

Nordic Countries

The five Nordic countries—Denmark, Finland, Norway, Sweden, and Iceland—have become central players in the European battle between file sharers, rights holders, and ISPs. While each country determines its own destiny, the presence of the European Union (EU) is felt in all legal controversies and court cases. The Internet industry extends across borders, and



so do filtering, military surveillance, and the monitoring of users. Privacy issues were formerly a concern of the elite, but with the growth of the information society, the right to privacy is now being discussed more widely in different political contexts. A popular civil rights movement of file sharers and privacy advocates has arisen out of Sweden in response to both national and international trends, and digital rights activism is increasingly directed at the European Parliament. Single-issue political parties concerned with privacy have now also begun to form in countries outside Europe.

Regional ICT Penetration

The World Economic Forum¹ ranks the Nordic countries at the very top of information and communication technology (ICT) use in the world. All five countries were listed in the top ten of a 2008–2009 survey prepared in partnership with the international business school INSEAD.²

The Nordic countries each have broadband Internet penetration rates of more than 30 percent of the population. According to a survey by the Organization for Economic Cooperation and Development (OECD) from June 2008, this figure places them in the top eight in comparison with the organization's 25 other member countries:³

1. Denmark 36.7 percent (1,996,408 subscriptions)
3. Norway 33.4 percent (1,554,993 subscriptions)
5. Iceland 32.3 percent (98,361 subscriptions)
6. Sweden 32.3 percent (2,933,014 subscriptions)
8. Finland 30.7 percent (1,616,200 subscriptions)

Regional Regulation

Norway and Iceland are the only Nordic countries that are not members of the EU. However, they do form a part of the European Economic Area (EEA) and have officially agreed to enact legislation similar to that passed in the EU in areas such as consumer protection and business law. As a result, laws are integrated in Norway⁴ and Iceland⁵ differently than in Sweden, Denmark, and Finland.⁶

Directives passed by the EU Commission and the European Parliament form a framework for lawmakers in the 27 member states to implement their own national laws before a certain deadline. Countries may decide to pass tougher laws than required by a directive. A key to understanding the heated European struggle surrounding intellectual property is an antipiracy directive called the International Property Rights Enforcement Directive (IPRED)⁷. This directive gives rights holders wide-ranging freedoms to investigate the identities of suspected file sharers and to obtain court orders to force ISPs to share personal information about customers suspected of digital piracy. The IPRED was introduced in 2004 and was repeatedly revised over the following years after complaints that its criminal-sanctions provisions were too wide ranging. An amended proposal (IPRED2) that may reintroduce some criminal sanctions was still being debated in 2009.⁸ However, the Anti-Counterfeiting Trade Agreement (ACTA) being secretly negotiated⁹ between the EU, the United States, and other countries seems to have taken over momentum from IPRED2.¹⁰

Sweden became the first EU country to put IPRED into effect on April 1, 2009. The BBC reported that Internet traffic in Sweden fell by 33 percent when the law was passed.¹¹ To protect the privacy of their customers following the implementation of IPRED, Swedish ISPs threatened to erase all their IP-number data.¹² Broadband operator AllTele offered their customers “dis-identification” services to hide file sharers from investigators.¹³ Another ISP, ePhone, refused to hand over any data to the courts.¹⁴

In early 2009, such actions were not against Swedish law,¹⁵ but they may be when another EU data-retention (logging) directive¹⁶ is implemented. Swedish lawmakers are working on a proposal for a law that would force ISPs to store data for at least six months.¹⁷

File sharing is extremely common in Nordic countries. The Swedish newspaper *Svenska Dagbladet* reported that 79 percent of Swedish males aged 15 to 29 are against the IPRED law.¹⁸ Open wireless local area networks (WLANs) have become an issue under IPRED, as innocent subscribers may be liable for illegal downloads by others. An IPRED-resistance movement started in Sweden encouraging people to open their networks and rename them Ipredia to mask actions by individuals.¹⁹

Copyright

The battles over copyright, private file sharing, and large-scale dissemination of links in the Nordic region are primarily playing out in the courts under the close watch of international organizations like the International Federation of the Phonographic Industry (IFPI). One Swedish court case over a file-sharing site has earned the most notoriety, but there have been several other cases in neighboring countries where copyright disputes ended in Internet filtering.

The Pirate Bay is a Swedish Web site that tracks BitTorrent files.²⁰ The Web site has an estimated 22 million users and is one of the Internet's largest sources for file sharing. While it is predominantly known for illegal P2P file sharing of music and films, it also handles links to content that can be legally shared. The fate of the Pirate Bay is the subject of a court battle as well as a forceful grassroots Swedish political movement that has resulted in the creation of a new political party called Piratpartiet (The Pirate Party).²¹

In Denmark, any attempt to access the Pirate Bay using a Danish ISP leads to a block page with links to a January 2008 ruling in a Danish civil court that all access to the Web site should be blocked. Rights holders originally filed the case against the Danish ISP Tele2, which today is owned by the Norwegian telecom Telenor. The Danish national court, Østre Landsret, confirmed the decision on November 26, 2008.²²

In April 2009, the Pirate Bay case²³ was submitted to the Danish Supreme Court. The basic question for the court to consider is whether an ISP can be charged with blocking access to a Web site, and whether the ISP, as the provider of the connection, can be held responsible for any content transmitted. Thus, the case is about the Danish interpretation of the EU Infosoc²⁴ directive on copyright and related rights, often called the Information Society Directive. Danish and Swedish parliaments and courts disagree on the interpretation of this directive.

This is not the first case of its kind in Denmark. In March 2006, the country's largest ISP, TDC, was forced to block certain IP addresses used for the transmission of copyrighted material by a Supreme Court decision.²⁵ The court declared that the transmission of copyrighted files was equal to temporary unauthorized copying and thus illegal. Court orders in 2007 forced Danish ISPs to block access to two Russian file-sharing Web sites, Allofmp3²⁶ and MP3Sparks.

On April 17, 2009, the four founders of the Pirate Bay were sentenced to one year in prison by a Swedish lower court and a combined fine of 30 million Swedish krona (USD 4 million). The Stockholm District Court determined that the defendants worked as a team in the operation and development of the Web site and that they had been aware that copyrighted material was being shared.

The convicted individuals filed a complaint that the presiding judge was biased, as a member of pro-copyright organizations. To the chagrin of the defendants, the court

official charged with deciding whether the first judge was biased was also known to have connections to pro-copyright organizations.²⁷ Furthermore, the judge²⁸ selected for the appeal case was a member of a pro-copyright group until 2005.

The Norwegian private law firm Simonsen Advokatfirma DA in 2007 obtained permission²⁹ from the Data Inspectorate (Datatilsynet) to register the IP addresses of users suspected of engaging in illegal file sharing. The firm represents rights holders. After not receiving assistance from the Norwegian police, the law firm attempted to have ISPs hand over the subscriber information associated with these addresses. Simonsen also drafted a cease-and-desist letter, which they requested the ISPs forward to copyright infringing customers. The International Federation of the Phonographic Industry asked Norwegian ISPs to block file-sharing sites, like the Pirate Bay. The ISPs refused to cooperate.

In a May 2009 copyright case regarding the Norwegian movie *Max Manus*, Simonsen sought a court order to get Norway's largest ISP, Telenor, to release the subscriber information of a person suspected of sharing the film illegally. The ruling was made in the lowest court (Stavanger Tingrett) on May 5, 2009, but the verdict was kept secret at the request of the film industry.³⁰ In fear of Swedish-style IPRED conditions, attempts are being made in Norway to initiate protests against secrecy.³¹ The case determined whether private industry (ISPs) or public authorities are the ones responsible for investigating breaches of law on the Internet. Dealing with a basic principle, the case is expected to be pushed into higher courts.

Norwegian telecommunications company and ISP Telenor has said that it is indifferent to preceding Swedish or Danish court decisions. A spokesperson for the ISP said the company would conform exclusively to the rulings of Norwegian courts. At the same time, a spokesperson for the Norwegian activist group FriBit rejected the idea that the *Max Manus* case had any significance, and said, "The Pirate Bay will continue and there are lots of other services like theirs ... the ruling gives no cause to automatically use other means, like censorship, to stop pirates."³² The fault lines in Norway are similar to the conflicts in other Nordic countries, but the solutions may not be identical.

Filtering

Internet service providers in all Nordic countries deploy filtering to isolate Web sites distributing child pornography. However, other infringements on freedom of expression and privacy have been controversial. Additionally, suspicions that the filters put in place could eventually be used to filter other sites have resulted in protests from many privacy and advocacy groups.

Nordic ISPs participate in the International Association of Internet Hotlines (INHOPE) project with 35 member countries.³³ Suspicious links are reported by organizations and the general public and passed on to relevant authorities for verification.

Partners in Denmark and Finland are Save the Children, and in Iceland, Heimili & Skoli. Financing originates from the EU Safer Internet Plus Program fund.³⁴ The Swedish nongovernmental child protection organization ECPAT does a similar job. In Norway, there is no official nongovernmental involvement.

Finland has a law to stop distribution of child pornography.³⁵ According to Section 1, the law was created to protect children and to block access to child pornography sites that are hosted outside of Finland. Finland also has laws against mocking God or religion (Criminal Act, Ch. 17, Sec. 10), but so far no content of this nature has been filtered.

The Finnish National Bureau of Investigation (NBI) compiles a secret list of Web sites containing child pornography and distributes it to ISPs for filtering.³⁶ In February 2008, the Electronic Frontier Finland (EFF) published an analysis of “Finnish Internet censorship.”³⁷ According to the report, the NBI filtering list contained about 1,700 Web sites in 2008. The EFF stated that a number of nonpornographic Web sites were found on the list.

In early 2009, the Web site Wikileaks,³⁸ which collects evidence of corporate and government misconduct, published a list of 797 Web sites censored by Finland. These were originally harvested and published by a well-known Finnish “white hat” hacker and activist Matti Nikki.³⁹ The list included his own Web site lapsiporno.info, where he criticizes secret censorship. Matti Nikki argued that there were several legal Web sites on the blocked list. On February 17, 2008, he stated that “nearly none of the sites on the child porn list seem to contain child porn.”⁴⁰ On March 23, 2009, all charges in a criminal investigation against him were dropped.

The blacklist operated by the Danish child pornography filtering system (3,863 blocked URLs) was leaked⁴¹ on December 23, 2008, and made available online. Its publication was a protest⁴² against secret censorship systems⁴³ and was supported by an activist group, IT-Politisk Forening. All Danish ISPs filter content based on the list. The head of the Telecommunication Industries Association of Denmark⁴⁴ says the list is of Web sites the authorities deem illegal, and that it should be expected to contain not only child pornography, but also racist, offensive, and libelous material. The Danish police IT investigation unit NITEC insists their list consists of illegal pornography sites only.⁴⁵ The Danish ISP industry staunchly refuses to filter questionable content (like gambling sites) unless they are contrary to statutory law or unless required to do so by court order. Attempts by politicians have been made in Denmark and other Nordic countries to protect government gambling monopolies from popular online poker.

All Norwegian ISPs operate a voluntary Child Sexual Abuse Anti-Distribution Filter (CSAADF). The filter is a blacklist of DNS addresses maintained and distributed by Kripos, the Norwegian police agency that deals with organized, financial, and other serious crimes. Each ISP implements this blacklist in its DNS servers by redirecting

attempts to access blacklisted Web pages to a page with a warning message.⁴⁶ The list is generated without judicial or public oversight and is kept secret by the ISPs using it. A list of supposedly blocked addresses was posted to Wikileaks in March 2009, containing 3,518 DNS addresses.⁴⁷ According to Wikileaks, many of the sites on the (Norwegian) list had no obvious connection to child pornography. The Norwegian and Danish lists had 1,097 URLs in common. Police in Germany raided the owner of the German Wikileaks domain name (a mirror site) in March 2009⁴⁸ because the Web site published copies of Nordic filtering lists.

As a member of the EEA, Norway has enacted legislation in line with the EU directive on electronic commerce,⁴⁹ which among other things states that ISPs shall not monitor their subscribers' use of the Internet. However, the general interpretation in Norway of the directive is that ISPs may be responsible for illegal content on their servers (e.g., child pornography, copyrighted material) if the provider, upon obtaining knowledge or awareness that such content is present, does not act expeditiously to remove or disable access to the content.

As a result of this directive, some ISPs have devised user agreements that empower the service provider to remove any controversial content, including content that is not illegal, to protect themselves from being held liable in any controversy surrounding content.

For example, in February 2008 the Norwegian ISP Imbera removed images of the Danish "Muhammad cartoons" from the Web pages of one of their customers, an organization called Human Rights Service, on the grounds that Imbera's user agreement prohibits users from uploading controversial content to Imbera's servers.⁵⁰

In Norway, the police can demand the subscriber information associated with a particular IP address from an ISP without a court order. This authority follows from a Supreme Court decision in 1999, in a case involving an Internet subscriber suspected of distributing child pornography.⁵¹ As a result of the ruling, the police can demand personal information in all types of cases. According to press reports, the refusal of the police to get involved in the *Max Manus* file-sharing case is the reason Simonsen Advokatfirma DA had to go to civil court.

Surveillance

All Nordic countries hold freedom of expression in high regard. Having military intelligence agencies monitor private citizens' telecommunications in detail and without controls has stimulated emotional debate and antisurveillance movements. The two major forces behind the legal changes in the Nordic countries are fear of terrorism and infringements on copyright. Government surveillance and censorship do not sit well with the Nordic notion of being free and democratic societies, and the introduction of new measures has created an unusually emotional debate in the region.

A survey of global surveillance activity by Privacy International in 2007 characterized Denmark as the only Nordic country that is an “extensive surveillance society,” while Finland, Sweden, and Norway were listed as exhibiting “systematic failure to uphold safeguards.”⁵² This classification included areas of privacy outside of digital life like democratic safeguards, visual surveillance, and workplace monitoring. Iceland had “some safeguards but weakened protection.” Denmark was placed in the same category as Bangladesh, France, India, Lithuania, the Philippines, and Romania, and was also the only Nordic country facing a “deteriorating situation.” Privacy International also publishes critical Country Reports Overviews⁵³ of current developments (latest dated December 14, 2007) in each country and wide-ranging in-depth analysis⁵⁴ (latest December 12, 2007) of each country (except Iceland).

The Danish national police IT-Efterforskningscenteret (NITEC), the center for IT investigations, is in charge of the blacklist for filtering child pornography sites. The unit has reportedly been investigating techniques for monitoring and deciphering conversations on the free online telephony service Skype.⁵⁵ The Danish police refuse to discuss their investigation methods. At the EU level, the judicial cooperation unit, EuroJust,⁵⁶ has mentioned Skype’s desire to cooperate with EU authorities, dating back to 2006.

On September 15, 2007, every Danish Internet user came under a comprehensive surveillance system, covering their history of Web sites visited, incoming and outgoing e-mails, and use of cell phones. The Danish implementation of the EU “data logging directive”⁵⁷ forces telecommunications companies, ISPs, hotels, Internet cafés, wireless hotspots, and apartment buildings with private Internet service to log and store information on all personal communication data for at least one year. These logs must be made available to police without a court order. The stated purpose is to fight terrorists. Two former heads of the Danish Security and Intelligence Service (PET)⁵⁸ are on record as opposing the expanded monitoring as unnecessary, worrisome, and damaging to the public’s basic democratic rights.⁵⁹

In Sweden, no logging law had yet been implemented in mid-2009, but surveillance of cross-border Internet and telecommunications had. Wiretapping and surveillance measures in Sweden have become a divisive issue in recent years. Those advocating the need for increased surveillance point to the threat from international terrorism and organized crime, and claim that additional measures are necessary to keep pace with changing technology. Opponents claim the measures extending the scope of surveillance pose a threat to civil liberties.

Following a prolonged political battle on privacy in the Swedish parliament, a law known as the “FRA-law” narrowly passed in June 2008, giving the Swedish National Defense Radio Establishment (FRA) the right to monitor all cross-border, cabled communication traffic.⁶⁰ In practice, all telephone calls, text messages, faxes, and e-mails passing into and out of Sweden became subject to surveillance as of January 1, 2009.

Public outrage over the law led to a significant revision in September 2008, and a number of wide-ranging surveillance permits were repealed.⁶¹ Among the compromises were requirements that court orders be issued before monitoring individuals, that no communications inside Sweden would be logged, and that the FRA could only work on behalf of the government and the military. The FRA thus monitors all “external threats,” not just “foreign military threats.”

Almost all telecommunication from Finland to the rest of the world passes through Sweden, leading to fear of the FRA-law in Finland. Both Swedish and Norwegian legal organizations have filed petitions at the European Court of Human Rights challenging the Swedish wiretapping law.⁶² In neighboring Denmark, citizens scrambled to assess whether they needed to change ISP and telephone companies in order to avoid being monitored. The Danish Federation of Industries, the largest commercial organization in the country, issued an elevated security warning, fearing commercial espionage by Sweden, and published guidelines on how to avoid surveillance of data by foreign governments at the end of 2008.⁶³

The law regulating the Norwegian intelligence agency establishes the rules for military Internet surveillance in Norway.⁶⁴ It gives the Intelligence Services under the ministry of defense (Forsvarets Etterretningstjeneste, FO/E) a very broad mandate to collect information that “serves the interests of Norway in relation to foreign states, organizations and individuals.” They must, however, refrain from collecting information about Norwegian citizens or legal entities, but there seem to be no restrictions as far as foreigners are concerned.⁶⁵

This broad mandate empowers the FO/E to perform electronic surveillance on communications originating from foreign individuals and organizations at the border, in a manner similar to the more explicit Swedish FRA-law. However, it is unknown how the FO/E currently exercises its surveillance mandate.

The legal framework with regard to Internet surveillance by the Norwegian police is the same as for all communications. The existing legal framework⁶⁶ for telephone wiretapping has simply been extended. To intercept e-mail or to tap an Internet line requires a court order, and a person under surveillance must be suspected of involvement in a serious crime punishable with ten years or more in prison (e.g., espionage).

Perspectives

All over Europe censorship and surveillance initiatives are promoted, like the French “three strikes” HADOPI law against piracy that introduced online snooping on suspected file sharers.⁶⁷ The law, which has already inspired clones in other EU countries, will be challenged because of a recent declaration by the European Parliament that it is illegal for an EU country to sever Internet access from anyone without the approval of

a court.⁶⁸ In May 2009, the European Parliament went through a new vote on details in a revision of the telecom rules directive.⁶⁹ Stemming from a Europe-wide mass mobilization, the European Parliament, with a large majority, essentially declared Internet access to be a fundamental right in the EU.⁷⁰ At the time of writing, conciliation between the European Parliament and the Commission was in progress. Nonetheless, six days later the French National Assembly passed the controversial law limiting these rights, and the following day the French Senate voted and confirmed the HADOPI law.⁷¹

In April 2008, the Danish parliament's Council on Technology published a report on IT security that said Danish Internet users seem to prefer the government having direct access to their computers in order to control and update their personal software prior to allowing them onto public Web sites.⁷² The report stated that users wanted public censorship of undesirable Web sites (e.g., those known for phishing) and preferred government security classification of selected software (like Web browsers). According to the report, there also seemed to be public demand for the introduction of hardware-based "digital identities," somewhat different from the prevailing secure "digital signatures." At the same time, fear of surveillance and registration of individual activities online was strong. The people surveyed also preferred that ISPs filter e-mail automatically rather than having the current opt-in solution.

The independent Danish IT-Political Association argued strongly against this vision of centralized control online. An extremely successful initiative of the association has been Polippix,⁷³ a Linux-based privacy protection software, distributed widely on CD and online. The Danish IT-Political Association, like its sister organizations in other Nordic countries, is a member of the European digital rights network EDRI, which tracks EU and national attacks on privacy, introduction of surveillance, and limits on Internet freedom. The work of EDRI is considered especially important because most regulation regarding the Internet, copyright, and privacy originate from European institutions or from international institutions with strong influence in Europe. However, the regulations do not prohibit individual countries from passing their own laws in addition to European ones.

A Swedish public opinion poll⁷⁴ published on May 18, 2009, showed that 43 percent of the population had no interest in the FRA-law, and among those who were interested, 34 percent were against and 23 percent in favor. The most critical sector of the population belonged to the 15–29 age group. The least worried group was conservatives over 60. The issue of privacy for the online generation has gained significance as a result of the FRA debate and the Pirate Bay file-sharing case. Indeed, a political party by the name Piratpartiet,⁷⁵ the Pirate Party, founded in 2006, was Sweden's third-largest party, with more than 48,000 members,⁷⁶ immediately before the June 7, 2009, elections. At the time of writing, public opinion polls indicated that Piratpartiet would win representation in the European Parliament and in the national parliament, Riksdagen, in the next general elections (expected in 2010).

Conclusion

Because they are at the forefront of ICT use in the world, the Nordic countries understandably have a lively public debate on copyright and privacy issues. New trends concerning online reality will likely originate here. In these countries, rights holders and the telecommunications industries are lobbying politicians in support of their different interests. Recent developments in Sweden offer hints that the general public, apart from indulging in massive pirating activities, is getting involved at the political level.

Following the FRA-law revision in Sweden, the governing right-wing alliance is deeply shaken by the unexpected and forceful youth movement that draws its energy from new age issues like privacy and file sharing. The Social Democratic Party, the originator of the antiterror surveillance law proposal a few years ago, has with its Green center-left partner announced that the issue of privacy (and the FRA) will be hot during the next Swedish general elections (expected in 2010). They intend to repeal the bill.

The battle over FRA in Sweden was fought with modern communication technology (e.g., Facebook, Twitter, blogs, texting). The use of new methods for political mobilization has reached critical levels, and activists are entering the political mainstream. Issues are crossing borders.

Political scientists Ulf Bjereld and Henrik Oscarsson at the University of Gothenburg in Sweden ask whether the security interests of the nation-state are colliding with the right to free cross-border communication in international networks. In an article published in the leading Swedish daily *Dagens Nyheter* on May 18, 2009, they question whether the Swedish state is struggling to retake control of the globally networked society's most valued raw material, means of influence, and driving force: information. These scholars see the Pirate Party as more than a single-issue platform, rather as a movement of liberal values, individual freedom, and personal integrity, where culture must be set free and patents and private monopolies opposed. Bjereld and Oscarsson believe the party's adherents favor citizen rights and freedoms, and demand clearer regulation and compliance with the social contract between government and citizens. It is a new civil rights movement of the information society.⁷⁷

It is obvious that very strong industrial interests are influencing politicians in the Nordic countries and Europe. The controversial decision by the European Parliament to make access to the Internet a "fundamental right" and the strong response, particularly in Sweden, from the predominantly young digital grassroots may be a forewarning of things to come. The EU and increasingly its individual members are struggling to regulate digital life, while activist users are trying to push back industrial dominance.

The Nordic countries are historically, legally, technically, and culturally very close to one another, and are all in some way associated with the EU. As more countries achieve the high Internet penetration rates of these five countries, we may see similar

cultural and political phenomena spilling over to the region, and maybe globally too. Already, “Pirate Parties” have formed or are in the process of being established in 22 other countries.⁷⁸ Certainly, the outcome of the legal battles regarding copyright, surveillance, and filtering in the Nordic countries should not be considered as without bearing on the wider region in the near future.

Notes

1. World Economic Forum, “The Global Information Technology Report 2008–2009,” March 2009, <http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/GlobalInformationTechnology>.
2. INSEAD, “Global Information Technology Report 2008–2009” (interactive version), <http://www.insead.edu/v1/gitr/wef/main/home.cfm>.
3. OECD Broadband Portal, <http://www.oecd.org/sti/ict/broadband>.
4. Norwegian Mission to the EU, <http://www.eu-norway.org/eu/norway+and+the+eu.htm>; Wikipedia on the relationship between Norway and the EU, http://en.wikipedia.org/wiki/Norway_and_the_European_Union.
5. Wikipedia on the relationship between Iceland and the EU, http://en.wikipedia.org/wiki/Iceland_and_the_European_Union.
6. Per Laegreid, Runolfur Smari Steinthorsson, and Baldur Thorhallsson, “Europeanization of Central Government Administration in the Nordic States,” *Journal of Common Market Studies*, Vol. 42, No. 2, pp. 347–369, June 2004, <http://ssrn.com/abstract=546906>.
7. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, http://eur-lex.europa.eu/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf; Amended proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights, COM/2006/0168 final—COD 2005/0127, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0168:FIN:EN:HTML>; Wikipedia on IPRED, Directive on the enforcement of intellectual property rights, http://en.wikipedia.org/wiki/Directive_on_the_enforcement_of_intellectual_property_rights.
8. Detailed Foundation for a Free Information Infrastructure (FFII) documentation of the IPRED2 proposals, <http://action.ffii.org/ipred2/#head-35c9f9ab741815ee371ba8a5f6fe95ad3a17b7a3>.
9. Foundation for a Free Information Infrastructure, “EU Council Deliberately Obstructs Access to ACTA Documents,” January 13, 2009, [http://press.ffii.org/Press_releases/EU_Council_deliberately_obstructs_access_to_ACTA_documents?highlight=\(ACTA\)](http://press.ffii.org/Press_releases/EU_Council_deliberately_obstructs_access_to_ACTA_documents?highlight=(ACTA)).
10. Ante Wessel, analyst for FFII, in conversation with author, June 4, 2009.
11. *BBC News*, “Piracy Law Cuts Internet Traffic,” April 2, 2009, <http://news.bbc.co.uk/2/hi/technology/7978853.stm>.

12. Mats Lewan, "Swedish ISPs Vow to Erase Users' Traffic Data," *CNET Digital Media*, April 28, 2009, http://news.cnet.com/8301-1023_3-10229618-93.html?tag=mncol;title.
13. Sten Gustafsson, "Bredbandsoperatör Döljer Fildelande" [Broadband Operator Hides File Sharers], *Dagens Nyheter*, May 14, 2009, <http://www.dn.se/ekonomi/bredbandsoperatör-doljer-fildelande-1.866108>.
14. Anders Frelin, "Bevisen i Första Ipred-fallet Ifrågasätts" [Proof of First IPRED Case Questioned], *Dagens Nyheter*, April 23, 2009, <http://www.dn.se/dnbok/bevisen-i-forsta-ipred-fallet-ifragasatts-1.850411>.
15. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF>.
16. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 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, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>.
17. Erika Svantesson, "Lagförslag: IP-adresser Ska Lagras ett Halvår" [Proposal: IP Addresses Must Be Stored for Half a Year], *Dagens Nyheter*, May 15, 2009, <http://www.dn.se/nyheter/politik/lagforslag-ip-adresser-ska-lagras-ett-halvar-1.867054>.
18. Tobias Olsson, "Klart Nej till Ny Fildelningslag" [Strong No to File-sharing Law], *Svenska Dagbladet*, March 17, 2009, http://www.svd.se/nyheter/inrikes/artikel_2604781.svd.
19. Ipreedia home page, <http://ipredia.se/wiki/Huvudsida>.
20. BitTorrent P2P file sharing site Pirate Bay, <http://thepiratebay.org/>.
21. Swedish Pirate Party English home page, <http://www.piratpartiet.se/international/english>.
22. Danish National Court confirms lower court decision to have ISP Tele2 block access to the Pirate Bay, November 26, 2008, http://issuu.com/comon/docs/kendelsetele2ifpi_261108.
23. Rune Pedersen and Mads Elkær, "Dansk Pirate Bay-sag Skal for Højesteret" [Danish Supreme Court Accepts Pirate Bay Case], *Computerworld*, April 24, 2009, http://www.computerworld.dk/art/51238/dansk-pirate-bay-sag-skal-for-hoejesteret?a=fp_3&i=5; Supreme Court date not set, May 25, 2009.
24. EU Infosoc Directive, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF>.
25. Danish Supreme Court decision, February 10, 2006, <http://www.it-retsforum.dk/index.php?module=Pagesetter&type=file&func=get&tid=4&fid=fil&pid=88&download=1>.
26. Allofmp3 verdict in Danish—for download, October 25 2006, <http://www.dr.dk/NR/rdonlyres/EF2AAB7A-0E04-4963-963A-463CD7550D72/361965/tele2...>; "Allofmp3, IT-Pol View,"

Danish IT-Political Association analysis of allofmp3 case, <http://itpol.polcast.dk/sager/nyheder/Allofmp3En>.

27. Ossi Carp, "The Pirate Bay: Nya Turer i Jävsfrågan" [Pirate Bay: News on Bias Case], *Dagens Nyheter*, May 20, 2009, <http://www.dn.se/kultur-noje/musik/the-pirate-bay-nya-turer-i-javsfragan-1.870677>.

28. Jenny Stiernstedt, "Ihrfeldt Ny Pirate Bay-domare" [Ihrfeldt New Pirate Bay Judge], *Dagens Nyheter*, May 19, 2009, <http://www.dn.se/kultur-noje/musik/ihrfeldt-ny-pirate-bay-domare-1.869487>.

29. Datatilsynet [Norwegian Data Inspectorate] licensing Simonsen Advokatfirma, December 8, 2006, http://www.datatilsynet.no/templates/article___1640.aspx.

30. Joakim Thorkildsen, "'Max Manus'-kjennelsen Blir Holdt Hemmelig" [Max Manus Verdict Kept Secret], *Dagbladet*, May 5, 2009, http://www.dagbladet.no/2009/05/05/kultur/film/max_manus/fildeling/6066821/; Øystein Sættem, "Why the Max Manus Verdict Encompasses So Much More," *FriBit*, May 11, 2009, <http://www.fribit.no/2009/05/11/why-the-max-manus-verdict-encompasses-so-much-more/>.

31. Marius Jørgenrud, "Aksjonerer mot Hemmelig Kjennelse" [Protests against Secret Judgment], *Digi.no*, May 6, 2009, <http://www.digi.no/812555/aksjonerer-mot-hemmelig-kjennelse>.

32. Ole Morten Knudsen, "Blir en Nøktern Feiring" [It Will Be a Sober Celebration], *Teknofil.no*, April 17, 2009, <http://teknofil.no/wip4/—noektern-feiring/d.epl?id=36355>.

33. European Commission, "INHOPE: Association of Internet Hotline Providers in Europe (INHOPE) as European Hotline Co-ordinator," http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2007-HC-121701.

34. European Commission, "Safer Internet Programme: The Main Framework for European Policy," http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm.

35. Laki Lapsipornografian Levittämisen Estotoimista 1.12.2006/1068 [Law against Spreading Child Pornography], <http://www.finlex.fi/fi/laki/ajantasa/2006/20061068>.

36. YLE, "Police Censor Porn Website," February 13, 2008, http://yle.fi/uutiset/news/2008/02/police_censor_porn_website_279365.html.

37. Kai Puolamäki, "Finnish Internet Censorship," Electronic Frontier Finland, February 18, 2008, <http://www.effi.org/blog/kai-2008-02-18.html>.

38. Wikileaks, "797 Domains on Finnish Internet Censorship List, Including Censorship Critic, 2008," January 5, 2009, http://wikileaks.org/wiki/797_domains_on_Finnish_Internet_censorship_list%2C_including_censorship_critic%2C_2008.

39. Lapsiporno.info, "Lapsiporno.info and the Finnish Internet Censorship," <http://lapsiporno.info/english-2008-02-15.html>.

40. Wikipedia, "Lapsiporno.info," <http://en.wikipedia.org/wiki/Lapsiporno.info>.

41. Wikileaks, "Denmark: 3863 Sites on Censorship List, Feb 2008," December 23 2008, http://wikileaks.org/wiki/Denmark:_3863_sites_on_censorship_list%2C_Feb_2008; Wikinews, "Wikileaks Tells Wikinews Why They Published Danish Child Porn Censorship List," December 23, 2008, http://en.wikinews.org/wiki/Wikileaks_tells_Wikinews_why_they_published_Danish_child_porn_censorship_list.
42. Mads Bang, "Hvorfor i Alverden vil I Boycotte Red Barnet?" [Why on Earth Do You Want to Boycott Save the Children?], *Computerworld*, September 18 2008, <http://www.computerworld.dk/art/47976>.
43. Mads Elkær, "Politiets Børneporno-liste Lækket på Nettet" [Police Child Porn List Leaked Online], *Computerworld*, December 23, 2008, <http://www.computerworld.dk/art/49524>.
44. Ib Tolstrup, CEO of The Telecommunication Industries Association of Denmark, personal communications, May 2009.
45. Søren Thomassen, deputy police inspector and head of NITEC, National police IT-investigations center, personal communication, May 2009.
46. The Child Sexual Abuse Anti-Distribution Filter warning Web page from Norwegian ISP Uninett, CSAADF is part of the COSPOL Internet Related Child Abusive Material Project (CIRCAMP) project initiated by the European Chief of Police Task Force, <http://csaadf.uninett.no/>.
47. Wikileaks, "Norwegian Secret Internet Censorship Blacklist, 3518 Domains, 18 Mar 2009," http://wikileaks.org/wiki/Norwegian_secret_internet_censorship_blacklist%2C_3518_domains%2C_18_Mar_2009.
48. Wikileaks, "Police Raid Home of Wikileaks.de Domain Owner over Censorship Lists," March 24, 2009, http://wikileaks.org/wiki/Police_raid_home_of_Wikileaks.de_domain_owner_over_censorship_lists.
49. "E-Commerce Directive," http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.
50. Ole Morten Knudsen, "Ytringsfriheten Overgår Ikke Alt" [Freedom of Speech Is Not Above Everything], *Teknofil.no*, February 22, 2008, http://www.teknofil.no/wip4/ytringsfriheten_overgaar_alt/d.epl?id=25769.
51. Norges Høyesterett afgørelse 1999 [Norwegian Supreme Court decision 1999], HR-1999-88-A (not online).
52. Privacy International, "The 2007 International Privacy Ranking," survey of Leading Surveillance Societies around the World, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559597&als\[theme\]=Communications%20surveillance](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597&als[theme]=Communications%20surveillance).
53. Privacy International, "PHR2006—Country Reports Overview," December 14, 2007, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559061](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559061).
54. Privacy International, "Denmark," December 18, 2007, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559545](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559545); Privacy International, "Norway," December 18, 2007, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559510](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559510); Privacy International,

"Sweden," December 18, 2007, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559487](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559487); Privacy International, "Finland," December 18, 2007, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559538](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559538).

55. Dan Mygind, "Dansk Skype-aflytning Mørklægges" [Danish Skype-interception Not To Be Discussed], *Computerworld*, August 1, 2008, <http://www.computerworld.dk/art/47198?cid=4&q=nitec&sm=search&a=cid&i=4&o=5&pos=6>.

56. "Eurojust Will Be Requested to Coordinate Internet Telephony Investigations," Eurojust press release, February 20, 2009, http://www.eurojust.europa.eu/press_releases/2009/25-02-2009.htm.

57. Logningsbekendtgørelsen [Logging Directive in Danish], <https://www.retsinformation.dk/Forms/R0710.aspx?id=2445>.

58. The Danish Security and Intelligence Service, PET, <http://pet.dk/English.aspx>.

59. Rune Pedersen, "Tidl. PET-chef: Logning Fremmer Mistænkeliggørelse" [Former PET-chief: Logging Furthers Suspicion], *Computerworld*, September 24, 2008, <http://www.computerworld.dk/art/41604/tidl-pet-chef-logning-fremmer-mistaenkeliggoerelse>; Rasmus Karkov, "Tidligere PET Chef Kritiserer Anti-terror Love" [Former Head of PET Criticizes Anti-terror Laws], *Comon.dk*, December 17, 2008, http://www.comon.dk/news/tidligere.pet.chef.kritiserer.anti-terror.love_39034.html.

60. Economist Intelligence Unit, "Surveillance Sweep: A New Surveillance Law Causes a Rumpus in Sweden," *Economist.com*, July 22, 2008, http://www.economist.com/displayStory.cfm?story_id=11778941.

61. Press release from Sweden's cabinet office: "Alliansen enig om stärkt integritet, tydligare reglering och förbättrad kontroll i kompletteringar till signalspaningslagen" [The alliance agrees on strong integrity, more clear regulation and improved controls in additions of the signals intelligence law], September 25, 2008, <http://www.regeringen.se/sb/d/10911/a/112332>; Wikipedia analysis of the FRA-law, <http://sv.wikipedia.org/wiki/FRA-lagen>; Wikipedia on the FRA-law, http://en.wikipedia.org/wiki/FRA_law.

62. David Landes, "Norwegian Group Joins Case against Sweden's Wiretapping Law," *TheLocal.se*, February 13, 2009, <http://www.thelocal.se/17578/20090213/>.

63. Rune Pedersen, "DI: Sverige Udgør Forhøjet Sikkerhedstrussel" [Danish Industry: Higher Security Threat from Sweden], *Computerworld*, November 14, 2008, <http://www.computerworld.dk/art/48926>.

64. Lov om Etterretningstjenesten av 1998-03-20 nr. 11 [Law on the Intelligence Agency], Norway's legal database, <http://www.lovdato.no/all/tl-19980320-011-0.html>.

65. Gisle Hannemyr, Department of Informatics, Oslo University, personal communication, May 21, 2009.

66. "Lov om Rettergangsmåten i Straffesaker av 1981-05-22 nr. 25" Kap 16a. Avlytting og Annen Kontroll av Kommunikasjonsanlegg (Kommunikasjonskontroll) [Penal Law Chapter 16a on Control of Communications], <http://www.lovdato.no/all/hl-19810522-025.html#map026>.

67. Eric Pfanner, "France Approves Crackdown on Internet Piracy," *New York Times*, May 13, 2009, <http://www.nytimes.com/2009/05/13/technology/internet/13net.html>.
68. European Digital Rights, "European Parliament Votes against the 3 Strikes, Again," May 6, 2009, <http://www.edri.org/edri-gram/number7.9/ep-plenary-votes-against-3-strikes>.
69. "No Agreement on Reform of Telecom Legislation," press release, European Parliament, May 6, 2009, http://www.europarl.europa.eu/news/expert/infopress_page/058-55086-124-05-19-909-20090505IPR55085-04-05-2009-2009-true/default_en.htm.
70. Gérard Sédrati-Dinet, "Amendment 138/46 Adopted Again: Internet Is a Fundamental Right in Europe," *laquadrature.net*, May 6, 2009, <http://www.laquadrature.net/en/amendment-138-46-adopted-again>.
71. European Digital Rights, "France: Three Strikes Law Voted for Good," May 20, 2009, <http://www.edri.org/edri-gram/number7.10/france-three-strikes-voted>; Ernesto, "France Passes 'Three Strikes' Anti-Piracy Law," *TorrentFreak*, May 12, 2009, <http://torrentfreak.com/france-passes-three-strikes-anti-piracy-law-090512/>; Marguerite Reardon, "France Passes Controversial Antipiracy Bill," *ZDNet*, May 13, 2009, <http://news.zdnet.co.uk/internet/0,1000000097,39651441,00.htm>.
72. "Brugernes It-sikkerhed" [User IT-safety], Teknologirådet [Danish Parliament's Council on Technology—listing of reports], April 22, 2009, <http://www.tekno.dk/subpage.php3?page=udgivelser/download.php3&toppic=udgivelser>.
73. "Privacy software collection Polippix details," IT-Pol, <http://itpol.polcast.dk/sager/polippix/polippix-den-politisk-cd-privatlivets-fred>.
74. Ulf Bjereld and Henrik Oscarsson, "Nästan Varannan Svensk Struntar i FRA-frågan" [Almost Every Second Person Doesn't Care about the FRA-question], op-ed article, *Dagens Nyheter*, May 18, 2009, <http://www.dn.se/opinion/debatt/nastan-varannan-svensk-struntar-i-fra-fragan-1.868277>.
75. Piratpartiet [Pirate Party's home page], <http://www.piratpartiet.se/>.
76. Membership listing of Swedish political parties, <http://www.piratpartiet.se/medlemsantal>.
77. Ulf Bjereld and Henrik Oscarsson, "Nästan Varannan Svensk Struntar i FRA-frågan," *Dagens Nyheter*, May 18 2009, <http://www.dn.se/opinion/debatt/nastan-varannan-svensk-struntar-i-fra-fragan-1.868277>.
78. List of countries with Pirate Parties: <http://www.pp-international.net/>.