COMPLIANCE OR OBSCURITY?

Online anonymity as a consequence of fighting illegal file sharing

Stefan Larsson[1] and Måns Svensson[2]

This is a work in progress, do not cite.

Abstract

Online anonymity in a weaker, ”pseudonymous” form, is in many ways the ”normality” of internet behaviour. Any legally enforced identification that breaks this veil of anonymity will have to be well founded in social norms regarding the legitimacy of the actual law not to disrupt this status quo. If not, such initiatives are likely to spur counter-measures en masse related to the diffusion of knowledge of how to strengthen the anonymity online, as well as counter-measures of smaller elites of pro-privacy activists, contributing to an ”obscurer” Internet. Our results indicate an increase of stronger and less traceable online anonymity as one of the consequences of legally enforced de-anonymisation not supported by social norms.

The Mertonian concepts “manifest functions” and “latent dysfunctions” is in the article used to analyse the consequences of recent legislative efforts to stop illegal file sharing. The European Union directive on Intellectual Property Rights Enforcement (Ipred) was implemented in Sweden on April 1st, 2009, and is meant to be the enforcement needed to achieve increased compliance with online copyright legislation. This, therefore, is the manifest function of the directive. An increase in active use of anonymity services, as a result of the implementation, is

1 LLM, MaSoS, Licentiate of Technology, PhD candidate in Sociology of Law, Lund University, Sweden, Stefan.Larsson@soclaw.lu.se

2 PhD in Sociology of Law at Lund University, Sweden. Mans.Svensson@soclaw.lu.se

a latent dysfunction, since it is not intended and it is ”self-defeating” in relation to the purpose of the implementation.

The article focuses on and empirically studies the changes in levels of use of anonymity services (IP VPN encryption services) as a result of Ipred's implementation, and discusses other possible latent dysfunctions. The data is from 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. The actual increase in the use of anonymity services is between 15 and 20 per cent. Those who share files on a daily basis use anonymity services twice as frequently as the average respondent in the first study, and almost three times as frequently in the second study.

Keywords: Anonymity, pseudonymity, anonymisation, manifest and latent, functions and dysfunctions, illegal file sharing, Ipred, copyright enforcement, IPR Enforcement Directive, encryption, vpn tunnel, sociology of law.

Introducing the legal and political background on online anonymity in Sweden

The spread of encryption enabling online anonymity has been put forward both as a tool for privacy, ensuring free speech and avoiding harassment of political dissidents in repressive states, as well as something that will impede criminal investigations (Lessig 2006, pp. 45-60, Rowland 2009). It is clear that this double-edged sword, working for de-identifying whoever master it serves, has an impact on both the character of the Internet as well as the character of law enforcement.

When Bob Kahn and Vince Cerf began working on what became the underlying protocol for Internet, TCP/IP, in 1973, they did it under Kahn's previously formulated ambitions of which one was that there should be no global control at the operations level. The simplicity and openness of the underlying structure created it 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 has 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 by the Internet Service Providers, the ISP's, which keep track of their subscribers mainly for billing purposes. This is the reason for that whenever anyone wants to find out the identity behind the actions committed ”by an IP-number”, for instance a violation of copyright, it is the door of the ISP's they come knocking on. 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 that broadens the identifying aspects off their ”offline identity”, or unwillingly, for instance when forced in a criminal investigation.

In Sweden, 2009 was the year that ”online anonymity” became a valid phrase in everybody's mind. It was the year when at least two new operators of services that provide anonymity as a subscription was started, and the already established ones saw a sudden increase in subscribers. One of the stronger contributors seems to have been the implementation of the ”Copyright Enforcement law”, called ”the Ipred-law” from its initiator, the European Directive on Intellectual Property Enforcement.[3] This article identifies the unintended effects of the implementation of the IPR Enforcement Directive in Sweden in terms of an increase in online anonymity, and it places 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

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

functions, as well as dysfunctions. By using the terminology of Robert K. Merton, the article focuses and empirically studies the changes in levels of anonymity as a result of the implementation of Ipred, and discusses other possible latent dysfunctions.

Unintended consequences of law

Vago (2009) describes several general types of dysfunctions of law that may ”may evolve into serious operational difficulties if they are not seriously considered” (Vago 2009, p. 22). This is also a main motivation for this study: if enforcement of copyright law ”stimulates” a more anonymous Internet, this will lead to an ”operational difficulty” for all law enforcement of computer mediated behaviour taking place online. A type of legal dysfunction, of the ones Vago suggests, that is the most fitting here is one stemming from the conservative mark that bears all law in the interest of predictability and continuity (Vago 2009, p. 22). In this case, copyright is the conservative legal construction that bears elements that do not fit with emerging social norms of sharing content and cultural expressions in a digitalising era of networks (Boyle 2008, Jensen 2004, Larsson 2010, Lessig 2008, Litman 2006, Svensson & Larsson 2009, Vaidhyanathan 2001, Weinstock Netanel 2008). The social changes are connected to technological development, which has ”moved” the behaviour into an interconnected milieu, which has brought a ”networking society, the interconnecting of people, processes, applications, work tasks and leisure pursuits, [which] has lead to a globalised society, a ‘one-world’ context where causes and effects can reverberate throughout the entire system”, in the words of Robert Hassan (2008). This interconnectedness also describes the importance of seeing online trends regarding the levels of anonymity as part of the very character of Internet. There are no lonely, cut-off areas of this milieu. The trends connected to human norms of conduct all have the potential to ”reverberate throughout the system”. The case of online anonymity and copyright enforcement in Sweden can tell what will what will come to other parts of the world as well.

The dysfunctions of a law can be described by the ”bad” consequences, which Cass R. Sunstein (1994, p. 1390) describes in terms of ”self-defeating”, meaning measures that actually makes things worse from the standpoint of their strongest and most public-spirited advocates. Sunstein points out what we hold for being one of the key problems of empirical limitations in a dogmatically incapsulated process of law-making, the problem of unintended consequences of legal implementation: what will be the real-world consequences of an implementation? Will it fulfil its intended purpose? Will it have dysfunctions that defeats its own purpose?

The ”dysfunctionality” in the case of this study speaks - in our view - of an increased responsibility for the legislators to think of consequences that will

not only counteract on enforcement of copyright laws (which can be questioned from a legitimacy point of view) but also on enforcement of any law that deals with internet-mediated illegal behaviour. Insensitive law-making can stimulate alternative Internets and the increasingly spread knowledge in encrypted communication (or in other ways less traceable) and therefore contribute to an obscurer Internet rather than behaviour in compliance with law attempting to regulate online conduct.

Anonymity and pseudonymity

There is a difference between (traceable) pseudonymity and true anonymity. In these terms, anonymity is the outer end of the scale of pseudonymity. Pseudonymity is the traceable version of anonymity, although it often might be perceived as truly anonymous by the individuals performing a task online (Du Pont 2001, Rao & Rohatgi 2000). The problem with pseudonymity, from a privacy point of view, is that it can be compromised by those with the appropriate technical skills, and the problem with true anonymity, from a governmental point of view, is that it can not lead to the offline identity of someone performing an (criminal or not) act online. The dilemma has been described 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, p. 310).

We will in this article use the term ”anonymity” in a broad sense, which can include ”true” untraceable anonymity, but mostly will regard the pseudonymous state of ”anonymity”. To keep clarity, we will speak of activities as more or less anonymous, and will see anonymity as a sort of scale rather than one, true, anonymous state.

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 Intellectual Property Rights Enforcement Directive (Ipred), which was implemented in Sweden on April 1st, 2009. Ipred has generated significant debate and protests in the media, the blogosphere and political arenas.

Ipred is an exception to the otherwise ruling legal principle of online anonymity, often expressed in terms of privacy.[4] The implementation of Ipred in

[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.

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. If the court finds that illegal file sharing has taken place, 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.

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 17th, 2009, which added to public interest in copyright and file sharing issues in Sweden and abroad.[5] This was not just an example of the fact that Hollywood stars rarely visit this sparsely populated country (although their lawyers do)—it also showed that Sweden is interesting as a case when it comes to social norms shaped by online preconditions, especially in relation to legal constructions such as copyright law.

The hunt for illegal file sharers 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 to then, quite naturally, seek to tie the identity of violators to IP numbers, giving the ISP a central role in the battle (see, for instance, Vincents, 2007 on copyright holder strategies). This puts into focus the retention of log data, which will be expanded by the ongoing implementation of the data retention directive in EU, even though the impetus for this directive was to battle terrorism and "serious crime".[6] The role of ISPs, as well as the issue of whether or not copyright violators should be blocked from Internet access, has been highlighted by the so-called HADOPI law in France, legislative actions in Britain, as well as in the EU Telecoms Reforms Package.[7]

---

5 Some examples of international magazines that reported from the trial include Spain's leading daily El Pais, ABC News, the Los Angeles Times, and The Telegraph. See the reference list for details.

6 DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of March 15th, 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.

7 HADOPI is the nickname for a French law officially entitled *Loi favorisant la diffusion et la protection de la création sur Internet,* which translates into the *law favouring the diffusion and protection of creation on the Internet*, regulating and controlling 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 European Telecoms Reform Package was presented to the European Parliament in Strasbourg on November 13th, 2007 but first voted upon on May 6th, 2009. This is a cluster of directives

This study should be viewed in this context. The relevance of such research expands beyond the Ipred directive, as Ipred is part of a larger legislative trend that places increased focus on identity/anonymity/privacy issues in connection to the Internet, and the seemingly low legitimacy the regulation has had. In the months after the implementation of Ipred in Sweden, the media reported that interest in anonymity services rose strongly, and ISPs 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 keep track of the anticipated court cases that followed from implementation, and petitions started in opposition to the law. Moreover, the youth sections of the 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.

Research context

There are surveys connected to encryption technologies and law. Antoniades et al (2009) compares p2p based file-sharing to file-sharing via One-Click hosting (OCH) services such as RapidShare, and conclude that OCH's have a number of features that can compete with BitTorrent as the leading file-sharing platform. 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 states that "law imposes few if any legal obstacles to the domestic use of privacy-enhancing technology such as encryption". Rosenzweig (2005) assess privacy issues of fighting terrorism via technologies including encryption and data-mining.

Although there seems to be no earlier studies conducted regarding copyright enforcement and resulting fluctuations in online anonymity there are naturally a wide variety of studies on unintended consequences of law, some of which described in terms of being "dysfunctions" (see Vago 2009, pp. 22-23). In

---

that are being prepared (COM (2007) 697): proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services.

The UK government introduced the Digital Economy Bill on November 20th, 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 20th, 2009, "A world class digital economy for Britain", 155/09). The bill was a result of more than one 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.

fact, the discipline Sociology of Law, has been described as a discipline generally dealing with studying consequences of law from a social scientific perspective, in order to state and study the flaws of the legal application (for instance by Svensson 2008, p. 72). This perspective often focus the difference between law in books and law in action, using empirical data regarding the second in order to criticise the first.[8]

This study is part of a bigger survey conducted at two different times, encompassing about 1,000 people 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 would increase the possibility of being caught illegally sharing files. The first survey was conducted two months *prior* to the implementation of Ipred, and the second one seven months *after*wards—affording the opportunity to study the consequences of implementation. The question of anonymity to be an important indicator of socio-legal research interest in the 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.

Research purpose

This article identifies unintended effects of implementing Ipred in Sweden. There are several probable effects of implementation, including manifest and latent functions as well as dysfunctions. The article focuses on and empirically studies the changes in levels of anonymity as a result of implementation, and discusses other possible latent dysfunctions using the terminology of Robert K. Merton.

This means that there are two key research questions. Firstly, what are the *latent functions and dysfunctions* of the implementation of Ipred in Sweden, and secondly, how do these relate to a broader context of online anonymity and legal enforcement as something revealing at least part of the character of Internet and in what direction predictions can be made?

When analysing the unintended "bad" consequences of a law's implementation its manifest and intended functions have to be touched upon. We have written about the actual manifest functions of the implementation of Ipred

[8] 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 the policy research that sociology of law studies deal with.

elsewhere (Svensson and Larsson, forthcoming). This question ties into the changes in social norms as well as behaviour regarding file sharing as a result of the implementation of Ipred, and therefore requires a more thorough examination, a well-outlined method for measuring social norms, and a theory for handling them. This can be found in a report based on the first survey, performed in January and February 2009, and is also the basis for a comparison between social norms in the field of copyright and the European legislative trend in the field (Svensson and Larsson 2009). It shows a gap that is also of relevance to the understanding of online anonymity.[9]

Analysing law: manifest functions and latent dysfunctions

Ever since Merton formulated the ”unanticipated consequences of purposive social action” in 1936, this terminology has been used in a multitude of areas. McAulay (2007) studies the ”unintended consequences” of computer-mediated communication and thereby focus what has not on beforehand been perceived as an outcome of a communication tool or programming software. This study uses five reasons leading to unintended consequences, developed by Merton (1976). It focuses the period before the introduction of a novel digital communication tool to explain its unintended consequences, but does not categorise the consequences in terms of the relation to the original purpose of the action, like the terms ”dysfunctional” and ”functional” do.

Studying consequences of legal implementation has spurred some interest using Merton's terminology (see Brown 1992, on the ”defamation experience”; Roots 2004 on ”unintended consequences of public policy”; and the above mentioned Sunstein 1994). Sociology of Law does not reveal a broad explicit use of the terminology, but the concepts of “manifest and latent functions” or “dysfunctions” have been used and debated within sociology and socio-legal studies.

Inspired by Merton, the concepts of latent functions and dysfunctions spread to research in the field of administration and organisation (see for instance House 1968; Ridgway 1956; Wagner 1954). The Norwegian sociologist of law and criminologist Thomas Mathiesen (2005) is one of the scholars in recent years to have adopted and employed these Mertonian concepts in relation to legal entities or punishment within the penal system. The concepts have been used in different directions in sociology, but early sociologists used the biological metaphor for describing and analysing society. An early example of research on latent social functions on punishment is the study undertaken by the Norwegian

[9] This study (Svensson & Larsson 2009) is performed before the implementation of Ipred, and therefore does not tell anything of the actual latent effects of the implementation.

sociologist of law Vilhelm Aubert (Aubert 1954). Later, Nils Christie (among others) also contributed to this discussion (Christie 1965).

The terms "manifest" and "latent" functions are sometimes used as equivalents for, respectively, "intended" and "unintended" consequences of an action such as legislation. Peter L. Berger's *Invitation to Sociology* (1963) describes Merton's approach using examples of the "manifest" function of anti-gambling legislation (which may be to suppress gambling), and its "latent" function (which may inadvertently create an illegal empire for the gambling syndicates). In another example, Christian missions in parts of Africa "manifestly" tried to convert Africans to Christianity, while "latently" helped to destroy the indigenous tribal cultures, and thus providing an important impetus towards rapid social transformation (Berger 1963, p. 41).

This use is a simplification of Merton's theoretical basis, and in this article we utilise more of the Mertonian terminology and speak of both latent functions and latent dysfunctions in our analysis of the implementation of Ipred in Sweden. Merton gave examples of items that could be analysed in this functional way, such as "social roles, institutional patterns, social processes, cultural patterns, culturally patterned emotions, social norms, group organisations, social structure, devices for social control etc." (Merton 1949/1968, p. 104). Ritzer (2007, p. 81) has described Merton as a "societal functionalist".

Merton defined *function* as "those observed consequences, which make for the adoption or adjustment of a given system" (1949/1968, p. 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 has no significant effect on contemporary society (Ritzer and Goodman 2003, pp. 241–249).

Functions, dysfunctions and non-functions can either be intended (*manifest*) or unintended (*latent*). There are latent functions that are unintended but still "make for the adoption or adjustment of the system". The Berger presentation does not acknowledge these unanticipated (and therefore not manifest) consequences that nevertheless function in accordance with the intended purpose of, for instance, a new law. In opposition to this, or at least diverging from these types of consequences, we find latent dysfunctions to be "negative consequences for the structures and systems under consideration", in the sense Sunstein speaks of "self-defeating legislation" (1994). From the perspective of implementing copyright enforcement legislation, unforeseen consequences that

somehow aid illegal file sharing in violation of copyright laws are such a latent dysfunction.

When attempting to analyse the consequences of the introduction of new legislation, for instance, one would ideally be able to compare the "positive" consequences (those in line with the intention of the legislation) and the "negative" consequences (those that are dysfunctional), in order to produce a "summary" of the comparison. The reason for making this comparison would be, for instance, to be able to determine if the implementation of the legislation is working "well enough" or creating too many deviating "negative" consequences. Merton refers to this type of summary as a "*net balance*", which he also states is a hard thing to arrive at given the fact that the issues are complex, based on subjective judgments and dependent on the perspective from which the judgments are made.

We use the Mertonian terminology in a manner that stipulates that all latent functions are unintended consequences but all unintended consequences are not necessarily latent functions. There are more unintended consequences than latent functions. We also regard latent dysfunctions as an unintended or unanticipated function, as well as the non-functions, which reasonably always are latent. The conceptual couple of "manifest dysfunctions" we consider as a contradiction in terms.[10]

Method

We conducted two surveys of about 1,000 persons between 15 and 25 years of age, which included questions on the degree of use of services that make Internet browsing anonymous. The surveys also included questions regarding individuals' expectations about starting to use such anonymity services if new legislation would increase the possibility of being caught illegally sharing files. 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, the surveys give us the opportunity to study some of the consequences of implementation.

[10] If we continue with the example of laws, the fact that new legislation would have manifest functions that would be irrelevant for the purpose of the law or for what the law seeks to regulate (i.e., to have manifest non-functions) would be strange, although not impossible (unless you believe that these "non-functions" were intended (manifestly), in which case these are not "non-functions", but simply "functions", and this law would be an odd one, which laws of course can be). In the case of "manifest dysfunctions", they would mean expected consequences that counter the very purpose of the law. The "manifest dysfunctions" would then have a purpose that seeks to create consequences that counter the purpose being fulfilled. Then, the consequences are not "dysfunctions" but really "functions" (the purpose cannot be countered because the countering would then *be* the purpose). This situation cannot exist.

Further, two interviews have been made, one with a head of one of the leading Swedish pay-services for online anonymity - who requested to remain anonymous - and one with a so called ”one-click hosting” company called Sprend with a strong majority of Swedish users. The operators of anonymity services 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.

About the surveys

The first survey was e-mailed 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 per cent and exceeding our target of 1,000 respondents. For the second survey, 1,477 participants were e-mailed, and once again 1,047 people responded, producing a slightly lower response frequency rate of 70.9 per cent.

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 the CINT panel eXchange register means that they on beforehand have accepted to participate in online self-administered questionnaires and that they receive a minor compensation for the participation.

The respondent group was limited in terms of age, 15 to 25-year-olds, because we were mainly interested in participants who have grown up with the Internet and who use it as a natural part of their daily lives, sometimes referred to as ”digital natives” (see Palfrey & Gasser 2008). In this way, the social norms and behaviours we study will have been influenced to a lesser degree by social structures, which may have arisen independently of the Internet. The national sample spread with regards to residence is positive.

Don Dillman (2000) has stated that the goal of writing a survey question for self-administration is to develop a query that every potential respondent will interpret in the same way, be able to respond to accurately, and be willing to answer. The questions of anonymity services asked in the study takes part in a larger battery of questions that is reported in another article (Svensson and Larsson, forthcoming). One part regards a self-estimation of the surrounding persons expectations on the respondents behaviour when it comes to possible copyright violations by sharing files online. The pressure is strikingly low. There seems to be very low expectations on the individuals of this age group to not file share illegally. These results can be interpreted as making it more likely that the respondents actually do not lie about their file sharing activities, at least not for the reason that it can be illegal, which on its hand is of importance for this article’s specified study on online anonymity.

This is a type of self-administered questionnaire (SAQ). Wolf 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 SAQ 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 (see Wolf 2008).

Socio-legal prerequisites: online anonymity and the law

The use of the term “anonymous” can be confusing from an online perspective. In fact, it is more reasonable to speak of levels of anonymity, although the online reality has been described in terms of being anonymous in and of itself (Morio and Buchholtz 2009). See Edman and Yener (2009) for a detailed explanation of anonymity systems. The absolutist definition of anonymity gives that this type of anonymity makes it ill-suited for most kinds of web-interactions (Rao & Rohatgi 2000). This is why it often is architected for pseudonymity, which is the traceable version of anonymity.

“Anonymity” in relation to the Internet can mean a variety of things, which is why this needs to be specified here. At the very least, this is of interest for the sole reason that different social norms are likely to apply to different types of *anonymising* actions—they can demand different levels of conscious behaviour. In addition to encryption technologies, such as IP VPN tunnel services and ”dark-nets”, we also consider internet cafés, one-click hostings services and offline, hand-to-hand sharing as variations of anonymity techniques. In many ways is anonymity the “natural” state of the Internet, and to identify someone (often) require considerable effort.

Encryption for sale

In this article we mainly refer to “anonymity services” as the use of IP VPN encryption services, which in general equal a technically pretty robust pseudonymity. These services provide the user with the means of avoiding having their IP numbers connected to their offline identity. An anonymity service, or anonymity server, is a server that provides the ability to send e-mail, 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. When speaking of anonymity in the digitalised context of the Internet an important part is to speak about encryption technology,

since many of the options of more actively seeking to be untraceable or anonymous online involves encryption to hide the digital traces you leave behind.

Cryptography has a long history. It is a technology for keeping information hidden or from being leaked to unwanted parties. Cryptography has a variety of uses and has, for instance, played an instrumental role in several military conflicts. One famous example from the Second World War involved the successful decryption of the German "Enigma" cipher by the Allies (see, for instance, Stephen Budiansky 2000). Cryptography can be described as:

> A transformation of a message that makes the message incomprehensible to anyone who is not in possession of secret information that is needed to restore the message to its normal plaintext or cleartext form. The secret information is called the key, and its function is very similar to the function of a door key in a lock: it unlocks the message so that the recipient can read it. (Diffie and Landau 1998, p. 13).

This "key in a lock"-technology has been revived in the digitised online world, and its potential strengthened into virtually unbreakable encryption possibilities. The anonymity services (for someone who wants to access Internet with a stronger anonymity) offered on the Swedish market today are generally the kind that show an IP number different from the one formally assigned to the user by their ISP. There is 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 part can see leads to the service provider, not the client. Some services can be administered through an e-mail account, which makes it even harder to identify the user.

The services for online anonymity that you can find on the Swedish market are the early established Relakks and Dold.se, and of course Ipredator, that the group related to The BitTorrent tracker site The Pirate Bay established during 2009 as a response to the Swedish Ipred-law, and Mullvad.se. In addition to these there are naturally foreign services, such as the SwissVPN and Ivacy, which naturally are open for Swedish subscribers.

Anonymous ways beyond the pay-services

Vinc Cerf, one of the inventors of the TCP/IP structure that is a cornerstone of what we today perceive as the Internet, has said that he regrets not adding stronger

standards for security to the structure, and mentions automatic encryption as an example (Ekström 2010, p. 234). There are of course ways to browse the web and still be quite anonymous without using an anonymity service.

Internet cafés is an example of a set-up achieving anonymity without encryption, which is why governments in both India and Italy have implemented mandatory identification for 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.

As a likely not majorly important but good example on anonymous, or at least ”pseudonymous”, way to send and receive large files is to use a so called ”one click hosting” (OCH) service. OCHs allow internet users to upload one or more files to a one click host’s server, free of charge, or for a small amount use a premium version. Most services return a URL, which can be given to people who then can download the file. If the service does not lock the amount of permitted downloads to a few, the service can be used for file sharing in larger numbers. The possibility to ”split archives” among friends creates possibilities to easily share a hidden ”area” of the Internet to share files within. There are for instance many internet forums that share URLs, which has further contributed to make these services a complement to p2p file sharing. And perhaps, a complement that not to any greater degree has been discussed in these terms. One of the few studies conducted is the Antoniades et al. from 2009 that among other things compared the OCH service RapidShare, which attracts large amount of users, to BitTorrent file sharing in general. 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, p 234). Another example of a globally popular OCH service is MegaUpload. On the Swedish arena there is, for instance, Sprend.

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, sometimes described as sneaker-nets. Pre-paid mobile phones can also access the Internet anonymously. BitTorrent sharing services providing a stronger level of anonymity than “traditional” BitTorrent sharing services are also under development.

There are networks that are being established with secrecy for users as their primary objective. These networks, such as Freenet, are not subject to any external censorship whatsoever; employing software that Ian Clarke released 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" (see, for instance, Bergman 2001). The above mentioned Tor, along with initiatives such as i2p, are examples of networked solutions that creates anonymity online that grew extensively during 2009. In the case of i2p, with around 500 per cent, according to their own statistics.[11] These services gets stronger the more users they get.

Copyright's new muscle in the digital world: The Ipred directive

In April 2004, the EU passed the Directive on the Enforcement of Intellectual Property Rights, the so-called Ipred directive. It was established because it was "necessary to ensure that the substantive law on intellectual property", and 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 spectra, the directive has in general been discussed in connection to copyrigt enforcement.

One of the most frequently debated issues is the fact that the directive gives copyright holders the right to retrieve, via a court decision, the identity information behind an IP address if they "have presented reasonably available evidence sufficient to support its claims" (Article 6.1). The "competent judicial authorities" may then order such information to be provided. Ipred is one of several legislative actions that focus on ISPs, aiming to place greater responsibility on them for the traffic running through their networks.

The Ipred directive is a minimum directive, meaning that Member States can establish national conditions that are even more favourable to rights holders than the directive prescribes (Article 2). The directive refers to all Member States being bound by the Agreement on Trade Related Aspects of Intellectual Property (TRIPS Agreement), which emphasises the global regulatory connection on copyright between nations, the EU as well as international treaties.

Background

The European Commission presented a Communique as early as November 2000 announcing a series of practical measures intended to improve and strengthen the fight against counterfeiting and piracy in the single market. As part of these measures, the Commission forwarded a proposal for a Directive harmonising the legislation of Member States to strengthen the means of enforcing intellectual property rights. By the time the Ipred directive was approved by the European Parliament (March 9th, 2004) it was criticised as being a result of "heavy-handed influence of the American entertainment industry" (Kirkegaard 2005). It caused a stir among citizens' groups in both the US and Europe (Kirkegaard 2005, p.

[11] http://www.i2p2.de/ [last visited 12 May 2010].

489).[12]

The final version of the directive differs in several respects from the Commission's proposed directive, which was met with massive criticism. It contains fewer of the copyright owner-friendly sanctions than the original proposal (Kirkegaard 2005, pp. 488-490). The penal provisions were completely removed, and served as the basis for a second enforcement directive (Ipred 2). However, the final version of the Ipred directive was extended with regard to its scope, which was expanded to include all kinds of violations—including file sharing between individuals.

Swedish implementation of Ipred

Most of the provisions in the Ipred directive were implemented in Sweden by April 1st, 2009. Sweden had already failed to fulfil its obligations under the directive within the prescribed time limit, as the European Court of Justice declared in a ruling on May 15th, 2008 (Case C-341/07).

Implementation of the Ipred directive in Sweden has been a strongly debated issue in Sweden, with a number of operators stating that they discard the identification information that the Ipred directive allows access to as early as possible, and that there are initiatives taken within online communities for creating new encrypted file-sharing services.[13] Neither the directive nor its implementation in Sweden requires ISPs to retain log data for any particular period of time. This 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 withhold such data (see Directive 2002/58/EC, and Chapter 6, Section 6 of the *Electronic Communications Act* in Sweden, 2003:389).[14] The implementation of Ipred in Sweden has put the log data policies of ISPs into focus again, causing a number of them to publicly announce that they do not store this type of data any longer than is absolutely necessary (see Svenska Dagbladet, April 28th, 2009).

---

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

13 For the preparatory legal work in Sweden, see Prop. 2008/09:67 Civilrättsliga sanktioner på immaterialrättens område - genomförande av direktiv 2004/48/EG.

14 In Sweden the regulation today regarding the protection of privacy in electronic communication is mainly found in the 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 emphasises the importance of not storing data too long, for the sake of privacy protection, following from Directive 2002/58/EC.

To date, the legislation has only led to two court cases, despite the initial reports in media of ”hundreds” of cases being prepared by copyright holder’s interest groups.[15]

Presenting data

The data on the general aspects of the responses to the two surveys is presented here. We will 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 an operator of an anonymity service and an operator of a ”one-click hosting” service.

First survey

The first survey was carried out from late January to early February 2009. Of the actual 1,047 respondents, about 59 per cent (619) were female and 41 per cent (427) were male. More than 99 per cent stated that they had access to a computer with an Internet connection at home. More than 75 per cent of the respondents spent at least two hours a day at an Internet-connected computer at home, and about 23 per cent more than six hours a day. About 6 per cent spent less than an hour a day at a computer with Internet access. The 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.

Second survey

The second survey was carried out in October 2009. Of the 1,041 respondents, about 60 per cent (624) were female and 40 per cent (418) were male. More than 98 per cent 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 per cent spent at least two hours a day on the Internet-connected computer (compared to the about 75 per cent of the first survey), and about 21 per cent 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.

Comparison between the two surveys

The mean age for the respondent in the first survey was about 20.9 years, while

[15] This includes the so called Ephone case (Case ÖÄ 6091-09, Oct 13 2009) and the TeliaSonera case (Case Ä 9211-09).

for the second survey it was about 19.9 years. About 8.6 per cent of the respondents in the first survey used an online anonymity service, and about 61.1 percent claimed that they will use one in the future if new legislation enhances the possibility of the respondent being held legally liable if caught file sharing copyrighted material without permission.

This can be compared to the second, post-Ipred implementation survey, where 10.2 per cent of respondents used an online anonymity service, and about 55.6 per cent claimed that they will use one in the future if new legislation enhances the possibility of being held legally liable if caught file-sharing copyrighted material without permission.

Those who file share on a daily basis use anonymity services twice as much as the average respondent in the first study, and almost three times as much in the second study. This particular group also shows a higher level of preparedness for the use of anonymity services if new legislation enhances the possibility of being caught file-sharing illegally. The overall file sharing show decreases, but the measured strength of the social norm had not changed much (Svensson & Larsson 2010), indicating rational rather than ethical or normative reasons for the change in behaviour.

According to the statistics on age groups in Sweden, as of December 31st, 2008 there were 1,332,813 people in Sweden between the ages of 15 and 25 (see Statistics Sweden – SCB). This gives us an estimate of about 115,000 persons in this age span using an anonymity service in January/February 2009, which increased to about 136,000 by October of the same year.

Additional data

The interview with a representative for one of the Swedish operators of a n anonymity service revealed that the effect of the Ipred implementation was instantaneous. The increase in subscribers to the online anonymity service was ”more than double, almost a triple” (interview in May 2010). The ”One-click host” Sprend is a relatively small service with about 95 percent of its users in Sweden, why its statistics, following the argument in this article, could be relevant for the implementation of Ipred. From the interview with the representative of Sprend, using Google Analytics, the increase of users from May 2009 to May 2009 was about 100 percent, from around 30 000 users to 60 000. The representative claims that there has been a big increase in users going from uploading and sending the file format .mp3 to .zip and .rar, bearing witness of a growing knowledge of the users that many files can be bundled into one that is later unpacked by the recipients.

Analysis

The respondents' actual increase in the use of anonymity services is between 15 and 20 per cent between February 2009 and October 2009, suggesting that about 21,000 more people between 15 and 25 years of age began using an anonymity service between the two surveys. There also seems to be a general potential for a majority of the respondents who are willing to pay for anonymity when Ipred is be *perceived* as a real danger, presumably if the law had been practiced more aggressively.[16]

One can speculate on the motives of being anonymous online. Is it just to share files without the risk of getting caught, or are there other reasons? One could hypothesise around, for instance, a desire to hide other types of crime in any organised form, or perhaps to hide *from* being exposed to criminal acts or fulfilling ideals about integrity. There are likely several motives, and some support can be found in the empirical data for the fact that the levels of anonymity have also increased for non-file sharers during the year; however, the numbers are too low to validate this hypothesis in a satisfactory manner.

Those who share files on a daily basis use anonymity services twice as much as the average respondent in the first study, and almost three times as much in the second study. The higher degree of anonymity indicates that illegal file sharing is a reason for seeking anonymity. The fact that the levels of use of anonymity services rose more within the regular file sharers than average indicates that the implementation of Ipred in Sweden was a driver for anonymity, as it generated an increase in the use of anonymity services, which then is a latent dysfunction of the legal implementation of Ipred.

There are other circumstances that point in the same direction. The interview with a representative for one of the Swedish operators revealed that the effect of the Ipred implementation was instantaneous. The increase in subscribers to the online anonymity service was ”more than double, almost a triple”. Further, when the anonymity service Ipredator was first released as a work in progress in April 2009 more than 170 000 signed up as being interested to subscribe. This is likely to be a Swedish phenomenon, meaning that it was likely mostly Swedes that signed up. This is not the same thing as that all of these actually was capable of signing up for the following pay service, but it shows the big interest for a more active online anonymity, and it is an evidence of an increase of the general consciousness related to these matters, brought to attention by the implementation of Ipred. The OCH service Sprend, with a large majority of Swedish users, does not show this explicit pattern of immediate interest when the law was

[16] This would total about 810,000 persons in Sweden between the ages of 15 and 25 that had this type of readiness at the time of the first survey, and 740,000 at the time of the second survey.

implemented, but it sees a constant increase over the year of 2009, doubling its users from May 2008 to May 2009.

Anonymity, although in a somewhat traceable and ”weak” form, is part of the status quo of online behaviour. There is a ”trust” that online activities should not easily reveal the offline identity. There are two exceptions to this trust, of which one is a voluntary release of information that leads to the offline identity, such as revealing birth name, age and pictures in social networks. The other exception is more intricate, and tied to social norms in another way. If de-anonymisation 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 is, the online ”trust” of 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-anonymisation will likely have a negative effect on the status quo of the weaker forms of anonymity. This ”trust” is adversely affected, rendering in counter-measures strengthening the lost anonymity, all in line with the social norms unsupported by the implemented law. This might lead to an escalation on both sides of what now clearly can be described as a conflict. In terms of the broader spread of online anonymity, a cold war has begun, and in terms of the ones being charged with offences in court, as well as counter attacks on for instance copyright agencies' web pages, the war is no longer cold. This type of ”polarisation” brings changes in the structures of how files are being shared, including ”core sharers” or uploaders seeking a higher level of intraceability and the sharers that follow in the chain of the diffusion of the shared material. The Antoniades et al study supports this conclusion also 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, p. 234).

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 not to be caught when violating copyright. Bearing Merton's explanation in mind, it is not possible to find an exact “*net balance*” in the implementation of Ipred in Sweden. One can mention, however, a few aspects on either side of the chart in order to assess whether or not the costs exceed the benefits. In the 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 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. For the sake of argument, however, one could consider the mindset of a policy-maker that has been able to foresee the counterproductive consequences of legal implementation, but still decides to go through with the implementation in the belief that the positive effects outweigh the negative ones. The policy-maker then tries to calculate a "net balance" of the implementation. We have, however, chosen not to call this policy-maker's assessment of a dysfunction as a manifest part of the legislation, but rather a latent one, due to the fact that it counters the articulated purpose of the directive.

There are trends that exceed the scope of the IPR Enforcement Directive that concern the anonymisation of personal information. The driving forces are not likely illegal file sharing, at least not merely, but a strong desire to be truly anonymous online. The initiatives and increased use of Tor and I2P are examples of this. According to their own statistics the I2P-network expanded by about 500 per cent during 2009. I2P's goal is "to operate successfully in hostile environments. even when an organisation with substantial financial or political resources attacks it."[17]

In terms of net balance it is of interest to bring forth a significant criticism regarding the idea that functional analysis tends to focus on the statics of social structure, and is hence too conservative and does not see transitions and shifts in society. It is in response to this critique that Merton introduces the concept of dysfunctions, "which implies the concept of strain, stress and tension on the structural level, provides an analytical approach to the study of dynamics and change" (Merton 1949, p 53). Even though increased anonymity online as a result of a copyright enforcement law will not overturn a century-old regulatory development, it is a sign of stress and tension, and it fuels an analysis of the "dynamics of change", questioning the ability of the legal structure to change.

Further, which is in line with the argument of this article: given the multitude of ways to strengthen untraceability, especially bearing in mind the weak support of the legal norms amongt the social norms in this case, a criminalisation of the operation of anonymity services would be an especially ill-suited attempt to solve "piracy-issues". Not only would such an initiative fail to reduce anonymous sharing of files, it would further stimulate the diffusion of knowledge of encryption and increase this and other techniques for anonymity. Which could be detrimental to all legal enforcement related to computer-mediated behaviour, including behaviour with no or little support in social norms.

[17] http://www.i2p2.de/ [last visited 12 May 2010].

Conclusion

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 behaviour. 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 not to disrupt this status quo. If not, such initiatives are likely to spur counter-measures en masse related to the diffusion of knowledge of how to strengthen the anonymity online, as well as counter measures of smaller elites of pro-privacy activists. The levels of of the different anonymising techniques, encrypted as well as other, is a sign that describes a part of the character of online behaviour, and hence, the character of Internet. Anonymity is a tool in an increasingly important battle between aspects of fighting very serious crime as well as the increase in data storage of individuals everyday actions for various just and unjust reasons on one side and individuals integrity and privacy on the other.

The fact that a growing group of the younger generation chooses to pay for online anonymity rather than to cease file sharing or paying for copyrighted content forces us to think more deeply about whether there is something malleable about how copyright is formulated and handled today. To share files illegally in Sweden is not socially deviant behaviour among those between 15 and 25 years of age, and these individuals feel no pressure from their friends, family, and so on that leads them to believe that illegal file-sharing is wrong. The results of this study therefore indicate that a continuation of the repressive legislative path would likely create more anonymous file sharing, under a variety of techniques, and a more anonymous Internet as a whole.

This initial evidence of an increase in online anonymity as a result of the implementation of a law for hunting illegal file sharers shows the need for understanding the different levels of anonymity on the internet, as well as the rationale behind individuals choosing to more actively go (more) anonymous. What are the driving-forces and social norms behind the various initiatives of ”dark-nets”, who is using it, when and for what reasons?

An anticipated conclusion, that require further assessment, is that the file sharing patterns are changing in terms of visibility. It is likely that a core of sharers are developing, that are more inclined to pay for anonymity services due to their anticipated need for and advanced protection for being caught violating copyright laws. The data supports this to some extent. It is however also likely that a more loosely formed group of sharers are developing, connected to the core shares but not centrally located in the sharing process. They are using other means for sharing, such as ”secret” groups and trusted networks and hand-to-hand and One Click hosting services.

A consequence of an increase in online anonymity, not solely for copyright violations but for law enforcement as a whole, is, as mentioned, that any criminal investigation that tracks illegal behaviour on the Internet will suffer from 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 Lessig made in Code v2 (2006) that there are choices to be made about how the character of Internet evolves, and that these choices will affect fundamentally what values are built into the network. The choices made will affect the very character of Internet, the levels of anonymity and pseudonymity, it will affect the speed of a broader introduction to encryption technologies and, hence, the criminal investigation not only in areas of copyright but on a much broader scale. In terms of law, legality and legitimacy, it is likely to participate in the creation of distance between nations' attempts to regulate online related behaviour and the actual behaviour. 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. It creates obscurity rather than compliance, risking to become a dysfunction that leads to "operational difficulties", to use the words of Vago (2009, p. 22).

References

Legal references

Case C-341/07, Judgment of the Court (Sixth Chamber) of 15 May 2008: Commission of the European Communities v Kingdom of Sweden (Failure of a Member State to fulfil its obligations – Enforcement of intellectual property rights – Failure to transpose within the prescribed time-limit).

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

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

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society: INFOSOC.

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.

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

SOU 2003:35 Upphovsrätten i informationssamhället - genomförande av direktiv 2001/29/EG, m.m.

Prop. 2004/05:110 Upphovsrätten i informationssamhället – genomförande av direktiv 2001/29/EG, mm.

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.

Literature

Antoniades, Demetris, Markatos, Evangelos P. Markatos and Dovrolis, Constantine. 2009. ”One-Click Hosting Services: A File-Sharing Hideout,” *Internet Measurement Conference*, *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, Chicago.

Appelstrand, Marie. 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, Matthias. 2003. *Norms and legal rules. An investigation of the tunnel construction through the Hallandsås ridge*, Department of Sociology, Lund University.

Berger, Peter L. 1963. *Invitation to Sociology*, NY: Doubleday, Anchor Books.

Bergman, Anna-Karin. 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, Michael K. 2001. “The deep web. Surfacing hidden value,” Citeseer.

Boyle, James. 2008. *The Public Domain. Enclosing the commons of the mind*, New Haven & London: Yale Universityt Press.

Brown, B., J. 1992. ”Latent effects of law: The defamation experience”, in *Singapore Journal of Legal Studies*, pp 315-346.

Budiansky, Stephen. 2000. *Battle Of Wits: The Complete Story of Codebreaking in World War II*, Free Press.

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

Diffie, W. and Landau, S. 1998 *Privacy on the line: The politics of wiretapping and encryption*. Cambridge, MA: MIT Press.

Dillman, D. A. 2000. *Mail and internet surveys: The tailored design method* (2nd ed.) . New York: Wiley.

Du Pont, George F. 2001. ”The criminalization of true anonymity in cyberspace”, in Michigan Telecommunications and Technology Law Review, 191.

Edman, Matthew & Yener, Bülent. 2009. ”On anonymity in an electronic society: A survey of anonymous communication systems”, in *ACM Computing Surveys* 42(1), pp. 1-35.

Ekström, Andreas (2010) *Google-koden*, Stockholm: Svante Weyler Bokförlag.

Froomkin, A. Michael. 2008. ”Anonymity and the Law in the United States”, in Kerr, Ian. *Lessons from the identity trail: Anonymity, privacy and identity in a networked society*, New York: Oxford University Press, 2009; University of Miami Legal Studies Research Paper No. 2008-42. Available at SSRN: http://ssrn.com/abstract=1309225

Rosenzweig, Paul. 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

Hassan, Robert. 2008. *The Information Society*, Polity Press.

House, Robert J., 1968. ”Leadership training: Some dysfunctional consequences”, in *Administrative Science Quarterly*, Vol. 12, No. 4, pp. 556-571.

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

Hydén, H. and Svensson, M. 2008. “The Concept of Norms in Sociology of Law,” in Wahlgren, Peter (ed.) *Scandinavian Studies in Law*, Law and Society.

Jensen, Christopher. 2003. The More Things Change, the More They Stay the Same: Copyright, Digital Technology, and Social Norms, in *Stanford Law Review*.

Johansson, Daniel and Larsson, Markus. 2009. “The Swedish music industry in graphs. Economic development report 2000-2008.” Stockholm: Royal Institute of Technology, and TrendMaze.

Larsson, Stefan. forthcoming 2010. “Enforcing copyright. A repressive European legal trend from a socio-legal perspective”, in *SCRIPTed*.

Larsson, Stefan. 2009. “Law as a gate keeper for participation. The case of 3G infrastructure development in Sweden,” in Baier, Mathias, ed. (2009) *Participative aspects on law - a socio-legal perspective*, Lund studies in Sociology of Law.

Larsson, Stefan. 2008. “Non-legal aspects of legally controlled decision-making – The failure of predictability in governing the 3G infrastructure development in Sweden,” in Hydén, Håkan and Wickenberg, Per, eds. (2008) *Contributions in Sociology of Law. Remarks from a Swedish horizon*, Lund studies in Sociology of Law.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolf (2009) A Brief History of the Internet, ACM SIGCOMM *Computer Communication Review*, vol 39, no 5.

Lessig, Lawrence. 2006. *Code version 2.0*, New York: Basic books cop.

Lessig, Lawrence. 2008. *Remix: making art and commerce thrive in the hybrid economy*, New York: Penguin Press

Litman, Jessica. 2006. *Digital Copyright: Protecting Intellectual Property on the Internet, the Digital Millennium Copyright ACT, Copyright Lobbyists Conquer the Book Description*, Prometheus books.

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

McAulay, Laurie. 2007. ”Unintended consequences of computer-mediated communications”, in *Behaviour and Information Technology,* Vol. 26, No. 5, 385-398.

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

Merton, Robert K. 1949. *Social theory and social structure: toward the codification of theory and research*, The Free Press, Glencoe, Illinois.

Merton, Robert K. 1936. ”The Unanticipated Consequences of Purposive Social Action”, *American Sociological Review*, vol. 1, pp. 894-904.

Morio and Buchholtz. 2009. “How anonymous are you online? Examining online social behaviors from a cross-cultural perspective,” *AI and Society 23*, 297–307.

Palfrey, John & Gasser, Urs. 2008. *Born Digital: Understanding the First*

Generation of Digital Natives, Basic Books.

Rao, Josyula R. and Rohatgi, Pankaj. 2000. ”Can pseudonymity really garantee privacy?”, in *Proceedings of the 9th USENIX Security Symposium*, Denver.

Ridgway, V. F. 1956. ”Dysfunctional Consequences of Performance Measurements”, in *Administrative Science Quarterly*, vol. 1, No. 2, pp. 240-247.

Ritzer, George. 2007. *Contemporary Sociological Theory and its classical roots: the basics,* second edition, New York: McGraw-Hill

Ritzer, George and Goodman, Douglas J. 2003. *Sociological Theory*, 6 ed., Boston: McGraw-Hill.

Roots, Roger I. 2004. ”When Laws Backfire. Unintended Consequences of Public Policy”, in *American Behavioural Scientist*, Vol 47., No. 11., 1376-1394.

Rowland, Diane. 2009. ”Privacy, freedom of expression and cyberSLAPPs: fostering anonymity on the internet?”, in *International Review of Law, Computers & Technology*, 17:3, 303-312.

Sunstein, Cass, R. 1994. ”Political Equality and Unintended Consequences”, in *Columbia Law Review*, vol. 94, No. 4, pp. 1390-1414.

Svensson, Måns. 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.

Svensson, Måns and Larsson, Stefan. 2009. “Social Norms and Intellectual Property. Online norms and the European legal development”, Research Report in Sociology of Law. Lund University.

Svensson, Måns & Larsson, Stefan. Forthcoming.

Vaidhyanathan, Siva. 2001. *Copyrights and copywrongs: The rise of intellectual property and how it threatens creativity*, New York: New York University Press, cop.

Wagner, Kenneth C. 1954. ”Latent Functions of an Executive Control: A Sociological Analysis of a Social System under Stress”, *Research Previews, vol. 2*, Chapel Hill: Institute for Research in Social Science.

Vago, Steven. 2009. *Law and society*, Upper Saddle River, N.J: Pearson Prentice Hall, cop.

Weinstock Netanel, Neil. 2008. *Copyright’s paradox*. New York: Oxford University Press. Wolf, James. 2008. "Self-Administered Questionnaire."

Encyclopedia of Survey Research Methods, SAGE Publications. [visited 21 May. 2010]. http://www.sage-ereference.com/survey/Article_n522.html

Vincents, Okechukwu Benjamin. 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), Oxford University Press.

Daily press

ABC News: *Pirate Bay Trial Turns into a Circus. The court case against the Pirate Bay four in Sweden is going from strange to surreal. Where is CourtTV when you want them?* By Jeff Bertolucci, PC World, February 20, 2009 *Availble at:* http://abcnews.go.com/Technology/PCWorld/story?id=6923048 [Last accessed 26 November 2009].

Editorial in Los Angeles Times, 18 April 2009, *Editorial, The Pirate Bay ruling. A Swedish court rules against a wesbsite notorious for bootlegged content. But the war rages on Availble at:* http://www.latimes.com/news/opinion/editorials/la-ed-pirate18-2009apr18,0,3705805.story [Last accessed 26 November 2009].

El Pais, ELPAÍS.com - Madrid – 18 February 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 Availble at:* http://www.elpais.com/articulo/internet/demandantes/juicio/The/Pirate/Bay/retiran/mitad/cargos/elpeputec/20090218elpepunet_3/Tes?print=1 [Last accessed 26 November 2009].

Gustafsson, Joel, 2009. *Nätoperatörer kringgår inte Ipred*, Svenska Dagbladet (28 April 2009). Available at http://www.svd.se/nyheter/inrikes/artikel_2805959.svd [Last accessed at 30 December 2009].

Statistics Sweden – SCB – Statistiska CentralByrån, www.scb.se [last accessed 30 November 2009].

The Telegraph, *What does The Pirate Bay ruling mean for the web?*, by Claudine Beaumont, Published: 12:23PM BST, 17 April 2009 *Availble at:* http://www.telegraph.co.uk/technology/news/5170684/What-does-The-Pirate-Bay-ruling-mean-for-the-web.html [Last accessed 26 November 2009].