today include ISPs, mobile network operators, content providers, and search engines such as Google and Yahoo![11] Those attempting to access the illegal content hosted abroad receive an error message as if the particular page were unavailable as a result of other connectivity problems.[12] Illegal content that is hosted within the UK, including child abuse images and content that is criminally obscene or incites racial hatred, is required to be taken down by ISPs and content providers under a notice-and-takedown regime.[13] Although this form of filtering is termed "voluntary," by the end of 2007 all broadband consumer ISPs in Britain are expected to have implemented a similar system, failing which, regulatory enforcement might be considered.[14,15] Other countries, such as Norway, Sweden, Denmark, and Italy, have implemented similar programs, while Finland is currently considering doing so.[16]

Filtering also takes place through "voluntary self-regulation" by search engines. As of early 2005 all major search engines in Germany — Google, Lycos Europe, MSN Deutschland, AOL Deutschland, Yahoo, T-Online, and t-info — have formed an organization that coordinates filtering of search results that are harmful to minors, based on a list provided by a government agency in charge of media classification. The move is seen as a response to pressure for voluntary self-regulation by industry at the EU level, and arguably to the fear among industry that a failure to comply will result in increased legislation. The system has been criticized, however, for a lack of transparency,[17] since the search engines cannot disclose the list of Web sites to the public, as per a codex signed by them.[18] In addition, disclosure would defeat the purpose of filtering search results, as the sites are removed only from the search results, not from the Internet.

Internet content is also monitored through online surveillance by authorities in the UK. The Child Exploitation and Online Protection Centre (launched in April 2006) made thirteen arrests in July 2006 after beginning investigations into pay-per-view Internet services.[19] The police in Britain have also been vested with the power to pass on to banks the personal details of those who access illegal content online using credit cards, based on an amendment to the Data Protection Act (1998).[20] Banks will then cancel the cards as a breach of their terms of service.

The public in nineteen European countries assists in identifying and reporting illegal content —particularly in the area of child pornography — through a network of hotlines that have been implemented on the basis of a recommendation at the EU level.[21] In Austria authorities were able to uncover a "child-pornography ring" involving seventy-seven countries in February 2007, based on a report by a man working for a Vienna-based Internet file-hosting service.[22] Recent reports show that the Save the Children Denmark Hotline, financed jointly by Denmark and the European Commission's Safer Internet Plus Programme, had nearly 9,000 reports of child abuse images in 2006 alone.[23] The police in Spain were able to arrest ninety people in 2004 in the country's largest operation against the distribution of child pornography, facilitated by the hotlines. The INHOPE Association acts as the coordinator of the network of hotlines, including in countries outside Europe such as Australia, Brazil, Canada, South Korea, Taiwan, and the United States.[24]

Although early filtering efforts had fairly limited agendas, proposals and laws are emerging in many nations toward filtering in other social realms, such as gambling and betting. A proposal was drafted in 2002 to revise Swiss federal laws on lotteries and betting, such that those providing access to games that are considered illegal face fines up to 1 million Swiss francs or up to a year of imprisonment. This effort was suspended in 2004, and no further action has been taken since. As of February 2006 ISPs in Italy are required to block access to Web sites that offer online gambling. The list of Web sites to be blocked is compiled by the Autonomous Administration of State Monopolies (AAMS, a part of the Ministry of Economy and Finances), which issued the decree.[25] The most broad-based proposal yet for filtering comes from Norway, where the government is considering blocking access to foreign gambling sites, Web sites that "desecrate the Flag or Coat of Arms of a foreign nation," sites that promote hatred toward public authorities, contain hate speech or promote racism, offensive pornography sites, and peer-to-peer sites that offer illegal downloads of music, movies, or television shows.[26]

Nationalistic filtering

There are no examples in Europe of filtering carried out to silence political opposition such as those that the ONI has documented in other regions. There are, however, examples of filtering that seeks to maintain the legitimacy of government institutions and preserve national identity. In December 2002 a local Swiss magistrate, Françoise Dessaux, ordered several Swiss ISPs to block access to three Web sites hosted in the United States that were strongly critical of Swiss courts,[27] and to modify their DNS servers to block the domain appel-au-people.org.[28] The Swiss Internet User Group and the Swiss Network Operators Group protested that the blocks could easily be bypassed and that the move was contrary to the Swiss constitution, which guarantees "the right to receive information freely, to gather it from generally accessible sources and to disseminate it" to every person. However, there was strong enforcement, as the directors of noncompliant ISPs were asked to appear personally in court, failing which they faced charges of disobedience.

On March 7, 2007, the video-sharing Web site YouTube was blocked in Turkey as per a court order, following the posting of certain videos on the site that were found to be derogatory toward Turkey's founding father, Mustafa Kemal Ataturk, the Turkish people in general, and the Turkish flag. The blocking invoked Article 301 of the Turkish Penal Code, known as the main obstacle to freedom of speech, which defines insults toward Ataturk as well as "Turkishness" as a crime. Turkey's leading ISP, Turk Telecom, complied with the order but petitioned to the court to allow access to the site to be restored. The court agreed on the condition that the particular videos

were removed. The two-day blocking was heavily criticized both within Turkey and abroad and likened to "closing a library because of a single book that was found to be improper."[29]

Hate speech

European states are also increasingly taking action against online hate speech, applying their offline policies to the Internet. Some efforts raise important issues such as the jurisdiction over material on the Internet. For example, a French court in 2000 ruled that U.S.-based Yahoo! Inc. is liable under French law for allowing the people of France access to auction sites that include Nazi memorabilia and demanded that Yahoo! must ensure that this content is impossible to access from France or face fines.[30] The case was brought by two French not-for-profit organizations[31] dedicated to fighting anti-Semitism.[32] Yahoo! brought suit in a U.S. District Court in San Francisco, claiming that the French court's ruling was unenforceable in the United States. The U.S. court ruled in Yahoo!'s favor in November 2001, but in 2004 a panel of the 9th U.S. Circuit Court of Appeals overturned the ruling by the lower court on the grounds that it "did not have sufficient jurisdiction over the French parties."[33] After reconsidering the decision, the 9th U.S. Circuit Court of Appeals dismissed Yahoo!'s case in January 2006 despite claiming jurisdiction over the matter because Yahoo! had already removed the materials and, therefore, the requirement to block would not have done any actual First Amendment harm.[34]

Similarly, the German Federal Court of Justice ruled in December 2000 that material glorifying the Nazis and denying the Holocaust must be censored as per German law, regardless of where it is hosted, based on a case involving an Australian-based Holocaust revisionist who was using the Internet to spread his message denying the atrocities of World War II.[35] In another case, seventy-eight ISPs in Nordrhein-Westfalen were ordered to block access to two foreign Web sites in 2002 that contained neo-Nazi content.[36] The same regional government of Düsseldorf also took an anti-censorship activist to court for posting hyperlinks on his Web site to radical rightwing content that had been censored.[37]

Other European countries also have laws against Holocaust denial and ban material that promotes racial hatred. These have been "harmonized" in a protocol to the Council of Europe's cybercrime treaty, which requires that "any written material, any image, or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as pretext for any of these factors" and "material which denies, minimizes, approves of or justifies crimes of genocide or crimes against humanity" must be made illegal by the signatories.[38] As with all illegal content, once brought to their attention, ISPs must either take down or block the relevant Web sites depending on whether the sites are hosted within the country or abroad.

Defamation

Member states of the EU have expressed the need for a simplified framework to be applied with respect to rules concerning defamation by media or publications via the Internet and other electronic networks. The general principle in cases of defamation concerning the media—that the law of the country where the defamed person lives is applicable—implies that media organizations must know the privacy and defamation laws of each European country, which is criticized as impractical. In Italy, for example, in 2000, a man in "a trans-border custodial battle" claimed that his ex-wife, now resident in Israel, was responsible for posting statements and images on the Internet that were defamatory of him and derogatory of his ability to care for their two daughters. The Italian Supreme Court, or Suprema Corte di Cassazione, overturned a prior verdict from a

lower court, affirming that Italy's laws of libel apply to content on foreign Web sites accessible by Internet users in the country.[39] The Court held that while the offending statements were posted outside of Italy, the effects were felt within the country and were therefore subject to the national laws.

The issue of the need for a unified framework was brought to the fore once more in February 2007 as a part of the European Parliament's second reading of the Rome II Regulation, which seeks to establish rules on the applicable law to noncontractual obligations relevant to publications via the Internet and other electronic networks. The Parliament's proposed amendment is that the law applicable should be that of the country to which "the publication or broadcast is most directed," which is to be determined "by the language of the publication or broadcast, or by sales or audience size in a given country as a proportion of total sales or audience size, or by a combination of these factors." Further, the amendment suggests that if these are not easy to determine, "the relevant law will be the one of the country where editorial control is exercised." With regard to the right to reply, it is suggested that the applicable law should be that of the country in which the publisher or broadcaster has its "habitual residence." The text, which has been adopted by the Parliament, is not expected to find easy favor with the European Council and must undergo a standard conciliatory procedure where member states and Members of European Pariliament, in equal representation, debate the proposal, and it will be approved as a regulation if an acceptable compromise is reached.[40]

In their current form, defamation laws at the country level, particularly in the UK, have been criticized for leading to a "Web takedown" culture where ISPs immediately remove content that is allegedly defamatory when brought to their notice, for fear of facing law suits. The concern in the UK, as in other nations, is that this can have a "chilling effect" on lawful online content and behavior.[41]

A landmark precedent in the UK led the way for the establishment of a notice-and-takedown system. In *Laurence Godfrey v. Demon Internet Limited,* a defamatory statement was made on a posting to a newsgroup called "soc.culture.thai," available on a server at the provider Demon Internet Limited. The message was found to be forged and only appeared to come from Godfrey. Despite a request by Godfrey to take down the content, as it was defamatory of him, the ISP did not comply. As a result, he claimed damages for libel under §1 of the Defamation Act, 1996, and settled with Demon out of court.[42]

Libel law in the UK has been known to be particularly sympathetic to libel plaintiffs—and is often contrasted with the law in the United States in this context—such that many individuals from outside countries have sued publications in the UK, despite a relatively small circulation there, for a better chance of winning. However, the *Jameel v. Wall Street Journal Europe* case significantly increased press protections against libel claims in October 2006.[43] There has also been debate over whether the protection of the reputation of individuals is in conflict with the Human Rights Act of 1998, insofar as it might infringe upon the right to free speech.[44]

Copyright

A few countries in Europe have begun to employ Internet filtering to combat copyright infringement, evolving toward the notice-and-takedown approach used in the United States. In Denmark, as per a ruling of the Copenhagen City Court on October 2006, TDC, the country's largest ISP, blocked access to a Web site that distributes illegally copied music.[45] In February 2007, as mentioned earlier, Norway proposed filtering on a much larger scale that would include blocking of peer-to-peer sites offering illegal downloads of music, movies, and television shows.[46]

On March 16, 2007, the police arrested the owner of www.arenabg.com, which is one of Bulgaria's largest BitTorrent trackers and one among the country's ten most popular Web sites,[47] providing links to copyrighted music, movies, and software.[48] Although the owner was released within twenty-four hours, the Web site was filtered by police order for the period March 16–19, on the grounds that it was "necessary to prevent foreign interference with the torrent trackers."[49] The order to filter the site was lifted by the General Office for Fighting Organized Crime, but has resulted in considerable citizen protest for what is considered unjust treatment toward the owners and operators of torrent sites.[50] Following the arrest, other tracker Web sites have reportedly closed, some under threat of confiscation of property by the police, or have moved their servers abroad to avoid prosecution under the Bulgarian Copyright Law. The extent of actual filtering of these sites in the country is not known because there are differing reports regarding accessibility by various ISP subscribers. Given that BitTorrent trackers point to content but do not host it, the legal recourse to deal with the copyright violation associated with these Web sites is especially unclear.[51]

Law suits concerning alleged copyright infringement by search engines have been raised in a few countries, with recent rulings in favor of a notice-and-takedown policy that could arguably serve as a precedent for other countries in the region. In February 2007 the Brussels Tribunal found Google Inc. to be in violation of national copyright laws in a case raised by Copiepresse of Belgium, a trade group representing seventeen of Belgium's French- and German-language newspapers, and the company was fined 2.4 million pounds for the breach.[52] As per a translation of the ruling, "the reproduction and publication of headlines as well as short extracts, and the use of Google's cache, the publicly available data storage of articles and documents, violate the law on authors' rights."[53] The former refers to the Google News service,[54] while the latter to Google Web Search. The outcome is that Google cannot include references to articles, pictures, or drawings of Copiepress members through its Google News service without prior agreements, and must remove Belgian newspaper content from its search results. Failure to comply will result in fines of 25,000 euros a day.

Google intends to appeal against the judgment, stating that Web search results and the news service in fact drive more traffic toward the newspaper Web sites, and that Google News does not earn any advertising revenue from this. Copiepress, however, holds that by allowing users to bypass the front pages of newspapers and link directly to articles, newspapers lose advertising revenue. In addition, by making old newspaper material available through its cache, newspapers effectively lose the ability to charge customers for access to their archives, while Google Web Search does in fact earn advertising revenue for this service. The court ruling also states that all copyright holders can notify Google in case of infringement, and the search engine will have to remove content within a twenty-four-hour period or pay a 1,000 euro daily fine.[55] This could lead to an attitude of risk aversion and immediate compliance on the part of ISPs, content providers, and search engines—similar to instances of alleged defamation—in the face of potential law suits.

Google had run into similar difficulty in France with respect to its news service when Paris-based Agence France Presse (AFP) had sued the company for USD 17.5 million in 2005. The suit was dropped in April 2007, following a licensing agreement where Google would be allowed to use stories and photographs from AFP for its news aggregator and for other Google services, including products that Google is expected to launch in the future. The financial terms of this arrangement have not been publicly disclosed.[56] Out-of-court settlements in Europe for copyright infringement should not be surpris-

ing, because the legal defenses available in the region for alleged infringers are relatively weak.[57]

At the regional level, Intellectual Property Rights pertaining to Internet content are addressed by two directives: the Copyright and Related Rights in the Information Society adopted on April 9, 2001, and the Electronic Commerce Directive 2000/31/EC, which came into force on June 8, 2000. Article 5(1) of the Copyright Directive exempts ISPs from liability for copyright infringement where "reproduction is transient or incidental" or where copies are an integral part of a technological process "whose sole purpose is to enable onward transmission in a network between third parties by an intermediary or a lawful use of a work or other subject-matter to be made." The Copyright Directive also exempts ISPs from liability where the copies have "no independent economic significance"; this is left to be adjudged independently by courts in the respective member states. As per the first condition, ISPs and telecommunications operators do not need to request permission to transmit transient copies across their networks. However, the second condition implies that ISPs still face a situation of differing degrees of liability across the member states of the EU, and the directive has been criticized in this regard.[58] The Electronic Commerce Directive deals with the liability of ISPs toward content more generally, but with important implications for copyright. In particular, the directive provides a "mere conduit" exception, limits liability for content associated with the caching and hosting functions, and exempts ISPs from any general obligation to monitor.

Security

Security concerns in Europe have resulted in legislation concerning the surveillance and monitoring of Internet use. Although distinct from filtering, these have many parallels in their potential impact upon online freedom of speech. A recent and controversial area of legislation at the EU level in this regard pertains to the surveillance of traffic data and its retention. As per the European Data Retention Directive, which was passed in March 2006 and must be put into effect for Internet traffic by March 2009,[59] ISPs in the various nations are required to retain specific data pertaining to communications—in particular, with regard to Internet access, e-mail and telephony—for a period of at least six months but not exceeding two years. The data to be retained do not concern the content of communications. The aim is to bring about a "common code" of data retention in order to facilitate the tracing of illegal content and the source of attacks against information systems, and to identify those who use the electronic communications networks for terrorist activities and organized crime.[60] As the directive is implemented across the member states, privacy groups are concerned about the ability of ISPs, search engines,[61] and Web companies to retain data and monitor people's online habits. Moreover, the retention period of up to twenty-four months has been argued to be an unjustifiable length of time.[62]

An example of security legislation at the country level is a proposed law drafted in March 2007 in Sweden, which would give the national defense intelligence agency power to monitor all cross-border phone calls and e-mail traffic without court order. This will be carried out by the National Defence Radio Establishment in the form of searches for sensitive key words through the use of computer software. With some suggested amendments, the Swedish Legislative Council has approved the proposal to go forward. Concerns for privacy have been raised, including for communications within the country, which are often routed via servers hosted abroad.[63] Critics include the country's national security police agency, SAPO, which considers the proposal to be in violation of "personal integrity."

Conclusion

Filtering of online content takes a variety of forms among the states of Europe. Examples include orders issued by states to ISPs to take down Web sites that contain illegal content if they are hosted within the country, blocking orders by enforcement authorities for illegal content hosted abroad, and search engines that filter results pertaining to illegal content as a form of self-regulation. Although forms of filtering by search engines and ISPs are often referred to as "voluntary self-regulation" in some countries, there appears to be an implicit understanding that cooperation with government orders will forestall further legislation.

Filtering in European countries has also given rise to several legal disputes over the question of jurisdiction involving content that is hosted abroad. While the degree of filtering that takes place tends to vary among states, there is a concern in many countries over an apparent increase in the overall extent of filtering, as manifested in recent proposals and revisions in laws. Filtering in European states has, however, largely been confined to content that is illegal, and the extent has been tempered by public dialogue, adherence to law, and commitment to free speech, although the latter is more constrained than it is in the United States.

At the EU level there have been efforts over the past decade to create a common platform of "harmonized" Internet regulation. With regard to the filtering of online content, the emphasis has been on greater cooperation among industry, the public, and enforcement authorities within states, and increased voluntary industry self-regulation. Although EU level discussions were initially focused on various forms of illegal content online (in particular child pornography and racist and xenophobic content), there is increased attention being paid toward the use of the Internet for terrorism and organized crime in recent years. The latter has spurred legislation in the area of data retention, and much debate on the need for greater security measures versus the associated implications for privacy. There have also been recent advancements in terms of regulation at the EU level in the areas of defamation law, copyright, and defining ISP liability for online content. Creating a common platform for legislation at the regional level is a slow and complex process given the significant differences in the cultures and existing legislations in the countries of the European Union.

Author: Sangamitra Ramachander

NOTES

1. See http://europa.eu.int/ISPO/legal/en/internet/communic.html#f10 (accessed May 11, 2007).
2. This has been followed by the Safer Internet Action Plan (2002–2005) and the Safer Internet Plus Programme (2005–2008).
3. See http://europa.eu.int/ISPO/legal/en/internet/communic.html#f10 (accessed May 11, 2007).
4. Even in the case of child pornography, variations between countries exist pertaining to the definition of child pornography, the range of criminal activities that are subject to legislation (the possession, production, and dissemination of material, and so on), the means of investigation, and the penalties. For an overview of the national-level legislation and initiatives to counter child pornography in various countries, see http://www.inhope.org/en/about/about.html (accessed May 11, 2007).
5. See http://europa.eu.int/ISPO/legal/fr/internet/actplan.html (accessed May 11, 2007).
6. http://www.jisclegal.ac.uk/pdfs/isp_liability.pdf (accessed May 11, 2007).
7. However, member states might impose additional obligations for ISPs to immediately convey information to relevant authorities "of alleged illegal activities undertaken, or information provided by recipients of their service." ISPs might also have to provide, on request, information that enables the "identification of recipients of their service with whom they have storage agreements." See http://www.jisclegal.ac.uk/pdfs/isp_liability.pdf (accessed May 11, 2007).
8. Project Cleanfeed is cited as the "first mass censorship of the web attempted in a Western democracy," http://observer.guardian.co.uk/uk_news/story/0,6903,1232422,00.html.
9. For further information on Project Cleanfeed, see http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf (accessed May 11, 2007).

10. As of early 2006, 35,000 illegal images were being blocked daily and four million access attempts were recorded in a period of four months among BT subscribers.
11. http://www.theregister.co.uk/2006/12/29/iwf_feature/ (accessed May 11, 2007).
12. Although BT records the number of access attempts, it does not retain information pertaining to the identity of persons who attempt to access these Web sites. See http://technology.guardian.co.uk/news/story/0,,1704342,00.html (accessed May 11, 2007).
13. Internet Watch Foundation, "Frequently Asked Questions by the Media," (page modified January 15th, 2006), http://www.iwf.org.uk/media/page.70.215.htm (accessed May 11, 2007).
14. http://publicaffairs.linx.net/news/?p=518 (accessed May 11, 2007).
15. Project Cleanfeed was introduced in the aftermath of Operation Ore, an operation in the UK that formed a part of a large-scale international police operation to track down pedophiles on the Internet, under which 6,500 police investigations, 1,200 arrests, and 655 convictions were made in the country. The accused were identified based on credit-card information used to access a pedophile Web site hosted in the United States, passed on to the UK by the FBI. (The U.S. counterpart of the project, which preceded Operation Ore, is known as Operation Avalanche). See http://news.bbc.co.uk/2/hi/uk_news/2445065.stm (accessed May 11, 2007).
16. http://press.telenor.com/PR/200505/994781_5.html; http://www.financialmirror.com/more_news.php?id=2574; http://en.wikipedia.org/wiki/Internet_censorship (accessed March 7, 2007); http://www.edri.org/edrigram/number5.1/italy_blocking (accessed May 11, 2007).
17. http://blogs.law.harvard.edu/ugasser/2005/03/10#a52 (accessed May 11, 2007).
18. http://www.heise.de/english/newsticker/news/56817 (accessed May 11, 2007).
19. http://news.bbc.co.uk/1/hi/uk/5213058.stm (accessed May 11, 2007).
20. http://www.theregister.co.uk/2006/06/27/child_convictions_passed_to_banks/ (accessed May 11, 2007).
21. For the list of countries running hotlines and the organizations involved, see http://ec.europa.eu/information_society/activities/sip/projects/hotlines/index_en.htm.
22. http://www.cnn.com/2007/WORLD/europe/02/07/kids.online.porn.ap/index.html.
23. http://www.redbarnet.dk/Files/Filer/Seksuelt_misbrug/Pressemedfebruar07_eng.doc (accessed May 11, 2007).
24. http://ec.europa.eu/information_society/activities/sip/projects/hotlines/index_en.htm (accessed May 11, 2007).
25. http://www.edri.org/edrigram/number4.12/italybetting (accessed May 11, 2007).
26. Article available in Norwegian, http://www.dagbladet.no/dinside/2007/02/12/491719.html, cited in: http://www.opennetinitiative.net/blog/?p=144 (accessed May 11, 2007).
27. The contested Web sites were www.appel-au-peuple.org, http://de.geocities.com/justicecontrol, and www.swiss-corruption.com.
28. http://www.fitug.de/news/newsticker/newsticker120203210053.html.
29. http://www.edri.org/edrigram/number5.5/youtube-turkey (accessed May 11, 2007).
30. http://www.cdt.org/publications/policyposts/2005/5 (accessed May 11, 2007).
31. La Ligue Contre Le Racisme Et l'Antisemitisme (LICRA) and L'Union Des Etudiants Juifs De France.
32. http://www.tomwbell.com/NetLaw/Ch03/YahoovLICRA.html (accessed May 11, 2007).
33. http://www.cdt.org/publications/policyposts/2005/5 (accessed May 11, 2007).
34. BBC News, "The Law, borders, and the Internet," January 24, 2006, http://news.bbc.co.uk/2/hi/technology/4641244.stm (accessed May 11, 2007).
35. Center for Democracy and Technology, "Foreign courts' exercise of jurisdiction over Web content seen in other cases," July 11, 2001, http://www.cdt.org/publications/pp_7.06.shtml. For more information on this case, please refer to the Toben case in the Australia and New Zealand Regional Overview.
36. For further details, see http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf.
37. http://www.edri.org/edrigram/number2.22/filtering (accessed May 11, 2007).
38. I. Brown, "Internet censorship: Be careful what you ask for." *Proc. International Conference on Communication, Mass Media and Culture,* Istanbul, October 2006.
39. http://www.cptech.org/ecom/jurisdiction/defamation2.html (accessed May 11, 2007).
40. http://www.edri.org/edrigram/number5.3/romeII (accessed May 11, 2007).
41. Libel law in Britain—known internationally to be particularly strict—was loosened in October 2006. See Sarah Lyall, "High court in Britain loosens strict libel law," *The New York Times,* October 12, 2006, http://www.nytimes.com/2006/10/12/world/europe/12britain.html.

42. Yaman Akdeniz, "Case Analysis of Laurence Godfrey v. Demon Internet Limited," 1999, http://www.cyber-rights.org/reports/demon.htm; Consumer Project on Technology, CPT's Page on Defamation and Libel Cases, http://www.cptech.org/ecom/jurisdiction/defamation2.html.
43. http://www.nytimes.com/2006/10/12/world/europe/12britain.html.
44. http://www.lawcom.gov.uk/docs/defamation(1).pdf (accessed May 11, 2007).
45. http://www.flickr.com/photos/jesper/336756697/ (accessed May 11, 2007).
46. Article at http://www.dagbladet.no/dinside/2007/02/12/491719.html (in Norwegian), cited February 13, 2007, in http://www.opennetinitiative.net/blog/?p=144.
47. BitTorrent is "a peer-to-peer (P2P) communications protocol for file sharing," and is a "method of distributing large amounts of data widely without the original distributor incurring the entire costs of hardware, hosting and bandwidth resources." In this system, "when data is distributed using the BitTorrent protocol, recipients each supply data to newer recipients, reducing the cost and burden on any given individual source, providing redundancy against system problems, and reducing dependence upon the original distributor." A BitTorrent client is any client that implements the BitTorrent protocol, and "each client is capable of preparing, requesting, and transmitting any type of computer file over a network, using the protocol. A peer is any computer running an instance of a client. To share a file or group of files, a peer first creates a 'torrent'. This is a small file which contains metadata about the files to be shared, and about the 'tracker', the computer that coordinates the file distribution. Peers that want to download the file first obtain a torrent file for it, and connect to the specified tracker which tells them from which other peers to download the pieces of the file." See http://en.wikipedia.org/wiki/BitTorrent (accessed May 11, 2007).
48. In May 2006 the Web site administrator and systems operator of www.arenabg.com had been arrested and subsequently released on lack of grounds for arrest.
49. http://www.novinite.bg.
50. http://torrentfreak.com/government-blocks-torrent-site-citizens-protest/ (accessed May 11, 2007).
51. Ibid.
52. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/02/13/wgoogle113.xml (accessed May 11, 2007).
53. http://www.out-law.com/page-7758 (accessed May 11, 2007).
54. Introduced in Belgium in 2006, Google News shows headlines, photos, and the first few lines of news stories with links to the full versions on the Belgian newspaper Web sites.
55. http://www.edri.org/edrigram/number5.3/google-belgium (accessed May 11, 2007).
56. http://news.com.com/2100-1030_3-6174008.html (accessed May 11, 2007).
57. http://wistechnology.com/article.php?id=3548 (accessed May 11, 2007).
58. http://www.jisclegal.ac.uk/ispliability/ispliability.htm (accessed May 11, 2007).
59. http://www.europarl.europa.eu/oeil/file.jsp?id=5275032 (accessed May 11, 2007).
60. http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-63514 (accessed May 11, 2007).
61. At present, IP addresses, search queries, and cookie details are retained by Google in Europe for eighteen to twenty-four months. After this period, server logs are anonymized and it is no longer possible to identify users.
62. See http://www.edri.org/edrigram/number5.6/google-data-retention (accessed May 11, 2007).
63. http://www.edri.org/edrigram/number5.5/sweden-wiretapping (accessed May 11, 2007).

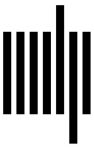
Access Denied

The Practice and Policy of Global Internet Filtering

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Denied: The Practice and Policy of Global Internet Filtering
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/7617.001.0001
ISBN (electronic): 9780262255998
Publisher: The MIT Press
Published: 2008



The MIT Press

For information about special quantity discounts, please e-mail special_sales@mitpress.mit.edu.

This book was set in Swis721 on 3B2 by Asco Typesetters, Hong Kong.
Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access denied : the practice and policy of global Internet filtering / edited by Ronald Deibert . . . [et al.].
p. cm. — (The information revolution & global politics series)
Includes bibliographical references and index.
ISBN 978-0-262-54196-1 (pbk. : alk. paper) — ISBN 978-0-262-04245-1 (hardcover : alk. paper)
1. Computers—Access control. 2. Internet—Censorship. 3. Internet—Government policy. I. Deibert, Ronald.
QA76.9.A25.A275 2008
005.8—dc22 2007010334

10 9 8 7 6 5 4 3 2 1