Compliance or Obscurity? Online Anonymity as a Consequence of Fighting Unauthorised File-sharing

Larsson, Stefan; Svensson, Måns

Published in:
Policy & Internet

DOI:
10.2202/1944-2866.1044

2010

PSO

Policy & Internet

www. psocommons.org/policyandinternet

Vol. 2: Iss. 4, Article 4 (2010)

Compliance or Obscurity? Online Anonymity as a Consequence of Fighting Unauthorized File sharing

Stefan Larsson, ***Lund University***
Måns Svensson, ***Lund University***

Abstract

The European Union directive on Intellectual Property Rights Enforcement (IPRED) was implemented in Sweden on April 1, 2009, and was meant to be the enforcement needed to achieve increased compliance with intellectual property online, especially copyright. This, therefore, was the manifest function of the directive. The article empirically shows changes in levels of use of Online Anonymity Services (OAS) as a result of the implementation of IPRED in Sweden, as being a latent dysfunction of the implementation The data consists of two surveys of about 1,000 people between 15 and 25 years of age, where the first survey was conducted two months prior to the implementation of IPRED, and the second one seven months afterwards. This data is complemented with OAS statistics as well as Google search engine statistics in Sweden during 2009 on a selection of phrases related to online anonymity, revealing the link between encrypted anonymity fluctuations and copyright enforcement.

The article suggests that a key to understand any relationship between IPRED and fluctuations in online anonymity can be found in the law's relationship to social norms and levels of perceived legitimacy. The implementation of illegitimate laws is likely to spur dysfunctional (for the law) counter-measures. In the case of copyright enforcement and encryption technologies, the first seems to drive the other to some extent, affecting the balance of openness and anonymity on the Internet, possibly and at worst leading to that the enforcement of legislation that has a weak representation among social norms negatively affects the enforcement of legislation that has a strong representation among social norms.

Published by Berkeley Electronic Press

Keywords: anonymity, pseudonymity, encryption, vpn, social norms, manifest and latent, functions and dysfunctions, unauthorized file sharing, IPRED, copyright enforcement, sociology of law

Author Notes: Stefan Larsson, LLM, MaSoS, Licentiate of Technology, PhD candidate in Sociology of Law, Lund University, Sweden, stefan.larsson@soclaw.lu.se. Måns Svensson, PhD in Sociology of Law at Lund University, Sweden, mans.svensson@soclaw.lu.se. This study is part of the research project Cybernorms: Norm-creation processes in young Web cultures, which is funded by the Knowledge Foundation in Sweden.

Recommended Citation:
Larsson, Stefan and Måns Svensson (2010) "Compliance or Obscurity? Online Anonymity as a Consequence of Fighting Unauthorised File sharing," *Policy & Internet*: Vol. 2: Iss. 4, Article 4.
DOI: 10.2202/1944-2866.1044
Available at: http://www.psocommons.org/policyandinternet/vol2/iss4/art4

Introduction

There have been a number of initiatives within the European Union to reduce illegal file sharing of copyrighted content, and to strengthen compliance with copyright legislation within the Union. One of these directives is the IPR Enforcement Directive (IPRED),[1] which was implemented in Sweden on April 1, 2009. The implementation received a lot of attention in Sweden: Internet Service Providers (ISPs) noisily defended their neutrality, their subscribers and their communication integrity, and copyright holders' representatives spoke of all the cases that could now—as a result of IPRED—be raised in court against violators of their clients' rights. In the midst of this clamour, the traceability of online actions was debated, with providers of encrypted IP VPN services claiming that the increased interest in their services was "explosive." The purpose of the directive is to regulate enforcement of intellectual property rights within the European Union by adding measures, but not by changing the substantive IP laws themselves. One such important measure is the rights holder's possibility to, by a court order, retrieve identification data connected to IP addresses from the ISPs.

This connects to larger questions of how the character of the Internet is balanced in terms of traceability and anonymity, relating to issues of legal enforcement, not only regarding copyright but also other legal areas. Anonymity—or rather, pseudonymity—can be seen as having been the normal state on the Internet, following from the way in which the Internet was built; a state only breached by choice. However, incompatible trends can be seen. As Andersson puts it in his thesis on file-sharing rationalities, "[t]he networks of the Internet, and p2p in particular, are similarly non-familial; they are essentially stranger-to-stranger, non-overseeable (at least beyond a set horizon) and strictly governed by protocol" (Andersson 2010b, 225). Contrasting with this, for private Internet use a more recent trend has been towards a less anonymized state (witness the massive numbers committed to social networks such as Facebook). In line with this, there is also a development whereby global service providers who own the physical infrastructure are increasingly moving towards so-called hosted services, i.e., software that is not present on your machine but in the "cloud." This often connects personal information in ways that can have de-anonymizing effects. Along with this development follows the transition from today's IP addresses (IPv4) to future IP addresses (IPv6), which can provide for each

[1] The directive's full title is Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights.

machine—including mobile phones, vehicles, clothing, and buildings—to be given its given unique address. This alone could de-anonymize a whole new set of behavioral patterns in a radical way (Andersson 2010a).

This article connects the use of Online Anonymity Services (OAS) to unauthorized file sharing of copyrighted content. The spread of encryption to enable online anonymity has been regarded both as a tool for privacy, ensuring free speech and avoiding harassment of political dissidents in repressive states, and as something that will impede criminal investigations (Lessig 2006, 45–60; Rowland 2009). It is clear that this double-edged sword, working to de-identify whichever master it serves, impacts both the character of the Internet and the character of law enforcement.

In many ways, 2009 was for Sweden the year in which "online anonymity" became a valid phrase in everybody's mind. It was the year in which at least two new operators of services that provide anonymity as a subscription started, and in which the already established ones saw a sudden increase in subscribers. One of the stronger contributors to this increase seems to have been the implementation of the IPR Enforcement Directive. This article identifies the unintended effects of the implementation of IPRED in Sweden in terms of an increase in online anonymity, placing this in a broader trend or context regarding the diffusion of techniques for anonymity online. There are several probable effects of implementation, including manifest and latent functions, as well as dysfunctions (see Merton 1936; 1949; 1976). In simple terms, manifest functions are those that are intended, and latent functions are unintended. Unanticipated consequences and latent functions are not exactly the same: a latent function is a type of unintended consequence that is still functional for the designated system, whereas the latent dysfunction is a type of unintended consequence that is self-defeating for the same. Further than this, there can be non-functions that "are irrelevant to the system which they affect neither functionally or dysfunctionally" (Merton 1949, 105). The interesting focus from a sociological perspective on law lies in finding the dysfunctions of an implemented law—the effects that directly counter the purpose of the law—which we elaborate on below. By using the terminology of Robert K. Merton, this article focuses and empirically studies the changes in levels of anonymity among 15- to 25-year-old Swedish Internet users as a result of the implementation of IPRED, and discusses other possible latent dysfunctions.

Research Context and Questions

Although there seem to be no earlier studies conducted regarding a link between copyright enforcement and resulting fluctuations in online anonymity, there is literature on privacy issues related to online anonymity/pseudonymity and law (Froomkin 2008; Rowland 2009), privacy issues related to fighting terrorism (Rosenzweig 2005), cryptography and regulability (Lessig 2006), and the question of online anonymity itself has received significant attention over the years. There are also, of course, a wide variety of studies on unintended consequences of law, some of which described in terms of being "dysfunctions" (see Vago 2009, 22–23). Sociology of Law has been described as a discipline that generally deals with studying the consequences of law from a social scientific perspective, in order to state and study the flaws of the legal application (see, for example, Svensson 2008, 72), and this perspective often focuses on the difference between law in books and law in action—using empirical data regarding the second in order to criticize the first.[2]

Regarding online anonymity as a regulated phenomenon, Froomkin (2008) concludes that the overall U.S. policy towards anonymity remains primarily "situational, largely reactive, and slowly evolving," and that "law imposes few if any legal obstacles to the domestic use of privacy-enhancing technology such as encryption." However, it is not long ago that encryption was seen as a tool not to be used by a broader public (Levy 2001). Cryptography was in the United States (and other countries) initially regulated as munitions, and used primarily by soldiers and spies, and there were long attempts to restrict its availability and use (Levy 2001). Cryptography is today accepted as an everyday use technology, for instance when it comes to banking or corporations sharing sensitive data (see, for instance, Lasica 2005, 232), but is often seen as problematic when connected to online anonymity. The American Pew Research Center conducted a survey ("Future of the Internet IV"), which gathered opinions from prominent scientists, business leaders, consultants, writers, and technology developers. This survey contained a section regarding online anonymity, and

[2] The Department of Sociology of Law at Lund University in Sweden studies the relationship between law, policy, and social norms (see, for instance, Appelstrand 2007; Baier 2003; Bergman 2009; Hydén 2002; Hydén and Svensson 2008; Larsson 2008; 2009; Svensson 2008; Svensson and Larsson 2009). Online anonymity in relation to stronger enforcement of copyright is a good example of the main interest of knowledge for policy research that is dealt with by sociology of law studies.

about 40 percent of the surveyed experts thought that anonymous activities online would be sharply restrained by 2020 (Pew Research Center 2010, 40).

The present study is part of a bigger survey conducted at two different time points, encompassing about 1,000 Swedish Internet users between 15 and 25 years of age. The data used for this article includes questions on the usage of services for anonymous Internet browsing, as well on individuals' expectations about starting to use such anonymity services if new legislation increased the possibility of their being caught sharing files illegally. The first survey was conducted two months prior to the implementation of IPRED in Sweden, and the second one seven months afterwards—affording us the opportunity to study the consequences of the Directive's implementation.

The question of anonymity is an important indicator of legitimacy issues of law in society. A change in anonymity levels online as a result of copyright enforcement legislation tells us something about the legitimacy of copyright law, as it does about how laws can have dysfunctional and unintended aspects that counter their very purpose. The above point leads to the four research questions that have guided this research:

1. To what extent can fluctuations in online anonymity be seen as an unintended consequence of the implementation of IPRED in Sweden?
2. If so, is it dysfunctional for copyright enforcement?
3. To what extent is the use of encrypted online anonymity services connected to unauthorized file sharing of copyrighted content?
4. In what way can the relationship between IPRED and fluctuations in online anonymity be found in the law's relationship to social norms and levels of perceived legitimacy?[3]

[3] We have written elsewhere about the changes in actual file-sharing frequencies as well as social norm strength regarding unauthorized file sharing as a result of the implementation of IPRED (Svensson and Larsson, forthcoming; see also Svensson and Larsson 2009). These articles can be interpreted as regarding the *intended purpose* of the law, where the unintended consequences and the role of online anonymity have remained overlooked.

Functions and Dysfunctions of Law

Vago (2009) describes several general types of dysfunctions of law that "may evolve into serious operational difficulties if they are not seriously considered" (Vago 2009, 22). The dysfunctions of a law can be described by the "bad" consequences, which Cass R. Sunstein (1994, 1390) describes in terms of "self-defeating," meaning measures that actually make things worse from the standpoint of their strongest and most public-spirited advocates. Sunstein points out what we here regard as being one of the key problems of empirical limitations in a dogmatically encapsulated process of law-making, the problem of unintended consequences of legal implementation: what will be the real-world consequences of an implementation? Will it fulfill its intended purpose? Will it have dysfunctions that defeat their own purpose?

By formulating the "unanticipated consequences of purposive social action" in 1936, Merton gave a higher profile to the idea of hidden effects to action. This idea has reverberated in a multitude of areas, often with reference to Merton (Aubert 1954; Brown 1992; Christie 1965; House 1968; Mathiesen 2005; McAulay 2007; Ridgway 1956; Roots 2004; Sunstein 1994). Merton defined *function* as "those observed consequences, which make for the adoption or adjustment of a given system" (1949/1968, 105). "Function" is therefore something other than "dysfunction," in the sense that just as structures or institutions could contribute to the maintenance of other parts of the social system, they also could have negative consequences for them. As a type of safety valve, for the cases when neither of the two terms above is applicable, Merton uses the term *non-functions*, which he describes as simply irrelevant to the system under consideration. This could be seen as a "survivor" from earlier historical times that have no significant effect on contemporary society (Ritzer and Goodman 2003, 241–249). As we have already seen above, functions, dysfunctions, and non-functions can either be intended (manifest) or unintended (latent). There are *latent functions* that are unintended but still operate in line with the intended purpose of the initial action. This means that *latent dysfunctions* are unintended and "negative consequences for the structures and systems under consideration" (Merton 1949/1968, 105). When it comes to law, these latent dysfunctions can be direct consequences of what Sunstein speaks of as "self-defeating legislation" (1994). From the perspective of implementing copyright enforcement legislation, unforeseen consequences that somehow aid unauthorized file sharing in violation of copyright laws are one such latent dysfunction.

Legal and Political Context of IPRED

There have been a number of initiatives within the European Union to reduce illegal file sharing of copyrighted content, and to strengthen compliance with copyright legislation within the Union. One of these directives is the IPR Enforcement Directive (IPRED), which was implemented in Sweden on April 1, 2009. IPRED generated significant debate and protests in the media, the blogosphere, and political arenas. The EU passed IPRED in April 2004 because it was held to be "necessary to ensure that the substantive law on intellectual property … is applied effectively in the Community"; further, it was held that the "means of enforcing intellectual property rights are of paramount importance for the success of the Internal Market" (Recital 3). Although the scope regards the entire IP spectrum, the Directive has in general been discussed in connection with copyright enforcement. The Directive refers to all Member States being bound by the Agreement on Trade Related Aspects of Intellectual Property (TRIPS Agreement), which emphasizes the global regulatory connection on copyright between nations, the EU as well as international treaties.

IPRED can be seen as an exception to the otherwise ruling legal principle of online anonymity, often expressed in terms of privacy.[4] The implementation of IPRED in Sweden means that intellectual property rights holders can, whenever they assume that their rights have been violated online, take their complaints to a court, which will then examine the evidence and extent of file sharing to establish if the IP address should be released or not (IPRED, Article 6.1; see Prop. 2008/09:67). If the court finds the copyright holders to have shown probable cause for that a violation of copyright has occured, the copyright holder can then send a warning to the alleged violator or take legal action against him/her, after having retrieved the identity from the ISP (Section 53c of the Swedish Copyright Act 1960:729). At the time of implementation, the parallel but (in terms of copyright-related events) interconnected case of the BitTorrent tracker site "The Pirate Bay" was unfolding in the District Court of Stockholm. The Court announced its verdict on April 17, 2009, which added to public interest in copyright and file-sharing issues in Sweden and abroad.[5]

[4] For instance, as regulated under the Data Protection Directive: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[5] The trial against the four men behind the Pirate Bay site was followed by the international press, such as Spain's leading daily, *El Pais*, *ABC News*, the *Los Angeles Times*, and *The Telegraph* (see the reference list). The four men were sentenced to a year's imprisonment and to collectively pay about 2.84 million euros in damages to the

The pursuit of unauthorized file sharing in order to enforce copyright legislation is of course in no way limited to the IPRED directive and its implementation in the EU. A common strategy for groups of rights holders has been to collect databases of IP numbers. They see this as the key to enforcing their rights against file-sharing violators and so seek, quite naturally, to tie the identities of violators to IP numbers, giving the ISP a central role in the battle (see, for example, Vincents 2007 on copyright holder strategies). For instance, British, U.S. and Danish law firms have been sending settlement letters to thousands of consumers after IP identification was made available by ISPs. The key role of ISPs has also been the center of attention in seminal cases in the United States, for example in the *RIAA v. Verizon* case in which the U.S. Court of Appeals for the D.C. Circuit ruled against the recording industry's attempts to compel ISPs to identify their subscribers (Kao 2004). In Sweden, the implementation of IPRED made many ISPs discard identity information at an even faster rate than before, often with reference to consumer integrity—neither the Directive nor its Swedish implementation requires ISPs to retain log data for any particular period of time. Log data retention is already regulated as a result of the previous implementation of an EU Directive under the principle of protecting subscribers' integrity; it therefore obliges ISPs to not store such data longer than necessary for subscriber invoicing.[6] The implementation of IPRED in Sweden has put the log data policies of ISPs into focus, causing a number of them to publicly announce that they do not store this type of data any longer than is absolutely necessary (Gustafsson 2009). To date, this legislation has only led to two court cases, despite the initial media reports of "hundreds" of cases being prepared by copyright holder's interest groups.[7]

The Directive puts the retention of log data in focus, which will be expanded by the ongoing implementation of the data retention Directive in the EU, even though the impetus for this Directive was to battle terrorism

media companies that were the plaintiffs. Both sides appealed, and the case had yet to be decided upon at the time for the submission of this article.

[6] In Sweden the regulation today regarding the protection of privacy in electronic communication is mainly found in Chapter 6 of the *Electronic Communications Act* (2003, 389). With regard to traffic data, Section 6 states that "Traffic data that is required for subscriber invoicing and payment of charges for interconnection may be processed until the claim is paid or a time limit has expired and it is no longer possible to make objections to the invoicing or the charge." The legislation emphasizes the importance of not storing data too long, for the sake of privacy protection, following from Directive 2002/58/EC.

[7] This includes the so-called Ephone case (Case Ä 2707-09, renamed in higher court to ÖÄ 6091-09, October 13 2009) and the TeliaSonera case (Case Ä 9211-09).

and "serious crime."[8] The role of ISPs, as well as the issue of whether or not Internet access should be blocked for copyright violators, has been highlighted by the so-called HADOPI law in France (2009) and The UK Digital Economy Act (2009), putting a new duty on ISPs to cooperate with copyright owners in identifying and pursuing infringements of their copyright. This was also discussed in the drafting of the EU Telecoms Reforms Package.[9] In line with the strong copyright trend, the EU is taking part in somewhat confidential negotiations, with for instance the United States, Japan, and Switzerland, of an Anti-Counterfeit Trade Agreement (ACTA) that may lead to a significant elevation of the copyright protection for the Member States (Kaminsky 2009; Larsson forthcoming). Also, despite the implementation of IPRED, the European Union is pushing for the enactment of a related Directive that would establish criminal sanctions for various intellectual property violations. This is called IPRED2: Intellectual Property Rights Enforcement Directive 2005/0127 (see Agarwal 2010, for critical commentary).

In the months after the implementation of IPRED in Sweden, the media reported that interest in anonymity services rose strongly, and OASs

[8] 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 an amendment to Directive 2002/58/EC.

[9] HADOPI is the nickname for a French law officially entitled *Loi favorisant la diffusion et la protection de la création sur Internet* ("the law favouring the diffusion and protection of creation on the Internet") which regulates and controls the usage of the Internet in order to enforce compliance with copyright law. The nickname is taken from the acronym for the government agency created by the law.

The UK government introduced the Digital Economy Bill on November 20, 2009, [HL] 2009-10. The bill "aims to support growth in the creative and digital sectors and includes measures aimed at tackling widespread online infringement of creative copyright, such as peer-to-peer file-sharing" (see the press release of November 20, 2009, "A world class digital economy for Britain", 155/09). The bill was a result of more than a year of consultation and debate, and includes plans to send warning letters to persistently unlawful file-sharers and pave the way for enduring illegal sharers to have their broadband cut off, starting in 2011.

The Telecoms Reform Package was presented to the European Parliament in Strasbourg on 13 November 2007, voted upon 6 May 2009 and finalised 25 November 2009. The reform package originates from a non-legislative resolution on "Cultural industries in Europe", generally referred to as the 'Bono Report' after the French Socialist MEP responsible for the drafting of the resolution. The reform package is a cluster of directives (COM [2007] 697) that to a great extent puts the role of the Internet Service Providers in focus.

http://www.psocommons.org/policyandinternet/vol2/iss4/art4
DOI: 10.2202/1944-2866.1044

claimed that they were having difficulty coping with all the new customers. Bloggers and net activists established websites denouncing the implementation of IPRED, and created other sites to track the court cases that were anticipated to follow from its implementation, and the petitions started in opposition to the law. Moreover, the youth sections of the Swedish political parties unified themselves in their struggle against the implementation of IPRED. Cryptography experts raised the issue that a more widely anonymous Internet would make it harder to find and counter other types of criminality, such as terrorism and child pornography.

Online Anonymity

When Bob Kahn and Vinton Cerf began working in 1973 on what became the underlying protocol for the Internet, TCP/IP, they did it under Kahn's previously formulated ambitions; of which one was that there should be no global control at the operations level (Leiner et al. 2009, 24–25). The simplicity and openness of the underlying structure created its own success by allowing networks to connect, and other applications such as the World Wide Web (addresses) and File Transfer Protocol, FTP, to operate upon it (Leiner et al. 2009). It is the Internet Protocols, the IP addresses that have become the key to unlocking the identities of the WWW-surfers on the Internet. The bridge between the "anonymous" IP address and the offline identity is watched over by the ISPs, which keep track of their subscribers mainly for billing purposes. This is the reason why whenever anyone wants to find out the identity behind the actions committed "by an IP-number," for instance a violation of copyright, it is at the door of the ISPs that they come knocking. From a sociological point of view, the normal state of online activities can be seen as anonymous. This anonymity can be breached willingly, for instance by individuals adding information on social networking sites (which broaden the identifying aspects of their offline identity), or unwillingly, for instance when forced in a criminal investigation.

The use of the term "anonymous" can be confusing from an online perspective (see Edman and Yener 2009, for a detailed explanation of anonymity systems). While it is reasonable to speak of "levels" of anonymity, online reality has also been described in more mundane terms of being anonymous in and of itself (Morio and Buchholtz 2009). When speaking of anonymity in such a sense it is not related to the degree of traceability, but to the lack of aspects such as image, voice, and situation in the online milieu. However, for the undertaking of this article, it is the

degree of traceability that is of most importance when it comes to anonymity. The absolutist definition of anonymity (i.e. complete untraceability) holds that this type of anonymity makes it ill suited for most kinds of web interactions (Rao and Rohatgi 2000). This is why web applications are often designed for pseudonymity (that is, the traceable version of anonymity—although this is often perceived as being truly anonymous by individual performing tasks online; Du Pont 2001; Rao and Rohatgi 2000). We use the term "anonymity" in a broad sense in this article; that is, we include "true" untraceable anonymity, but mostly will deal with the pseudonymous state. To keep this clear, we will speak of activities as being more or less anonymous, and will regard anonymity as a form of scale, rather than as a single, true, anonymous state.

Encryption for Sale

In this article we refer to OAS as the use of IP VPN encryption services, which in general result in a technically pretty robust pseudonymity. These services provide the user with the means of avoiding having their IP numbers connected to their offline identity; often for a subscription fee. An anonymity service, or anonymity server, is a server that provides the ability to send email, visit websites, or undertake other activities on the Internet anonymously. All traffic between the user (client) and server (host) is encrypted so as not to be decipherable by third parties. There is a form of trust issue with the OAS, in the sense that they are not always held to be completely reliable, for instance in terms of maintaining connectivity.

There are a variety of services, which work in slightly different ways. With some services, users connect to the service supplier's servers with a 128-bit encrypted Virtual Private Network (VPN) connection. The encrypted VPN "tunnel" between the user's computer and the ISP server ensures that the ISP cannot determine what type of information is being sent to and from the user, which obviously prevents or impedes intrusion. The IP number that any external party can see leads to the service provider, not the client. Some services can be administered through an email account, which makes it even harder to identify the user. Services for online anonymity that can be found on the Swedish market include (the early established) Relakks and Dold.se services, and of course Ipredator[10] and Mullvad.se. In addition to these there are of course foreign services, such as the SwissVPN and Ivacy, which naturally are open for Swedish subscribers.

[10] Established in 2009 by a group related to the BitTorrent tracker site "The Pirate Bay," as a response to the Swedish IPRED law.

Anonymous Ways Beyond the Pay services

There are ways to browse the web and still be quite anonymous without using an anonymity service. Using Internet cafés is an example of a set-up that achieves anonymity without encryption, which is why governments in both India and Italy have implemented mandatory identification for the customers of such establishments. Per-minute Internet access in convenience stores is a growing market (at least in Sweden), providing strong levels of anonymity through open networks in train stations and libraries. Large files can be sent and received anonymously or pseudonymously by using a "one click hosting" (OCH) service; these allow users to upload one or more files to a server, either free of charge or for a premium. Most services return a URL, which can be given to people who then can download the file. If the service does not lock the number of permitted downloads to a few, the service can be used for file sharing in larger numbers. There are for instance many Internet forums that share URLs, which has further contributed to make these services a complement to p2p file sharing: one of the few studies to address this (Antoniades et al. 2009) compared the OCH service RapidShare, which attracts large amount of users, to BitTorrent file sharing in general.[11] When including the study of OCH content indexing sites, which are an essential component for file sharing using OCH services, they concluded that "in OCH services, much like in p2p file sharing systems, a very small number of users upload most files, which are often copyrighted content, favouring audio albums, video movies, and applications" (Antoniades et al. 2009, 234). This is likely true. On the other hand, once an initial upload is performed, there is little incentive to perform a second initial upload of the same content, unless this second upload comes with a useful difference such as improved quality or smaller size. This could possibly be relevant for OAS use, where the group of initial uploaders have a stronger incentive of being less traceable.

One could also speak of "offline anonymity" in the sense that if the will to share digital content is strong enough, it will occur in the form of hand-to-hand sharing via USB sticks or other storage media; generally referred to as sneakernets. Pre-paid mobile phones can also be used to access the Internet anonymously. BitTorrent sharing services providing a stronger level of anonymity than the "traditional" BitTorrent sharing services are also under development. There are also networks being established with secrecy

[11] Another example of a globally popular OCH service is MegaUpload. On the Swedish arena there is, for instance, Sprend.

for users as their primary objective. These networks, such as Freenet, are not subject to any external censorship whatsoever; employing software that released by Ian Clarke in 2000, the network does not leave traces and cannot be found by search engines. These are uncontrolled, relatively untraceable areas of the Internet that have been referred to as the "deep web," the "dark web," or "beneath the surface web" (Bergman 2001; Lasica 2005, 224f.). Other examples of networked solutions that create anonymity with extremely low traceability are The Onion Router (TOR) and i2p.

Method

We conducted two surveys of about 1,000 Swedish Internet users between 15 and 25 years of age, including questions on the degree of use of services that anonymize Internet browsing. The first survey was conducted in January and February 2009, and the second survey in October 2009. Since IPRED was implemented between the two surveys (April 2009), the surveys give us the opportunity to study some of the consequences of its implementation.

Two interviews were also conducted, one with a representative from one of Sweden's leading pay services for online anonymity (who requested that the company remain anonymous), and one with a representative from "Sprend," a company running a one-click hosting service with a strong majority of Swedish users. Anonymity service operators are reluctant to release data regarding their subscribers, mostly due to competition reasons: they simply do not want their competitors to know how their business is doing. So in order to complement the surveys, and as a way to corroborate the connection between the implementation of IPRED and online anonymity, statistics from Google Trends have been used. These have been compared for a selection of search phrases relating to online anonymity in the geographical area of Sweden (identified by Google from IP address information). The selected phrases were: "vpn," "tor," "ipredator," "relakks," "dold.se," "mullvad," "ivacy," "anonymous," "megaupload," and "hide."

About the Surveys

The first survey was emailed to 1,400 recipients during January–February 2009; by the end of the survey process, the respondents numbered 1,047, generating a response frequency of 74.8 percent and exceeding our target of 1,000 respondents. For the second survey, 1,477 participants were emailed,

and once again 1,047 people responded, producing a slightly lower response frequency rate of 70.9 percent. The selection was made randomly for the age group, from the CINT panel eXchange register that contains 250,000 individuals in Sweden (nine million inhabitants) that represent a national average of the population. The fact that the respondents are part of this register means that they have already agreed to participate in online self-administered questionnaires, for which they receive a minor compensation. The respondent group was limited in terms of age, to 15- to 25-year-olds, because we were mainly interested in participants who had grown up with the Internet, and who used it as a natural part of their daily lives. The questions of anonymity services asked in the study are part in a larger battery of questions regarding social norms, perceived pressure from others to comply with copyright regulation, will to pay for music and movies, etc., that is reported elsewhere (Svensson and Larsson forthcoming; Svensson and Larsson 2009).

The surveys were self-administered questionnaires (SAQ). Wolf (2008) concludes that "research has shown that respondents are more likely to report sensitive or illegal behaviour when they are allowed to use a SAQ format rather than during a personal interview on the phone or in person." Traditionally the SAQ has been distributed by mail or in person to large groups, but now SAQs are being used extensively for web surveys. Because the questionnaire is completed without ongoing feedback from a trained interviewer, special care must be taken in how the questions are worded as well as how the questionnaire is formatted in order to avoid measurement error (Wolf 2008; see also Dillman 2000 on web based surveys).

Survey Data

The data on the general aspects of the responses to the two surveys is presented here. We then compare the relevant data on anonymity between the two surveys—from before and after the implementation of IPRED in Sweden. Additional data comes from the two interviews mentioned above.

Of the 1,047 respondents in the first survey, about 59 percent (619) were female and 41 percent (427) were male. More than 99 percent stated that they had access to a computer with an Internet connection at home. More than 75 percent of the respondents spent at least two hours a day at an Internet-connected computer at home, and about 23 percent more than six hours a day. About 6 percent spent less than an hour a day at a computer with Internet access. Downloading of content in terms of music, movies or

other files that are possibly protected by copyright is evenly spread over the categories. About one-third of the respondents download potentially copyright material more than once a week, and about one-fifth never download this type of content.

Of the 1,047 respondents in the second survey, about 60 percent (624) were female and 40 percent (418) were male. More than 98 percent said that they had access to a computer with an Internet connection at home. With regard to time spent on this computer, more than 70 percent spent at least two hours a day on it (compared to about 75 percent in the first survey), and about 21 percent spent more than six hours daily. The group that downloaded potentially copyrighted material more than once a week (including daily) decreased from one out of three to one out of five.

Comparing the Two Surveys

The mean age for respondents in the first survey was about 20.9 years, while for the second survey it was about 19.9 years. Although the number of answers on the survey was 1,047 both times, the exact number of respondents that answered both the question of file-sharing frequency and the question on use of online anonymity services was a little bit lower. That is why the total number in Table 1 is lower than 1047. Note that the groups of file-sharing frequency (Table 1) have been clustered in different ways in order for us to significantly shed light on the fluctuations in OAS usage before and after IPRED.

http://www.psocommons.org/policyandinternet/vol2/iss4/art4
DOI: 10.2202/1944-2866.1044

Table 1. Usage of Online Anonymity Service in Relation to File-sharing Frequency

File-sharing frequency	Usage of OAS, before IPRED (%)	Usage of OAS, after IPRED (%)	Actual increase/decrease (% points)	Possible margin error (% points)*	Statistically significant or not
1. Never file share	2.8 (of 217)	5.5 (of 384)	+2.7	+/– 3.17	No
2. Never file share + Once a month at the most	4.8 (of 459)	5.6 (of 638)	+0.8	+/– 2.65	No
3. Never file share + Once a month at the most + Once a week at the most	6.5 (of 681)	7.2 (of 797)	+0,7	+/– 2.58	No
4. File share daily	20.6 (of 107)	28.6 (of 63)	+8.0	+/– 13.5	No
5. Daily + More than once a week	13.2 (of 325)	23.0 (of 187)	+9.8	+/– 7.07	Yes
6. Daily + more than once a week + once a week at the most	11.9 (of 547)	18.5 (of 346)	+6.6	+/– 4.91	Yes
All	8.6 (of 1,006)	10.2 (of 984)	+1.6	+/– 2.56	No

* Given a confidence interval of 95 percent.

The main findings displayed in the table is the connection between unauthorised file sharing and OAS usage in relation to the IPRED implementation. For group 5, for instance, the share of OAS use is almost doubled after the introduction of IPRED. For group 6, the share of OAS usage increase is about as large. It is of course possible that the increase for

the ones that file-share daily would also have been statistically significant, had the selected population been bigger in the survey. However, as the numbers in brackets indicate, the file-sharing frequency was reducing quite heavily post-IPRED (compare the decrease before/after IPRED in groups 4–6 with the increase in groups 1–3). One can note that the increase in OAS share is pretty remarkable in group 1—the ones who do not file share at all—however, this is still not statistically significant.

Since the respondents received the questionnaire by email, one could ask to what extent the survey respondents tend to be more computer literate than the population as a whole. While this is a fair question, it is more relevant for populations where there is a significant divide between groups with low computer literacy and those with high. In Sweden, however, as shown by the 2008 WII report on Internet use, 94 percent of the Swedish individuals between 16 and 25 use Internet at home (WII 2008, 14). In 2010 the Internet usage among 16- to 25-year-olds is 99 percent for "sometimes" and 92 percent for "daily use" (WII 2010, 10). Although our survey excludes a group of people by being an emailed online survey, this group is likely very small.

Additional Data—OAS Statistics and Search Trends

The companies that run the online anonymity services are reluctant to share their statistics on subscriber fluctuations—quite understandably, they do not want to give away any information on this competitive market. An interview with a representative for one of the Swedish operators of an anonymity service revealed that the effect of the IPRED implementation was instantaneous. The increase in subscribers to the OAS was "more than double, almost a triple."[12] This was later corroborated with subscriber statistics from the company stating that the increase of subscribers during the short span from March 15 (two weeks before the implementation of IPRED) to May 1, one month after, was 298 percent. However, as the OAS representative commented, immediately after April 2009 "the increase levelled off a bit, likely due to overload in our systems. We were unprepared for the increase in demand. I believe the increase in sales could have been at least five times if we had been prepared. Many potential customers probably gave up on anonymisation, others went to alternative suppliers." This tells of an immediate increase around the time IPRED was implemented. The intense media attention received by the implementation likely played an important role in people becoming conscious of this type of service.

[12] Interview with the authors, May 2010.

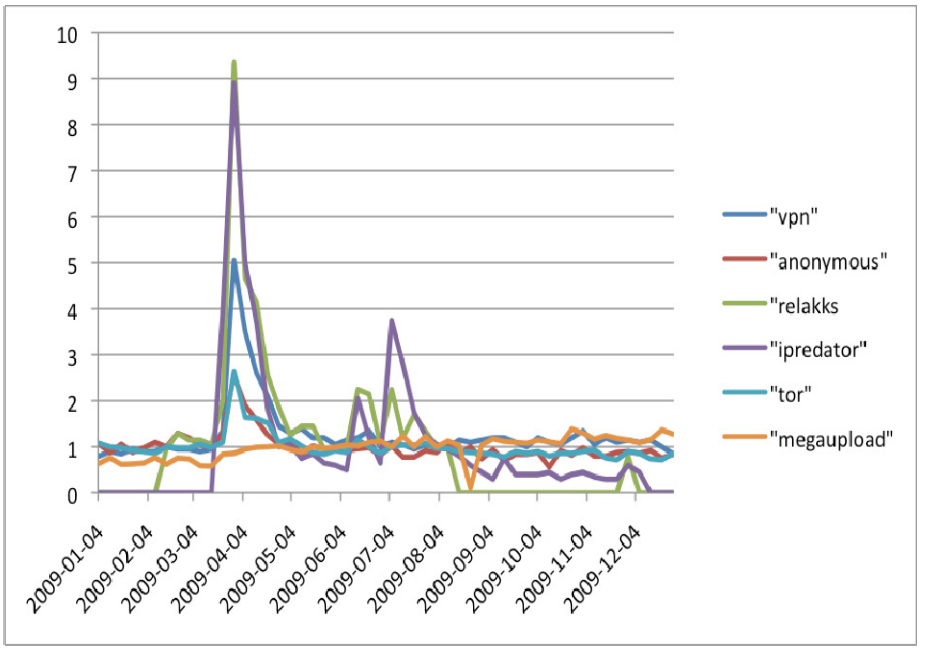
The marked, but perhaps short-lived, public interest in online anonymity around the time of IPRED's implementation can further be corroborated by search engine statistics from Google Trends (Figure 1).[13] Google Trends search engine statistics for Sweden from 2009 show that searches on words like "anonymous," "vpn," "relakks," "ipredator," and even "hide" show a remarkable peak exactly around the time that IPRED was implemented in Sweden. This goes also for "tor," which likely is aimed for the darknet routing system, but not for "MegaUpload." OASs other than ipredator and relakks, such as mullvad, ivacy, and dold.se, as well as a number of other related search terms, do not have enough search volume to show reliable statistics.

The most significant peaks are found for "relakks," "ipredator," and "vpn"; "relakks" being almost 10 times as high as the normal frequency, "ipredator" a little over eight times, and "vpn" about four times as high. The peaks last for a little more than a month, starting in mid-March and level off in the last week of April.

The one-click host "Sprend" is a relatively small service, with about 95 percent of its users based in Sweden. This is why its user statistics, following the argument in this article, could be relevant for the question of responses to the implementation of IPRED in Sweden. From the interview with the representative of Sprend, the increase of users from May 2009 to May 2009 was about 100 percent, from around 30,000 users to 60,000 (data from Google Analytics). The representative claimed that there had been a big increase in their users uploading and sending data in .zip and .rar file formats, rather than as .mp3, which is a sign of a trend regarding this service towards more efficient sharing of bigger amounts of data—copyright protected or not.

[13] For example, Google Flu Trends has proven to be a useful tool for tracking influenza outbursts, following from the quite simple fact that we tend to perform Google searches on topics that are of concern to us (Carneiro and Mylonakis 2009; Ginsberg et al. 2009).

Figure 1. Fluctuations in Searches on Google during 2009 from within Sweden for a Selection of Words Relating to Online Anonymity[14]



Analysis

Although the increase of OAS use over the whole Swedish population is not significant, the increase of the share in some groups related to file-sharing frequency definitely is. Groups 4 and 5 in Table 1 show that unauthorized file sharing of copyrighted content is at least one reason for seeking stronger anonymity online. The increase from before to after the IPRED implementation was significant for these relatively high-frequency file sharers. There are other circumstances that support an increase in enhanced anonymity as a result of IPRED. As mentioned, a representative from one of

[14] The standard deviation is 10 percent, and the geographical data is based on IP address information. The data is scaled to the average search traffic for the selected search term (represented as 1.0) during the time period selected (2009). Hence, the numbers are not absolute search traffic numbers. The scaling is relative to the time period chosen (and not fixed to January 2004, as is also offered by the Google Trends). See more: http://www.google.com/intl/en/trends/about.html#7.

the Swedish OAS revealed that the effect of the IPRED implementation on subscriber numers had been instantaneous.[15] This sense of an effect was also supported by Google statistics for various Internet search terms associated with anonymity, searched for by Swedish users in 2009. The OCH service approached by the authors, Sprend (a large majority of whose users are Swedish), did not report this explicit pattern of immediate interest when the law was implemented, but they did report a constant increase over the year of 2009, doubling its users from May 2008 to May 2009. While this could be connected to unauthorized sharing of copyrighted content, there is no way of corroborating such a claim at this time, and it cannot reliably be connected to IPRED.

One can of course speculate on the motives for wanting to be anonymous online. Is it just to share files without the risk of getting caught, or are there other reasons as well? One could hypothesize around, for instance, a desire to hide other types of crime (in any organized form), or perhaps to protect oneself from being exposed to criminal acts or integrity breaches, for instance from the Firefox plugin Firesheep, that spread rapidly globally in October 2010 and was used to obtain access to people's accounts on Facebook, Twitter, and other services, over open wireless networks. There are idealists that see too strong and sweeping surveillance trends in law making in terms of data retention directives, IPRED, and signals surveillance, such as the FRA law in Sweden (Kullenberg 2009). There are likely several motives—as there are many completely legitimate and never questioned uses for encrypted communications, such as in Internet banking, password protection, or when I use the VPN service of my university to log on to its server, etc. This all ties on to the double-edged sword of encrypted anonymity: it can be used to do good and bad. It can stop governments from preventing malicious acts being done by individuals, and it can help individuals from preventing malicious acts being done by governments. The fact that we increasingly lead our lives connected to the Internet makes the traceability of our traces a sensitive and important question for new legislation in terms of privacy. Law directs power, such as who has the right to get access to identity information connected to IP addresses. IPRED puts the finger on this sensitive balance between intellectual property rights and individuals privacy. If this legally directed power is not perceived as

[15] The interest in how to be more anonymous in Sweden at the time can further be described by the fact that when the anonymity service Ipredator was first released as a work in progress in April 2009, more than 170,000 people indicated their interest in subscribing. Its not likely that all of them signed up for the following pay service, but it is still indicative of the general consciousness of these matters and the strong interest in a more active online anonymity, brought about by the implementation of IPRED.

legitimate, encryption technology is always there as a means to diminish that power. Some support can be found in our empirical data for the fact that the levels of OAS use have also increased for non-file sharers in relation to the implementation of IPRED; however, the numbers are too low to validate this hypothesis in a satisfactory manner (Table 1, group 1).

Anonymity—albeit in the somewhat traceable and weak "pseudonymous" form—can be understood as part of the status quo of online behavior; that is, users generally trust that their online activities will not easily reveal their offline identities. There are two exceptions to this trust, of which one is a voluntary release of information (such as revealing birth name, age, and pictures in social networks). The other exception is more intricate, and is tied to social norms in another way. If de-anonymization is forced by law, this will only seem just and legitimate if this law is in compliance with the structures of social norms: if it does comply, then online "trust" in anonymity will not suffer from this breakage of confidentiality, since most people will experience the breakage as just. However, if the law is not in line with social norms, this de-anonymization will likely have a negative effect on the status quo of the weaker forms of anonymity. This "trust" is adversely affected, resulting in counter-measures designed to strengthen the lost anonymity, all in line with the social norms that have been affected by the implemented law. This might lead to an escalation on both sides of what can clearly now be described as a conflict. In terms of the broader spread of online anonymity, a cold war has begun.

Linking back to the discussion earlier in this paper, it is striking that the use of anonymity services really is a latent dysfunction and not just a latent non-function; in truth, it opposes the intended enforcement of copyright legislation by helping file sharers to avoid being caught when violating copyright. In this article we mention various other ways of achieving online anonymity besides using an IP VPN encryption service: given that the legal initiatives do not overlap well with the social norms of the online community, it is likely that the use of several of these methods for achieving anonymity will increase. In fact, they are likely to have already increased in Sweden following the implementation of IPRED, although our study was not designed to identify the levels of these other types of techniques for anonymity. We have focused on the dysfunctions of IPRED implementation, and concluded the increased anonymity to be a latent effect.

Conclusion

This study shows that unauthorized file sharing of copyrighted content is at least one reason for seeking stronger anonymity online. The increase from before to after the IPRED implementation was significant for high-frequency file sharers. These results must however be seen in a grander perspective of law in relation to social norms. Online anonymity is not only about a few services being offered for an obscure and small group in the corners of society; it is often perceived as part of the "normality" of Internet behavior. There is a dilemma here regarding the striking of a balance between law enforcement and public trust in the system: governments need to choose their battles carefully, for fighting socially accepted behavior may actually hinder the fight against socially non-accepted behavior. This dilemma has been described in general terms as that "governments are increasingly nervous of anonymous/pseudonymous traffic on the Internet and conversely users are increasingly nervous of governments using their powers to intercept and force identification of those who attempt to hide behind a cloak of anonymity for good or bad reason" (Rowland 2009, 310).

Given the generativity of the Internet, any legally enforced forced identification that breaks this veil of anonymity will have to be well founded in social norms regarding the legitimacy of the actual law, if it is not to disrupt this "trust." If not, such initiatives are likely to spur counter-measures involving the diffusion of knowledge of how to strengthen online anonymity; as well as the counter-measures of smaller elites of pro-privacy activists. The levels of the different anonymity techniques, encrypted as well as other, are a sign that describes a part of the character of online behaviour, and hence the character of the Internet.

An anticipated conclusion that requires further assessment is that the file-sharing patterns are changing in terms of visibility. It is likely that a core of sharers are developing, who are more inclined to pay for anonymity services due to their anticipated need for advanced protection from being caught violating copyright laws. Our data supports this to some extent. Antoniades et al.'s (2009) study also supports this conclusion in the case of OCHs, finding that in OCH services, "much like in p2p file-sharing systems a very small number of users upload most files, which are often copyrighted content, favouring audio albums, video movies, and applications" (2009, 234). It is however also likely that a more loosely formed group of sharers will develop, who are connected to the core shares, but who are not centrally located in the sharing process. They are using other means for sharing, such as "secret" groups and trusted networks, sneakernets, and One Click hosting services.

Given the multitude of ways in which pseudonymity can be strengthened, especially bearing in mind the weak support of the legal norms among the social norms in this case, a criminalization of the operation of anonymity services would be an especially ill-suited attempt to solve so-called "piracy-issues."[16] Not only would such an initiative likely fail to reduce anonymous sharing of files, it would further stimulate the diffusion of knowledge of encryption and other techniques for anonymity. A consequence of an increase in online anonymity, not solely for copyright violations but for law enforcement as a whole, is (as mentioned before) that any criminal investigation that tracks illegal behavior on the Internet will be set back by an increase in encrypted traffic. On the basis of this study, one can conclude that the fight against copyright violations has increased the use of encryption technologies, which will likely have a detrimental effect on police investigations regarding other crimes as well. This follows the argument made by Lessig in Code v2 (2006) that there are choices to be made about how the character of the Internet evolves, and that these choices will affect fundamentally what values are built into the network; expressed by Zittrain in terms of the risk of going from the "generative" Internet towards an "appliancised" network (Zittrain 2008). However, given the generativity of the technology—think for instance of the multiple ways for enhancing anonymity outlined above—this choice is not simply made by any content rights holder or legal enforcement without counteractions. One point here is that the attempted enforcement of legislation that has a weak representation among social norms will affect the enforcement of legislation that has a strong representation among social norms. IPRED must be seen in the light of how copyright regulation has legitimacy issues in the digitized society. Enhanced surveillance and detection methods that connects to this regulation—with EU initiatives such as the data retention Directive, possibly the Telecom reforms package, and ACTA, and with national laws like the French HADOPI and the UK Digital Economy Act—will likely not only polarize law from social norms in this area, but also lead to the diffusion of more and stronger online anonymity.

[16] With the term "piracy" being a metaphoric term with political content, and also (for many reasons) misleading connotations (see Larsson and Hydén 2011).

References

Agarwal, N. 2010. "Evaluating IPRED2: The Wrong Answer to Counterfeiting and Piracy." *Wisconsin International Law Journal* 27: 790.

Andersson, J. 2010a. "Det Dumma Nätet." In *Efter The Pirate Bay*, eds. Andersson and Snickars. Mediehistorisk Arkiv, Stockholm: Kungliga Biblioteket.

Andersson, J. 2010b. "Peer-to-Peer-Based File-Sharing Beyond the Dichotomy of 'Downloading is Theft' vs. 'Information Wants to be Free': How Swedish File-sharers Motivate their Action." Goldsmiths, University of London, for the degree of PhD in Media and Communications.

Antoniades, D., E.P. Markatos, and C. Dovrolis. 2009. "One-Click Hosting Services: A File-Sharing Hideout." *Internet Measurement Conference, Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement*, Chicago.

Appelstrand, M. 2007. *Miljömålet i skogsbruket – styrning och frivillighet*, Lund studies in Sociology of Law 26, Lund University.

Aubert, Vilhelm. 1954. *Om straffens sosiale funksjon*, Oslo: Akad. forl.

Baier, M. 2003. *Norms and Legal Rules. An Investigation of the Tunnel Construction through the Hallandsås Ridge*. Department of Sociology, Lund University.

Bergman, A.-K. 2009. "Law in Progress? A Contextual Study of Norm-Generating Processes – The Example of GMES." Lund Studies in Sociology of Law No. 30, Lund University.

Bergman, M.K. 2001. "The Deep Web. Surfacing Hidden Value." *The Journal of Electronic Publishing* **7** (1).

Brown, B.J. 1992. "Latent Effects of Law: The Defamation Experience." *Singapore Journal of Legal Studies* 315–346 (Dec).

Carneiro, H.A. and E. Mylonakis. 2009. "Google Trends: A Web-Based Tool for Real-Time Surveillance of Disease Outbreaks." *Clinical Infectious Diseases* 49: 1557–1564.

Case ÖÄ 6091-09, October 13, 2009, Court of Appeal. Five publishing houses seeking identity information from an ISP.

Case Ä 2707-09, June 25, 2009, District Court. Five publishing houses seeking identity information from an ISP.

Christie, N. 1965. *Kriminalsosiologi*. Oslo: Universitetsforl.

Dillman, D.A. 2000. *Mail and Internet Surveys: The Tailored Design Method*. 2nd edn. New York: Wiley.

Directive 2002/58/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights.

Du Pont, G.F. 2001. "The Criminalization of True Anonymity in Cyberspace." *Michigan Telecommunications and Technology Law Review* 7: 191.

Edman, M., and B. Yener. 2009. "On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems." *ACM Computing Surveys* 42 (1): 1–35.

El Pais, ELPAÍS.com—Madrid—February 18, 2009, *Los demandantes del juicio contra The Pirate Bay retiran la mitad de los cargos. El sitio de intercambio de archivos es acusado de distribuir material con derechos de autor.* http://www.elpais.com/articulo/internet/demandantes/juicio/The/Pirate/Bay/retiran/mitad/cargos/elpeputec/20090218elpepunet_3/Tes?print=1 (accessed November 29, 2010).

Froomkin, A.M. 2008. "Anonymity and the Law in the United States." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society,* ed. I. Kerr. New York: Oxford University Press, 2009; University of Miami Legal Studies Research Paper No. 2008-42. Available at SSRN: http://ssrn.com/abstract=1309225

Ginsberg, J., M.H. Mohebbi, R.S. Patel, L. Brammer, M.S. Smolinski, and L. Brilliant. 2009. "Detecting Influenza Epidemics Using Search Engine Query Data." *Nature* 457: 1012-1014.

Gustafsson, J. 2009. *Nätoperatörer kringgår inte IPRED*, Svenska Dagbladet, April 28, 2009. http://www.svd.se/nyheter/inrikes/artikel_2805959.svd (accessed November 29, 2010).

House, R.J. 1968. "Leadership Training: Some Dysfunctional Consequences." *Administrative Science Quarterly* 12 (4): 556–571.

Hydén, H. 2002. *Normvetenskap*, Lund Studies in Sociology of Law. Lund: Lund University.

Hydén, H., and M. Svensson. 2008. "The Concept of Norms in Sociology of Law." In *Scandinavian Studies in Law*, ed. P. Wahlgren. Law and Society. Stockholm: Stockholm Institute for Scandinavian Law.

Kaminsky, M. 2009. "The Origins and Potential Impact of the Anti-Counterfeiting Trade Agreement (ACTA)." *Yale Journal of International Law* 34: 247.

Kao, A. 2004 "RIAA v. VERIZON: Applying the Subpoena Provision of the DMCA." *Berkeley Technology Law Journal* 19: 405.

Kullenberg, C. 2009. "The Social Impact of IT: Surveillance and Resistance in Present-Day Conflicts How can Activists and Engineers Work Together?" *FlfF-Kommunikation* 1: 37–40.

Larsson, S. 2008. "Non-legal Aspects of Legally Controlled Decision-Making – The Failure of Predictability in Governing the 3G Infrastructure Development in Sweden." In *Contributions in Sociology of Law. Remarks from a Swedish horizon*, eds. H. Hydén, and P. Wickenberg. Lund Studies in Sociology of Law. Lund: Lund University.

Larsson, S. 2009. "Law as a Gate Keeper for Participation. The Case of 3G Infrastructure Development in Sweden." In *Participative Aspects on Law – A Socio-Legal Perspective*, ed. M. Baier. Lund Studies in Sociology of Law. Lund: Lund University

Larsson, S. 2011. "The Path Dependence of European Copyright." *SCRIPTed*. Edinburgh: School of Law, University of Edinburgh.

Larsson, S., and H. Hydén. 2011. "Law, Deviation and Paradigmatic Change: Copyright and its Metaphors." In *Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives*, eds. Garcia-Ruiz et al. IGI Global. Forthcoming.

Lasica, J.D. 2005. *Darknet: Hollywood's War Against the Digital Generation*. Hoboken, NJ: John Wiley & Sons, Inc.

Leiner, B.M. et al. 2009. "A Brief History of the Internet." ACM SIGCOMM *Computer Communication Review* 39(5): 22-31.

Lessig, L. 2006. *Code Version 2.0*. New York: Basic Books Cop.

Levy, S. 2001. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. New york: Viking Press.

Los Angeles Times. 2009. "Editorial, The Pirate Bay ruling. A Swedish court rules against a website notorious for bootlegged content. But the war rages on." April 18, 2009. http://www.latimes.com/news/opinion/editorials/la-ed-pirate18-2009apr18,0,3705805.story (accessed November 29, 2010).<CE: Please check citations>

Mathiesen, T. 2005. *Rätten i samhället: En introduktion till rättssociologin*, [Original title: *Retten i samfunnet*]. Lund: Studentlitteratur.

McAulay, L. 2007. "Unintended Consequences of Computer-Mediated Communications." *Behaviour and Information Technology* 26 (5): 385–398.

Merton, R.K. 1936. "The Unanticipated Consequences of Purposive Social Action." *American Sociological Review* 1: 894–904.

Merton, R.K. 1949. *Social Theory and Social Structure: Toward the Codification of Theory and Research*. Glencoe, IL: The Free Press.

Merton, R.K. 1976. *Sociological Ambivalence and Other Essays*. New York: The Free Press.

Morio and Buchholtz. 2009. "How Anonymous are you Online? Examining Online Social Behaviors from a Cross-Cultural Perspective." *AI and Society* 23: 297–307.

Pew Research Center. 2010. *The Future of the Internet IV*.

Prop. 2008/09:67 *Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG*.

Rao, J.R., and P. Rohatgi. 2000. "Can pseudonymity really garantee privacy?" *Proceedings of the 9th USENIX Security Symposium*, Denver.

Ridgway, V.F. 1956. "Dysfunctional Consequences of Performance Measurements." *Administrative Science Quarterly* 1 (2): 240–247.

Ritzer, G., and D.J. Goodman. 2003. *Sociological Theory*. 6th edn. Boston: McGraw-Hill.

Roots, R.I. 2004. "When Laws Backfire. Unintended Consequences of Public Policy." *American Behavioural Scientist* 47 (11): 1376–1394.

Rosenzweig, P. 2005. "Privacy and Consequences: Legal And Policy Structures For Implementing New Counter-Terrorism Technologies And Protecting Civil Liberty." Available at SSRN: http://ssrn.com/abstract=766484.

Rowland, D. 2009. "Privacy, Freedom of Expression and cyberSLAPPs: Fostering Anonymity on the Internet?" *International Review of Law, Computers & Technology* 17 (3): 303–312.

Sunstein, C.R. 1994. "Political Equality and Unintended Consequences." *Columbia Law Review* 94 (4): 1390–1414.

Svensson, M. 2008. *Social Norms and the Observance of Law, [In Swedish. Sociala normer och regelefterlevnad. Trafiksäkerhetsfrågor ur ett rättssociologiskt perspektiv*]. Lund Studies in Sociology of Law. Lund: Lund University.

Svensson, M., and S. Larsson. 2009. "Social Norms and Intellectual Property. Online norms and the European legal development." Research Report in Sociology of Law. Lund University.

Svensson, M., and S. Larsson. forthcoming. Intellectual Property Law Compliance in Europe: Illegal File sharing and the Role of Social Norms.

The Swedish Act on Copyright in Literary and Artistic Works – Act 1960:729, of December 30, 1960. Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk.

The Telegraph. 2009. "What does The Pirate Bay Ruling Mean for the Web?" by Claudine Beaumont, April 17, 2009. http://www.telegraph.co.uk/technology/news/5170684/What-does-The-Pirate-Bay-ruling-mean-for-the-web.html (accessed November 29, 2010).

Vago, S. 2009. *Law and Society*. Upper Saddle River, NJ: Pearson Prentice Hall, Cop.

Vincents, O.B. 2007. "When Rights Clash Online: The Tracking of p2p Copyright Infringements vs. the EC Personal Data Directive." *International Journal of Law and Information Technology* 16(3): 270-296.

Wolf, James (2008) Self-Administered Questionnaire, *Encyclopedia of Survey Research Methods*, SAGE Publications. [Last visited 10 December, 2010]. http://www.sage-ereference.com/survey/Article_n522.html.

World Internet Institute. 2008. *Svenskarna och Internet 2008*. Hudiksvall.

World Internet Institute. 2010. *Svenskarna och Internet 2010*. Hudiksvall.

Zittrain, J. 2008. *The Future of the Internet. And How to Stop It*. New Haven and London: Yale University Press.