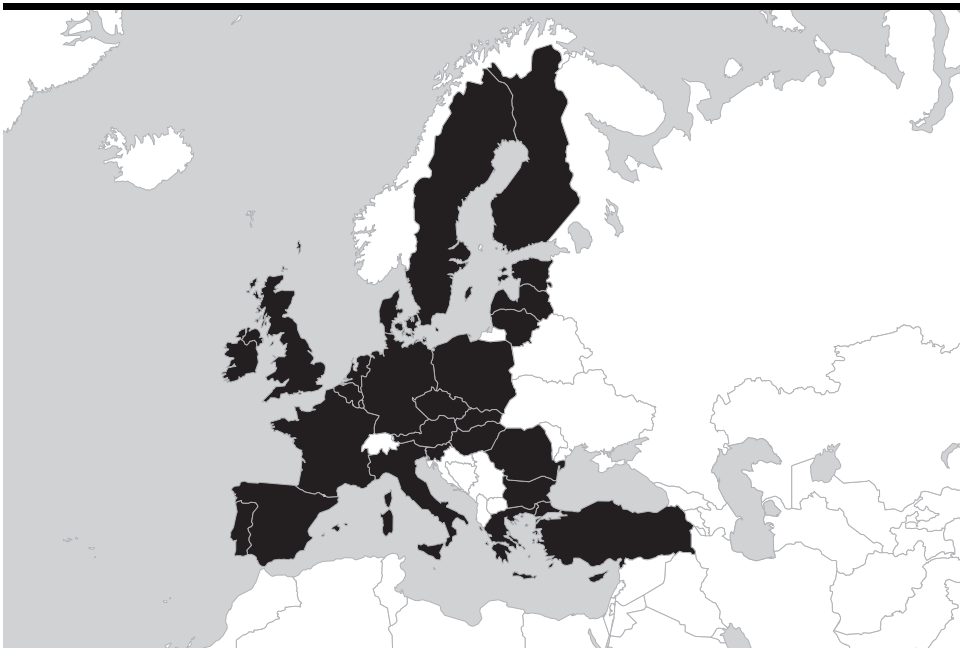
Europe

Europe Overview



The Internet in Europe is controlled predominantly through a combination of governments and information and communication technology (ICT) companies. Countries, whether members of the 27 member European Union (EU) or otherwise, have all regulated the Internet in some way, with a number of them censoring defamatory speech or monitoring copyright infringement. Meanwhile, ICT firms have taken it upon themselves to censor child pornography and hate speech.

Unlike in other parts of the world, however, the Internet in Europe is regulated to a large degree through the coordinated action of states, usually through the processes of the EU. As European governments look to harmonize their cyber-law policies over the coming years, they will increasingly turn to the EU to decide what to regulate and how to regulate the Internet.

Regional Regulation

There is no explicit obligation at the EU level mandating either governments or ICT firms to filter or remove online content, though this position may soon change. In December 2008, the EU approved the next phase of studies of new filtering technologies to fight illegal content. The Safer Internet Program adopted by the EU Council of

Ministers intends to protect minors from illegal and harmful content online, in particular, ''child sexual abuse material, grooming and cyber bullying.'' This program will operate from 2009 to 2013 and cost EUR 55 million.[1] Part of the program involves the development of tracking technologies that will monitor child pornography and help build a Europol database of illegal online behavior.[2]

This program is the latest in a series of related initiatives introduced by the EU. The first EU attempt, ''Action Plan for a Safer Internet,'' aimed at regulating content deemed illegal or harmful by individual states, was passed in 1999 and has been in force since 2002.[3] Illegal content varies between countries; Nazi propaganda, for example, is illegal in France and Germany but not in the United Kingdom. Harmful content is defined more broadly and can include anything that would offend the values and sentiments of races, religious groups, or other minorities. The action plan emphasized the need to take steps in five broad areas in order to curb illegal and harmful content on the Internet:

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. Encouraging Internet service provider(s) to provide 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 ICT firms to allow users to control access to content;
4. Exploring the legal implications of promoting the safer use of the Internet; and
5. Encouraging international cooperation in the area of regulation.

For the most part, the 2002 action plan left it to individual states to take these steps. The Safer Internet Program, passed in 2005, aims to give the EU broader powers and new tools to achieve these goals itself. Among other things, the 2005 program funded hotlines for citizens to report offending content, sponsored education efforts on consumer and data protection, and authorized new studies into filtering technology for illegal content.[4]

Two European directives may form the basis of expansive legislation regulating the Internet in the coming years. The Electronic Commerce Directive limits the liability of online providers for transferring, caching, and hosting illegal content.[5] The Audiovisual Media Services Directive (AVMSD), meanwhile, aims to extend current EU regulation for broadcast television content to the Internet.[6] The regulations include, among other things, the right of member states to sue content providers living outside their jurisdictions and the responsibility to make harmful content inaccessible to minors. Because the AVMSD was passed only in 2008, it remains unclear whether or not the directive applies to all Internet video content, or just on-demand programming sent over TCP/IP.

Most existing EU regulation regarding filtering overlaps with or supplements the existing policies of individual states. On issues of child pornography, human trafficking, terrorist propaganda, and fraud, there exists a broad consensus to monitor and block offending material. Surprisingly, no such consensus exists on who or what should be held responsible for such material. Most countries have agreed to treat ISPs as mere conduits of information. However, some countries have held these entities responsible for offending material.

The EU maintains a liberal regional policy toward ISPs, limiting their liability under the Electronic Commerce Directive,[7] however, member states have been inconsistent in applying the directive. In July 2007, a Belgian court required an ISP to implement technical measures in order to stop copyright infringements committed by its subscribers through P2P networks.[8] In 2008, the British government warned that, absent ISPs' ''voluntary self-regulation,'' it would hold service providers legally responsible for allowing unlawful file sharing.[9] British ISPs have, by all appearances, already chosen to self-regulate.[10]

Despite the lack of strong EU-level regulation, many member states have taken it upon themselves to filter unwanted content. Many countries, such as the United Kingdom,[11] Sweden,[12] Finland,[13] Denmark,[14] Germany,[15] and Italy,[16] filter child pornography, and some governments (e.g., United Kingdom, France) have pressured ISPs to prevent copyright infringements by filtering.[17] Quite recently, it was reported that a number of Web sites in Belgium were blocked. In contrast to other countries, the Web sites were filtered not because of displaying pornographic content but in order to guarantee the privacy rights of suspects or criminals who committed sexual offenses against children and whose identity was accordingly revealed in the targeted Web sites.[18]

In addition to filtering directed by governments, ISPs and search engines within countries have often taken it upon themselves to monitor and filter controversial content. Often, these companies have decided to self-regulate in order to preempt government regulation.

Copyright

Film studios, record labels, and their associations have all strongly lobbied the EU to require ISPs to block potential copyright infringements and terminate the contracts of subscribers who visit particular Web sites. Yet the EU has been slow to act, authorizing studies but rarely taking action. Generally, however, where the EU has failed to assist the content industries, individual states have been quick to act, enthusiastically prosecuting companies and individuals who violate copyright law, both within and outside their borders.

The EU's policy on intellectual property and illegal file sharing is laid out in three directives. The Electronic Commerce Directive standardizes information and

transparency requirements for ISPs, commercial communications, and electronic contracts.[19] The 2001 Directive on Copyright and Related Rights gives authors, performers, and film producers the sole right to reproduce and distribute their respective writings, performances, sound recordings, and films.[20] And the 2004 Directive on the Enforcement of Intellectual Property Rights aims to harmonize intellectual property protection regimes across the EU and allows member states' judges to issue injunctions against ongoing or impending intellectual property violations.[21] None of these directives have mandated the use of filtering technologies to protect intellectual property regimes. However, where the EU has been slow to respond to the demands of the film and music industry, individual countries have been more proactive. In 2007, a Danish court ordered the country's largest ISP to block Allofmp3.com, a Web site offering illegal music downloads.[22] In March 2007, Bulgarian police arrested the owner of Arenabg.com, one of Bulgaria's largest BitTorrent trackers, and blocked the Web site for four days.[23] Most seriously, in June 2008, France established the High Authority for Copyright Protection and Dissemination of Works on the Internet to monitor Internet content for illegal file sharing and eventually suspend the Internet connections of repeat file sharers.[24]

European courts have been skeptical of claims to fair use of copyrighted content. In February 2007, a court in Brussels found that Google, Inc., had violated the copyrights of Copiepresse, a Belgian newspaper consortium. The court ruled that by taking headlines and short news extracts from Copiepresse's newspapers, Google's news feature illegally allowed Internet users to read articles without paying proper subscription fees and without viewing the advertisements on Copiepresse's sites. The court fined Google GBP 2.4 million and prohibited it from sampling Copiepresse members' articles, pictures, or drawings.[25] The court also required that Google remove, within 24 hours, any future content that copyright holders said infringed on its rights, or pay a fine of EUR 1,000 per day.[26] Google had similar fair use problems in France when Agence France-Presse (AFP) sued the company for USD 17.5 million in 2005. The suit was dropped in April 2007, following a licensing agreement under which Google could use stories and photographs from AFP for its news aggregator and for other Google services. The financial terms of this arrangement have not been publicly disclosed.[27] Overall, where the EU has hesitated to take aggressive action on intellectual property regime enforcement, individual states have been eager to step in, enforcing the laws of their individual regimes on companies both inside and outside their borders.

A controversial Internet piracy bill was adopted by the French Parliament in March 2009. According to the so-called three-strikes bill, the French government will launch a new agency, HADOPI (High Authority for the Diffusion of Works and the Protection of Rights on the Internet), that would assess whether a suspect is guilty of having violated copyright provisions when downloading material online. If it is determined that the user violated a copyright provision, he or she would receive a warning, followed by a suspension of Internet access for a maximum of 12 months if he or she did

not comply. Critics of the bill stress that cutting Internet access would require a court order, which is not guaranteed by the law at this stage.

Social Filtering

On issues of child pornography, European nations have worked well together to block offending content, often recruiting private companies to help them in their cause. However, on other social issues, such as gambling, states have been less effective in controlling content, either individually or in coordination with each other.

The landmark model of large-scale voluntary ISP filtering in Europe originated in the United Kingdom. Britain's largest ISP, BT, launched Project Cleanfeed in June 2004,[28] in consultation with the British Home Office. Under the auspices of this program, BT blocks Web sites that the nonprofit Internet Watch Foundation (IWF) declares as hosting images of child abuse. When individuals attempt to access Web sites on IWF's list, they receive an error message.[29] If the Web sites are hosted within the United Kingdom, the ISP is required to take down the offending material. Cleanfeed's success has inspired imitators: in 2008, the ISP Brightview began offering a filtering device, WebMinder, free to other service providers. Today, some 90 percent of broadband subscribers in the United Kingdom have filtering programs of one form or another.[30]

Other countries, such as Norway, Sweden, Denmark, and Italy, have implemented similar programs, though not without controversy.[31] Finland's pilot program received negative attention early on when the Finnish National Bureau of Investigation, which prepares the list of Web sites to be filtered, included lapisporno.info—a Web site discussing the issue of Internet censorship—on the list. A 2005 effort by German search engines to delist harmful content providers came under criticism when the search engines refused to say which Web sites were being removed.[32]

In December 2008, the Romanian Regulatory Authority for Communications and Information Technology on the basis of Law No. 196/2003 ordered ISPs to block access to 40 Web sites containing illegal material. If an ISP does not execute such a blocking order within 48 hours, it may be fined between ROL 100,000 and ROL 500,000,000 (from USD 41,400 to USD 207 million).[33] The block list[34] contained mainly pornographic Web sites, although reportedly a well-known user-generated video-sharing site was also included.[35] The Romanian Regulatory Authority can compel ISPs to block access to any Web site that does not comply with the provisions of the law stating that pornographic Web sites have to be officially authorized, password protected, and charged for at a per-minute rate (determined by the site's operator).[36] The authority is not required by the legislation to give an appropriate waiting period to Web site owners to comply with these legal requirements; instead, it can immediately order ISPs to block access.

Despite criticism, individual countries' efforts at stopping child pornography have met with remarkable success. In 2006, the U.K. Child Exploitation and Online

Protection Center made 13 arrests in a pay-per-view pornography program.[37] In February 2007, Austrian authorities were able to uncover a child-pornography ring involving more than 2,300 people in 77 countries.[38]

As individual countries have moved to filter pornographic content online, they have done so with increasing coordination. Citizens in 19 countries assist in identifying and reporting illegal content—particularly in the area of child pornography—through a network of hotlines established by the EU.[39] Recent reports show that the Save the Children Denmark hotline, financed in part by the European Commission's Safer Internet Plus Program, had nearly 9,000 reports of child abuse images in 2006 alone. In 2004, Spanish police arrested 90 people in the country's largest operation against the distribution of child pornography, also facilitated by the hotlines. At the same time, new regulations at the regional level could force countries to impose stricter filtering regimes within their own countries. The new AVMSD requires member states to take measures to ensure that on-demand audiovisual services that might seriously impair the ''physical, mental or moral development of minors'' are made inaccessible to minors.[40]

While Europe has been very successful in mobilizing filtering technologies against child pornography, it has been less successful at coordinating efforts against gambling. In 2006, Italy enacted a law that requires ISPs to block the Web sites of gambling operators not licensed nationally. In 2007, however, the European Court of Justice ruled Italy's law in violation of EU standards.[41] In 2002, Swiss politicians attempted a similar block on online gambling. The effort was suspended in 2004, and no further action has been taken since. A 2007 proposal in Norway blocked access to foreign gambling Web sites; Web sites that ''desecrate the Flag or Coat of Arms of a foreign nation''; Web sites that promote hatred toward public authorities, contain hate speech, or promote racism; offensive pornography sites; and P2P networks that offer illegal downloads of music, movies, or television shows.[42] To date, no action has been taken on the bill.[43]

Individual countries have been very proactive in instituting filtering and monitoring programs to control child pornography. This enthusiasm has extended to EU-wide regulation. However, no such enthusiasm exists for controlling gambling. Filtering, where it has been instituted, has been done at the country, not the regional, level.

Nationalistic Filtering

European governments have not censored direct political opposition. However, they have on occasion censored content that had the potential to ''threaten 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[44] and to modify their DNS servers to block the domain www .appel-au-peuple.org.[45] 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.[46] Nevertheless, the order was enforced, and directors of noncompliant ISPs were asked to appear personally in court, or they would risk facing charges.

On March 7, 2007, Turkey forced ISPs to block YouTube after several videos were posted denigrating Turkey's founding father, Mustafa Kemal Atatürk, and the Turkish flag. In blocking the Web site, Turkish officials invoked Article 301 of the Turkish Penal Code, which criminalizes insults toward Atatürk as well as ''Turkishness.'' Turkey's leading ISP, TurkTelecom, complied with the order but petitioned the court to allow access to the Web site to be restored. The court agreed on the condition that the particular videos be 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.''[47] Yet YouTube and similar Web sites were again blocked in March 2008 for hosting content insulting to Atatürk.[48]

Hate Speech

Within Europe there is a general consensus in favor of censoring anti-Semitic or Holocaust-denying speech online. Where individual states have more expansive anti-hate regimes, they have enforced those laws, with some success, at the national level. In 2000, a French court ruled that U.S.-based Yahoo! Inc. was liable under French law for allowing the people of France access to auction Web sites that included Nazi memorabilia and demanded that Yahoo block this content in France or face fines.[49] Yahoo brought a 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,[50] but in 2004 the Ninth U.S. Circuit Court of Appeals overturned that ruling on the grounds that it did not have sufficient jurisdiction over the French parties.[51] After rehearing the case *en banc*, the appeals court dismissed Yahoo's case in January 2006.[52] Though split, the court reasoned that the fact that Yahoo had complied voluntarily and removed the offending content precluded claims as to a possible violation of the right to freedom of expression.[53]

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.[54] In 2002, the Bezirksregierung Düsseldorf (district government) obliged 56 ISPs to restrict access to four foreign Web sites.[55] The attempts to block access have attracted nationwide attention and met fierce opposition from users and service providers.[56] However, neither political demonstrations nor lawsuits have been successful in stopping the blockade. By the end of 2005, 76 Internet service providers had been required to block the named Web sites.[57]

Germany has engaged in other efforts to combat hate speech. According to one study published by the Berkman Center for Internet and Society in 2002, about 91 Web

sites were completely or partly excluded by the German sections of the search engine Google.[58] In 2008, about 23 suspects were apprehended by German police in eight German states, and a further 70 suspects had been identified in the investigation because of their illegal sale of right-wing extremist material over the Internet.[59]

Holocaust denial is also legislated at the country level. Fifteen European countries also have laws against Holocaust denial,[60] and others 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.[61] As with all illegal content, once it is brought to their attention, ISPs must either take down or block the relevant Web sites (depending on whether they are hosted domestically or abroad).

One issue Europe has yet to resolve with regard to hate speech is whether merely linking to offending content constitutes a crime. A 2000 case, in which French citizens were barred from shopping on Web sites selling Nazi memorabilia,[62] would suggest that Europeans would think it is. Yet, in 2004, the political activist Alvar Freude was accused of linking to right-wing extremist Web sites and was brought to court. A local court found this to be a criminal offense. However, the Stuttgart higher regional court overturned that decision in 2006 and absolved Freude.[63]

Defamation

Two forces are intersecting to shape defamation law in Europe. On the one hand, states are relying on the ''effects test'' to determine legal jurisdiction; that is, so long as harm is done within the country's borders, the injured party can sue within that country. On the other hand, individual countries are also exercising comparatively harsh antidefamation laws. Together, these forces mean that more people are being sued outside their home countries, and for more money, than ever before.

Member states of the EU have sought a simplified electronic defamation framework. The traditional principle in cases of defamation concerning the media—that the law of the country where the defamed person lives is applicable—creates a strong incentive for media to gain a potentially impractical degree of knowledge about the privacy and defamation laws of each European country. In Italy, for example, a man in a cross-border custodial battle claimed that his ex-wife, now a resident of Israel, was responsible for posting statements and images on the Internet that were defamatory of him and his ability to care for their two daughters. Italy's highest appellate court, the

Suprema Corte di Cassazione, overturned a prior verdict and held that Italy's laws of libel applied to content on foreign Web sites accessible by Internet users in the country.[64] Italian doctrine thus supports an effects test for choice of law, similar to that used in the United States for personal jurisdiction: if the offending statements, wherever posted, created an effect within the country, they are subject to the Italian law. Other countries are reaching similar conclusions. The German Federal Court of Justice decided in 2000 that the Australian owner of an Australian Web site which denied the Holocaust could be held liable in Germany.[65]

Simultaneously, anti-defamation laws at the domestic level, particularly in Britain, have been criticized for leading to a ''Web takedown'' culture in which ISPs immediately remove content alleged to be defamatory for fear of lawsuits. A landmark precedent in the United Kingdom led the way for the establishment of a ''notice and takedown'' system. In *Laurence Godfrey v. Demon Internet Limited*,[66] a defamatory statement was made on a posting to a newsgroup, www.soc.culture.thai, available on a server of Demon Internet Limited. Despite Godfrey's request to remove the post, Demon did not comply. As a result, he claimed damages for libel under section 1 of the Defamation Act of 1996[67] and settled with Demon out of court for over GBP 250,000.[68]

On rare occasions, some countries have attempted to achieve tight Internet regulation by subjecting Web sites to mandatory registration under general media laws or Internet-specific regulations. Such registration directly submits Web site owners and users to civil and/or criminal law liability for content published online, which may arise under provisions sanctioning defamation, dissemination of illegal content, and pornography (among others). In some cases such publication may require preapproval by a state agency. Poland, for instance, shows lack of clarity with regard to the status of online media. A television broadcast segment that criticized the work of a Polish debt collector prompted a series of threatening comments on a forum on the GazetaBytowska.pl (Bytów Newspaper) Web site. Polish police asked the Web site's administrator to give them identifying information for the commentators in question, but he refused. The police then charged the Web site under article 45 of the Press Law Act (PLA) of 1984.[69] A local court determined the Web site to be a daily publication and therefore subject to the PLA, which provides for punishment for editors who publish—even unintentionally—''criminal content,'' including threats like the ones made in the online forum. The case was appealed to the Regional Court, which ruled in February 2008 that Web sites such as GazetaBytowska.pl must be registered.[70] A ruling of the Polish Supreme Court a year earlier stated that ''journals and periodicals do not lose the character of a press release due solely to the fact that they appear in the form of an Internet transmission'' and that ''the publishing of press in an electronic form, available on the Internet, requires registration.'' Subsequently, a Supreme Court spokesman emphasized that the ruling was not intended to suggest that all regularly updated Web sites needed to be registered.[71]

Together, these two trends—the increasing use of the effects test and increasingly harsh damages for defamation—have given an incentive for European countries to coordinate anti-defamation laws at the European level.

A 2007 amendment to the Rome II convention attempted to set regional standards for the application of anti-defamation laws. The amendment instructed European courts to obey, with some exceptions, the anti-defamation laws of the country in which the damage occurred.[72]

Surveillance

European countries have worked to coordinate security directives at the regional level, yet these consensus directives have been criticized by outside groups as far too extreme. The 2006 European Data Retention Directive[73] prescribes surveillance on a regional level in the public interest. Because the directive has been transposed into the national legislation of most of the EU member states, ISPs at the local level are required to retain specific data pertaining to electronic communications to assist in tracking down crimes and for future prosecutions. Such data can be collected through users' activities, in particular Internet access, e-mail, and telephony, and can be retained for a minimum period of six months but not exceeding two years.[74] The aim is to bring about a common code of data retention in order to trace illegal content and the source of attacks against information systems, and to identify those who use electronic communications networks for terrorist activities and organized crime. The data to be retained do not concern the content of communications. Yet the directive has inspired controversy within member states and was challenged recently at the German Constitutional Court.[75]

Yet some countries are far exceeding the scope of surveillance allowed by the EU. In March 2007, the Swedish government granted its national defense intelligence agency the power to monitor all cross-border telephone calls and e-mail traffic, even without a warrant. Various critics have raised privacy concerns about the plan, positing that the proposal violates privacy rights and breaches EU law. Notwithstanding the criticism, in January 2009 amendments to the Swedish wiretapping law entered into force, allowing the National Defense Radio Establishment sweeping surveillance powers over online activities. The new law allows special state agencies to monitor telephone calls and Internet traffic, including the content of the traffic itself, which is outside of the scope of the EU Data Retention Directive. In addition, the state agency could develop a plan to search for sensitive keywords in transmitted messages and could even require monitoring content on servers outside the country's borders.[76] A nongovernmental organization has already brought a case against the new law in the European Court of Human Rights.[77] Sweden's own national security police agency called the plan a violation of ''personal integrity.'' Such pervasive policies against online activities have triggered disapproval among big international ICT companies, some of which announced that they

would cease making significant investments in the country if the controversial law was not revisited.[78]

A different development of events occurred in Finland, where employers organizations (reportedly including handset giant Nokia)[79] lobbied strongly for introducing legislation that would allow employers to track employees' e-mails to prevent corporate espionage. In March 2009, the Finnish government adopted such a law granting employers access to information about their workers' messages, including the recipients, senders, and the time when e-mails were sent or received, and whether the e-mails contained attachments. The law does not allow the employers to read the content of the messages outright. Nonetheless, employers' otherwise broad rights over employees' electronic communications raise serious privacy concerns.

Germany, too, is taking active steps toward increasing government surveillance online. A new amendment to the national telecommunication law requires that ISPs retain personal data, such as e-mail senders' IP addresses, recipients' IP addresses, date and time of all messages, IP address for each Internet subscriber, and a unique identifier for each client to track online activity.

Germany's federal crime police, the Bundeskriminalamt, have not only monitored e-mails and chat rooms, but also begun performing so-called online raids.[80] The idea is to infect a suspect's personal computer with Trojan horse software to secretly record data entered into the computer. However, this technique remains highly controversial. The federal constitutional court ruled in March 2008 that online raids could only be used in exceptional circumstances.[81]

In 2005, the Italian government authorized increased surveillance of the Internet and telephone networks.[82] The bill requires Internet cafés to keep photocopies of customers' passports and to periodically submit logs of all Web sites visited to the police.[83] The law also increases licensing requirements for telecommunication service operators, making licensing approval dependent upon the existence of satisfactory data-monitoring and retention systems.[84]

In France, two laws have granted increased surveillance powers to the government. The Daily Safety Law (LSQ) was approved almost unanimously by parliament on November 15, 2001, and the Internet Safety Law (LSI) was enacted on February 13, 2003. Together, these laws require that ISPs keep a record of their customers' Internet activity and e-mail traffic for a year and that encryption firms assist authorities in decoding messages involved in criminal trials. Additionally, in June 2008 the French government established the High Authority for Copyright Protection and Dissemination of Works on the Internet, which will monitor all network traffic for possible copyright infringement.

Similar surveillance policies were introduced in Poland, with a February 2003 amendment to the Telecommunications Law. The law requires telecommunication companies to provide the police and other state agencies with access to information sent through telecommunications networks for the purpose of national defense, state

security, and public order.[85] The data that may be requested by the police include caller identification, network terminals and/or telecommunication devices used in the connection, data generated during the connection, the circumstances, and the type of connection.[86]

The Polish government has been criticized for conducting a large number of wiretapping operations that may be seen as an invasion of privacy. In early March 2009, the office of the Polish prime minister announced that it had plans to compile a ''super database'' of information on all Polish citizens. The database would be compiled during the 2011 census and would include information from the ministries of finance, justice, and home affairs, social insurance information, and information gathered from telecommunications suppliers. The plan has met with outrage from Polish Internet users, who claim the database would violate their constitutional rights. The prime minister's office has since released a statement explaining that the database will only include necessary information.[87] It remains to be seen who would then determine what information is necessary and how Internet users' right to privacy would be guaranteed.

The prospect of revenue from online advertising has sometimes driven operators to exercise surveillance over their customers' preferences. Major British operators BT, Talk Talk, and Virgin have all signed up to use Phorm,[88] a Web tracking service, which uses information gathered from a user's browsing history to deliver targeted advertising on members' Web sites. An admission has been made by BT that it ran secret trials of a new advertising platform among 18,000 of its broadband customers in 2006 in order to determine the operational and technical performance of the service. The platform targets advertisements at the operator's customers using their browsing profiles. The EU threatened in April 2009 to pursue legal action against the United Kingdom for breaching Internet privacy laws by allowing operators to use the platform to track their customers' online activities for commercial gain (estimated at GBP 3 billion a year).

Conclusion

Today, Internet content in Europe is controlled by three groups of factors: region-wide organizations (the EU), individual countries, and companies (e.g., ISPs, search engines). While governments have been extremely active in promoting filtering technologies for child pornography and surveillance technologies for copyright infringement, they are increasingly finding that they can achieve their aims through indirect means. Rather than passing explicit regulations, governments have pressured companies to voluntarily self-regulate content, be it pornography, hate speech, or content that infringes upon copyrights. Such pressures show a creeping tendency toward the second- and third-generation controls found elsewhere.

At the EU level, countries are increasingly working to harmonize Internet regulation, especially with regard to defamatory and pornographic content. Given the significant

cultural differences between countries and existing regulatory frameworks, creating a common platform for legislation at the regional level is a slow and complex process. Nonetheless, it is increasingly the arena where decisions about Internet filtering and monitoring are made.

Notes

1. European Commission, ''Safer Internet Programme 2009–2013.'' http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm.

2. Web Designers Blog, ''EU Share 55 Million to Create Surveillance Technology on the Internet,'' November 1, 2008, http://web.pdesigner.net/2008/11/01/eu-share-55-million-to-create-surveillance-technology-on-the-internet/.

3. European Commission, ''Action Plan for a Safer Internet 1999–2004,'' January 19, 2007, http://europa.eu/legislation_summaries/information_society/l24190_en.htm.

4. European Commission, ''Safer Internet Programme 2005–2008 (Safer Internet Plus),'' January 19, 2007, http://europa.eu/legislation_summaries/information_society/l24190b_en.htm.

5. European Commission, Directive 2000/31/EC of the European Parliament, August 17, 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.

6. European Commission, ''Audiovisual Media Services Directive (AVMSD),'' 2007, http://ec.europa.eu/avpolicy/reg/avms/index_en.htm.

7. European Commission, ''E-Commerce Directive,'' May 22, 2000, http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

8. Brussels Court of First Instance (TGI), *SABAM v. s.a. Scarlet (anciennement Tiscali)*, 04/8975/A, June 29, 2007, http://www.juriscom.net/documents/tpibruxelles20070629.pdf.

9. Francis Eliot, ''Internet Users Could Be Banned over Illegal Downloads,'' *Times Online*, February 12, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article3353387.ece.

10. *Cable Forum*, ''Virgin Media First UK ISP to Adopt 3-Strikes-and-Out on Illegal Downloads,'' March 31, 2008, http://www.cableforum.co.uk/article/394/virgin-media-first-uk-isp-to-adopt-3-strikes-and-out-on-illegal-downloads.

11. Wendy M. Grossman, ''IWF Reforms Could Pave Way for UK Net Censorship,'' *The Register*, December 29, 2006, http://www.theregister.co.uk/2006/12/29/iwf_feature/.

12. *Telenor*, ''Telenor and Swedish National Criminal Investigation Department to Introduce Internet Child Porn Filter,'' May 17, 2005, http://press.telenor.com/PR/200505/994781_5.html.

13. *Helsingin Sanomat*, ''Anti-Internet Censorship Website Placed on Police Filter List over Links to Child Porn Sites,'' February 14, 2008, http://www.hs.fi/english/article/AntiInternet+censorship+website+placed+on+police+filter+list+over+links+to+child+porn+sites/1135234057449.

14. Kristian Hansen, ''Danish Filter Catches Romanian Child-Porn Sites,'' *Computerworld*, June 11, 2008, http://www.computerworld.com/s/article/9097018/Danish_filter_catches_Romanian_child_porn_sites.

15. Lars Vage, ''German Search Services Collaborate to Exclude Child Pornography, Right Wing Extremism, and Glorification of Violence,'' *Pandia*, March 8, 2005, http://www.pandia.com/sw-2005/10-germany.html.

16. Loverock Davidson, ''Italy Adopts Microsoft Anti-Child-Porn Technology,'' *ZDNet*, October 17, 2006, http://talkback.zdnet.com/5208-9588-0.html?forumID=1&threadID=26363&messageID=494518&start=0.

17. Kate Holton, ''UK Could Follow France on Internet Piracy Plan,'' Reuters, February 12, 2008, http://www.reuters.com/article/rbssTechMediaTelecomNews/idUSL1282127820080212.

18. Bart B. Van Bockstaele, ''Belgian Government Trying to Censor the Internet,'' *Digital Journal*, April 22, 2009, http://www.digitaljournal.com/article/271340#tab=featured&sc=0&contribute=&local=.

19. European Commission, ''E-Commerce Directive,'' 2000, http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

20. European Commission, ''Copyright and Related Rights in the Information Society: Harmonisation of Certain Aspects,'' January 14, 2008, http://europa.eu/legislation_summaries/internal_market/businesses/intellectual_property/l26053_en.htm.

21. European Commission, ''Enforcement of Intellectual Property Rights,'' December 13, 2007, http://europa.eu/legislation_summaries/fight_against_fraud/fight_against_counterfeiting/l26057a_en.htm.

22. City Court of Copenhagen, *IFPI Denmark v. Tele2*, October 25, 2006, Case F1–15124/2006; P2P.net, ''IFP vs Tele 2—in English,'' http://www.p2pnet.net/story/10319.

23. European Digital Rights, ''Bulgarian Police Ordered ISPs to Block US-Based Torrent Tracker,'' April 12, 2007, http://www.edri.org/edrigram/number5.7/bulgarian-block-isp.

24. *Kaldata*, ''French Bill Would Ban Internet Use for Illegal Downloaders,'' June 20, 2008, http://www.kaldata.net/comments.php?catid=3&id=20895.

25. Bruno Waterfield, ''Google to Pay £2.4m over 'Copyright Breach,''' *Daily Telegraph*, February 14, 2007, http://www.telegraph.co.uk/news/worldnews/1542549/Google-to-pay-andpound2.4m-over-%27copyright-breach%27.html.

26. European Digital Rights, ''Belgium Court Backs Decision against Google,'' February 14, 2007, http://www.edri.org/edrigram/number5.3/google-belgium.

27. Caroline McCarthy, ''Agence France-Presse, Google Settle Copyright Dispute,'' *CNet*, April 6, 2007, http://news.com.com/2100-1030_3-6174008.html.

28. *BBC News*, ''BT Acts against Child Porn Sites,'' June 8, 2004, http://news.bbc.co.uk/2/hi/technology/3786527.stm.

29. 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 Michael McDonough, ''35,000 Blocks a Day on Internet Child Porn,'' *Guardian*, February 7, 2006, http://technology.guardian.co.uk/news/story/0,,1704342,00.html.

30. 446 Parl. Deb., H.C. (6th ser.) (2006) 709W.

31. See *Telenor*, ''Telenor and Swedish National Criminal Investigation Department to Introduce Internet Child Porn Filter,'' May 17, 2005, http://press.telenor.com/PR/200505/994781_5.html; *Financial Mirror*, ''Filter Blocks Danes from Accessing Child Pornography,'' November 28, 2005, http://www.financialmirror.com/more_news.php?id=2574; European Digital Rights, ''New Italian Law to Block Child Pornography Websites,'' January 17, 2007, http://www.edri.org/edrigram/number5.1/italy_blocking.

32. *Heise Online*, ''Search Engine Providers Practice Self-Regulation,'' February 25, 2005, http://www.heise.de/english/newsticker/news/56817.

33. ''Law on the Prevention and Fighting of Pornography,'' No 196/2003 [Unofficial translation from Romanian], http://www.legi-internet.ro/index.php?id=89&L=2.

34. *Nicu*, ''Romanian Censored Sites,'' December 16, 2008, http://nicubunu.blogspot.com/2008/12/romanian-censored-sites-warning-about.html.

35. European Digital Rights, ''Romanian Authority Asks ISPs to Block 40 Pornographic Websites,'' http://www.edri.org/edri-gram/number6.24/anc-blocks-isp-pornography-romania.

36. ANCOM, ''ANC cere Blocarea Accesului la 40 de Site-uri cu Caracter Pornografic'' [ANC Calls for Blocking Access to 40 Pornographic Sites], December 11, 2008, http://www.anrcti.ro/DesktopDefault.aspx?tabid=3483.

37. *BBC News*, ''13 Arrests over Child Sex Images,'' July 25, 2006, http://news.bbc.co.uk/1/hi/uk/5213058.stm.

38. *BBC News*, ''Vienna Busts Huge Child Porn Ring,'' February 7, 2007, http://news.bbc.co.uk/2/hi/europe/6338125.stm.

39. For the list of countries running hotlines and the organizations involved, see European Commission, ''Hotlines,'' May 5, 2008, http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2007-HC-121701.

40. European Parliament, ''Coordination of Certain of the Member States' Provisions Concerning the Pursuit of Television Broadcasting Activities,'' December 19, 2007, http://www.europarl.europa.eu/oeil/file.jsp?id=5301252.

41. Eric Pfanner, ''Ruling Could Open EU Gambling Market,'' *New York Times*, March 6, 2007, http://www.nytimes.com/2007/03/06/technology/06iht-gamble.4817616.html?_r=1.

42. Gunnar Hellieson, ''The Great Firewall of Norway,'' *Luni.net*, February 13, 2007, http://luni.net/?p=77.

43. *Libertus.net*, ''ISP 'Voluntary'/Mandatory Filtering,'' February 28, 2008, http://libertus.net/censor/ispfiltering-gl.html#norway.

44. The contested Web sites were http://www.appel-au-peuple.org; http://de.geocities.com/justicecontrol; and http://www.swiss-corruption.com.

45. FITUG e.V., ''EDRI-gram,'' February 12, 2003, http://www.fitug.de/news/newsticker/newsticker120203210053.html.

46. Article 16, sec. 3; unofficial English translation available at http://www.admin.ch/org/polit/00083/index.html?lang=en.

47. European Digital Rights, ''YouTube Blocked for 2 Days in Turkey,'' March 14, 2007, http://www.edri.org/edrigram/number5.5/youtube-turkey.

48. Eric Auchard, ''Turkey Blocks Web Site over Insults to Atatürk,'' Reuters, March 25, 2008, http://www.reuters.com/article/internetNews/idUSN2434354220080325.

49. Center for Democracy and Technology, ''Appeals Court Agrees to Reconsider Ruling about French Censorship of U.S. Speech,'' February 15, 2007, http://www.cdt.org/publications/policyposts/2005/5.

50. *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 169 F.Supp.2d 1181 (N.D. Cal. 2001), *rev'd*, 433 F.3d 1199 (9th Cir. 2006), *cert. denied*, 126 S.Ct. 2332 (2006).

51. *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 379 F.3d 1120 (9th Cir. 2004).

52. *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 433 F.3d 1199 (9th Cir. 2006) (en banc), *cert. denied*, 126 S.Ct. 2332 (2006).

53. *BBC News*, ''The Law, Borders, and the Internet,'' January 24, 2006, http://news.bbc.co.uk/2/hi/technology/4641244.stm.

54. 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.

55. *Heise Online*, ''Nordrhein-Westfälische Provider Sollen Nazi-Web sites Ausfiltern'' [North Rhine-Westphalia Providers Should Filter Nazi Web sites], December 8, 2001, http://www.heise.de/newsticker/Nordrhein-westfaelische-Provider-sollen-Nazi-Websites-ausfiltern–/meldung/21627.

56. *Online-Demonstrations-Plattform für Menschen*, ''Declaration for Freedom of Information in the Internet,'' http://odem.org/informationsfreiheit/en/.

57. *Heise Online*, ''Düsseldorfer Bezirksregierung Sieht Sich Erfolgreich im Kampf Gegen Nazi-Websites'' [Düsseldorf District Government Sees Itself Successful in the Fight against Nazi Web sites], November 22, 2005, http://www.heise.de/newsticker/Duesseldorfer-Bezirksregierung-sieht-sich-erfolgreich-im-Kampf-gegen-Nazi-Websites–/meldung/66501/.

58. Germar Rudolf, ''Censorship of the Internet,'' 2003, http://www.germarrudolf.com/civil/internet.html.

59. *Lancaster Unity*, ''German Police Raid Homes in Far-Right Internet Probe,'' February 28, 2008, http://lancasteruaf.blogspot.com/2008/02/german-police-raid-homes-in-far-right.html.

60. Wikipedia, ''Laws against Holocaust Denial,'' http://en.wikipedia.org/wiki/Laws_against_Holocaust_denial.

61. Ian Brown, ''Internet Censorship: Be Careful What You Ask For,'' Proceedings of the International Conference on Communication, Mass Media and Culture, Istanbul, October 2006.

62. *CNN.com*, ''Yahoo! Loses Nazi Auction Case,'' November 20, 2000, http://archives.cnn.com/2000/TECH/computing/11/20/france.yahoo.02/.

63. *Heise Online*, ''Revisionsverhandlung Gegen Netzaktivisten Steht An'' [Revision Negotiation against Net Activists Lines Up], April 19, 2004, http://www.heise.de/newsticker/Revisionsverhandlung-gegen-Netzaktivisten-steht-an–/meldung/72134.

64. Consumer Project on Technology, ''CPT's Page on Defamation and Libel Cases,'' http://www.cptech.org/ecom/jurisdiction/defamation2.html.

65. Florian Rötzer, ''Update: Leugnung des Holocaust im Internet Nach Deutschem Recht Strafbar,'' *Telepolis*, December, 13, 2000, http://www.heise.de/tp/r4/artikel/4/4467/1.html.

66. [1999] 4 All ER 342, [2001] QB 201 (QBD).

67. 1996, c. 36, sec. 1 (Eng.).

68. 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.

69. The text of the law states, ''Anybody who publishes a daily newspaper or a periodical without registration or with registration suspended is subject to a fine penalty or the restriction of liberty.'' Article 45, Polish Press Law Act of January 26, 1984.

70. Tomasz Rychlicki and Piotr Waglowski, ''Polish Courts Say Websites Should Be Registered As Press,'' *Computer and Telecommunications Law Review*, 2009, 15(1), 9–14, http://prawo.vagla.pl/node/8306.

71. Joanna Kulesza, ''Which Legal Standards Should Apply to Web-logs? The present legal position of Internet journals in the European jurisprudence in the light of the European Parliament Committee's on Culture and Education report and Polish Supreme Court decision,'' *Lex Electronica*, Vol. 13, no. 3 (Winter 2009), http://www.lex-electronica.org/fr/resumes_complets/221.html.

72. European Digital Rights, ''MEPs Support Again the Rules on Defamation in Rome II,'' February, 14, 2007, http://www.edri.org/edrigram/number5.3/romeII.

73. Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

74. European Parliament, ''Electronic Communications: Personal Data Protection Rules and Availability of Traffic Data for Anti-terrorism Purposes,'' March 15, 2006, http://www.europarl.europa.eu/oeil/file.jsp?id=5275032.

75. *Heise Online*, ''Data Retention: ISPs Rely on Constitutional Appeals and Exception Rules,'' January 10, 2008, http://www.heise.de/english/newsticker/news/101624/.

76. European Digital Rights, ''Cross-Border Wiretapping Proposed by the Swedish Government,'' March 14, 2007, http://www.edri.org/edrigram/number5.5/sweden-wiretapping.

77. David Landes, ''Norwegian Group Joins Case against Sweden's Wiretapping Law,'' *The Local*, February 13, 2009, http://www.thelocal.se/17578/20090213/.

78. Paul O'Mahoney, ''Google Likens Sweden to Dictatorship,'' *The Local*, May 30, 2007, http://www.thelocal.se/7452/20070530/.

79. Matti Huuhtanen, ''Finnish Parliament Approves e-Mail Tracking Law,'' *The Age*, March 5, 2009, http://news.theage.com.au/breaking-news-technology/finnish-parliament-approves-email-tracking-law-20090305-8ona.html.

80. Wikipedia, ''Online-Durchsuchung,'' http://de.wikipedia.org/wiki/Online-Durchsuchung#Deutschland.

81. *BBC News*, ''The Most Spied Upon People in Europe,'' February 28, 2008, http://news.bbc.co.uk/2/hi/europe/7265212.stm.

82. *Palomar*, ''Decision of the Italian Constitutional Court on the Legitimacy of Immediate Deportation of Aliens for National Security Reasons (Constitutional Court Decision n. 432/2007),'' April 2008, http://www.unisi.it/dipec/palomar/italy001_2008.html#6.

83. Sofia Celeste, ''Want to Check Your e-Mail in Italy? Bring Your Passport,'' *Christian Science Monitor*, October 4, 2005, http://www.csmonitor.com/2005/1004/p07s01-woeu.html.

84. Legislation Online, ''Italy Adopts New Anti-Terrorism Legislation—2005-08-16,'' August 16, 2005, http://www.legislationline.org/documents/id/3138.

85. European Digital Rights, ''Polish Providers Fight Email Monitoring Obligation,'' March 27, 2003, http://www.edri.org/edrigram/number5/email.

86. Privacy International, ''PHR 2006—Republic of Poland,'' http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559594.

87. *PC World*, ''GUS chce Przygotować Superbazę Danych o Polakach?'' [Does the Chief Statistical Office Want to Prepare a ''Superdatabase'' of the Poles?], March 17, 2009, http://www.pcworld.pl/news/342115/GUS.chce.przygotowac.superbaze.danych.o.Polakach.html.

88. *BBC News*, ''Phorm 'Illegal' Says Policy Group,'' April 9, 2008, http://news.bbc.co.uk/1/hi/technology/7301379.stm.