The three domains of copygrey business

On the need for a balanced Internet policy

Jan Nolin

Paper presented at the 11th Annual Conference of the Association of Internet Researchers (AoIR), Gothenburg, October 21-23, 2010

Abstract
This article is structured around three aims. First, a number of historical contextual factors are described which are seen to create a restrictive policy for intellectual property rights on the Internet. Furthermore, this has tended to be the sole major policy initiative on Internet policy. The restrictive policy is seen to be a historical construct, ill-fitting for a mature Internet.

Second, it is argued that there is a need for a more balanced policy approach concerning the free circulation and manipulation of media files on the Internet. Thereby, policy could work with, rather than against the huge creative energy relating to what is here called Internet-based cultural consumption (IBCC). I maintain that much is won by utilizing a broad concept, such as this, as it enable us to understand filesharing as an information practice in transformation where the major drivers of change are commercial ventures that are actually exploiting legislative weakness.

Third, it is maintained that the heavy-handed and one-sided Internet policy actually has served to create a copygrey business. The three domains of copygrey services are described in the text.

Keywords: Internet-based cultural consumption, filesharing, peer-to-peer, DMCA, IPRED, copygrey business, copygrey service, Copyright Act, ACTA, intellectual property rights, safe harbor, fair use, DMCA takedown notice, DMCA loopholes
1. Introduction

Arguably the most severe problem in analyzing the Internet concerns the complex relationship between this artefact and society. The development of the Internet in various ways serves as a significant factor in the development of national cultures and economies. It is therefore vital that a sophisticated Internet policy is developed that is firmly in touch with a number of policy sectors, primarily economic and cultural policy. Furthermore, due to the complexity of the issues involved and their cross-policy sector character, it becomes essential that policy is supported by research based knowledge.

As an information scientist involved with policy studies, it is frustrating to review a general absence of policy initiatives within Internet policy. Even worse, the major initiative that has been ongoing as a global policy agenda, intellectual property, is essentially flawed by lack of cross-policy insights. The US Copyright Act of 1976 and the Digital Millennium Copyright Act (DMCA) from 1998, and their various national-based off shots concerning intellectual property, builds on a set of old ideas that certainly have the feel of coming from another millennium.

This article is structured around three aims.

The first is to reconstruct the basic ideas that constructed a containment of Internet policy within policy for trade and commerce. More specifically, the current policy strand represents the "monopoly view" of a long-standing conflict on intellectual property rights.

The second is to argue for a more balanced policy approach concerning the free circulation and manipulation of media files on the Internet. In this way, it becomes natural to reconceptualize "filesharing". As a term suitable for both policy and research, I here suggest "Internet-based Cultural Consumption" (IBCC). This refers to a wide, lively and important part of Internet which now has a relatively long history, moving through several complex phases. In this paper, I suggest that IBCC is entering a new phase/era/chapter in which it becomes evident that the restricted Internet policy on, what is obviously a complex policy issue, produces unintended commercial structures. I maintain that much is won by utilizing a broad concept, such as this, as this enable us to understand the filesharing as an information practice in transformation where the major drivers of change are commercial ventures exploiting legislative weakness.

The third aim is therefore to characterize "the copygrey business", which can be seen to be a commercial response to one-dimensional and heavy-handed legislation. This strange phenomenon constitutes the price that we pay for our attempts to abide to ideas whose time has gone.

This article is the first in several discussing the recent transformation in IBCC within the project Filesaharing after IPRED (FILIP). Forthcoming articles will be concerned with changes in IBCC-and information-practices among a number of Swedish users.
2. How Internet policy became intellectual property

2.1 The hands off approach

While the role of politics is certainly important in shaping societies, there has historically been an obvious absence of heavy-handed Internet regulation. This seems to have several causes. Most essentially, Internet is a global phenomenon that disrupts the relation between geographic location and power (Johnson & Post 1997). This makes it difficult for the nation-state to claim legitimacy in regulating as well as assembling the necessary resources for creating local restrictions on a global network. Geographical location tends to become a non-issue on the Internet. Furthermore, contrary to the development of other media such as TV or radio, Internet service providers have not needed government licenses in most industrial countries.

The lack of regulation can also be explained in terms of the Internet being such a quickly developing and changing technology. The "hands off approach" can also be the result of ideology. Already in 1977, Langdon Winner argued that politicians are susceptible to the idea of a technological development out of control, being happy to leave this area to the business community. However, there are certain commercial ventures that have highlighted the need for Internet regulation and found a favorable response from politics. Lessig (1999; 2002; 2006; Lessig et al. 1999) argues that US Internet politics rhetorically have been aimed to allow the Internet to take care of itself. He is, however, much concerned about the one major exception: intellectual property rights. Here, we have actually seen a massive expansion.

2.2 The drawbacks of allowing the business community to dictate Internet policy

It is easy to agree with Barney (2000) that the political reluctance to realize the role of Internet politics opens the door for big business, in turn circumventing democratic potential. The larger picture was sketched by Castells (2000) in his *The Rise of the Network Society* trilogy. These books highlight a classical duality between commercial agenda setting promoted by the business community and the resistance identity of the people. Given such a conflict, it becomes problematic if policymakers constrain themselves to seeing the Internet as a vehicle for commerce. Given the insight, identified statistically by Kedzie (1997), that there is a correlation between the third waves of ICT (Toffler 1980) and democracy (Huntington 1991), there are fundamental societal aspects of the Internet that policy simply ignores.

An exclusively business oriented Internet policy fails to connect with the new private sector of social and commercial activists identified in the works of Dyson (1997; 1998). Dyson stresses that the Internet serves to undermine all kinds of central authorities. She identifies the decentralizing and fragmenting character of the Internet as a destabilizing force and therefore as a revolutionary tool for redefining local and global citizenship.
An exclusively business oriented Internet policy also becomes sidelined by the energies of a new global youth culture that redefines their lives through the Internet. This new generation has been conceptualized as digital natives (Palfrey & Gasser 2008) the net generation (Tapscott 1998; 2009), generation M (Strauss & Howe 1991; Cvetkovic & Lackie 2009), and the Google generation (Gunter et al. 2009). As legal scholars Palfrey & Gasser (2008) put it:

> The explosion of creativity online has given rise to new forms of expression and extended others, like sampling, to a broader population of creators... When we combine this challenge to existing copyright law with the common practice of illegal file-sharing of music and movies... We see the makings of a legal trainwreck. And it is digital natives and traditional copyright holders who will be facing one another down. (118)

This comment relates to one of the major points that I want to argue in this article: as the business community (or rather "communities") pushed for early legislation, they effectively worked against the construction of a well functioning digital market on the Internet. The digital landscape on the Internet became, with the ancient Copyright Act of 1976 and the DMCA of 1998, a forbidding territory. The legal ideas were as poorly respected as The Volstead Act during the US alcohol prohibition. The recent decade has been a veritable lawless Wild West with the wealthy cattle owners/media conglomerates attempting to hire trigger-happy sheriffs.

### 2.3 The essential conflicts of Intellectual property rights

My perspective on intellectual property and its historical development is inspired by the works of political economy researchers Susan Sell and Christopher May (May 1998; 2000; Sell 1998; 1999; Sell & May 2001). This research provokes a shift of perspective from the two views that tend to dominate research on intellectual property. The first of these views sees the development of intellectual property as the result of a process with no inherent conflict of interest. The alternative perception is to recognize conflict of interest, although this is visualized as a fair negotiation process where involved actors can come to an agreement. Sell and May, instead, suggests a critical perspective in which the resolution of conflicts of interests will tend to rely on power structure and power play.

Historically, the development of intellectual property rights has been a never ending competition between two different views. The first of these maintains that the public should be allowed free access to information as this is a prerequisite for the development of culture, society and democracy. As an extension, this ensures an educated labor force, increases in entrepreneurial activity and economic growth. The second view argues that creative producers of original content should benefit from their activities. As an extension, this creates drivers for innovation, creativity and entrepreneurship.

As the conflict between these two views is so fundamental, history has tended to show that every settlement opens up for new difficulties. The rules are changed, opportunities become redefined and the winners in the old framework are now labeled losers (Sell & May 2001). In other words, any settlement on this issue, so fundamental for society, is a response to earlier injustices and will redefine the issue itself. As the new state of affairs will be skewed in the opposite direction, it is only a matter of time before a new backlash sets in.
The dominating conception of this conflict during the 20th century was monopoly (strong ownership) versus free trade. Up until the 1980s, legislation tended to favor free trade. Therefore, when Kodak in 1976 duplicated the instant camera developed by Polaroid, this was allowed. However, a decade later things had turned round as Polaroid won a devastating settlement against Kodak in 1986.

Intellectual property rights have a long history, which is, however, unevenly developed from country to country. The US enacted the first Copyright Act in 1790. Copyright holders were given exclusive ownership today works for 14 years with the possibility of a 14 year renewal. In 1831, this was considered to be too short time periods and therefore extended to 28 years with a 14 year renewal option. The major revision of the Copyright Act was made in 1976. The author/artist was given exclusive rights for 75 years or life of author plus an additional 50 years.

It is still these ideas, from the mid-1970s, that constitute the legislative framework for the Internet. Actually, the frequent litigation from the music industry in recent decade is often misleading in its reference to the DMCA. The relevant legislative support is not a few years old, rather, these ideas were formulated at least two decades before the breakthrough of the Internet.

The revision of the Copyright Act in 1976 was necessary in order to solve the fundamental problem in the US context: existing double standards in federal and state law. In a radical turn, the Copyright Act took precedence over all state law and became title 17 of the US Code. Since the most recent revision had been made in 1909, the new copyright law dealt with specific requirements for television, motion pictures, phonograms and radio. Once again, the Internet and the World Wide Web was not envisioned.

It is in this legislative text that we find two of the three most fundamental loopholes that today governs the copygrey business.

The first is the formulation under section 102 of the act. It is said that copyright protection extends to "original works of authorship fixed in any tangible medium". Translated into the Internet, this means that it is hosting a media file which is illegal. Linking to it is not.

The second loophole lies in the codification of the exceptionally vague legal concept "fair use". At the time, this was applicable to personal recordings of phonograms and TV/radio broadcasting. This was relatively unproblematic. Translated into the Internet, this meant that recordings from streaming radio and video became allowed. Fair use in today's legal setting has been extremely problematic.

The third loophole was the concept of safe harbor and was introduced in the 1994 TRIPs agreement (see below). From there, it was transferred into the US Code with the DMCA of 1998. Safe harbor serve as a protection for distributors of information and culture. In the translation to the DMCA this became a protection for Internet service providers who were not to be liable for content distributed by their customers. However, this could also serve as a loophole for other types of distributors such as YouTube and USENET providers. Safe harbor also becomes an essential loophole for link pages and for search engine companies such as Google. In order to qualify for safe harbor, there needs to be an efficient takedown procedure and policy in place.
However, it is also required that the service provider does not have any knowledge of or benefit economically from the infringement of customers. This requirement creates a legal hotspot that threatens all actors with a strategy of working within the safe harbor protection. As this applies to practically every Internet service provider, it becomes a touchy legal issue.

US copyright law has been formative for international legislation in several ways.

First, the strong tradition of copyright legislation goes back to the U.S. Constitution. This has enabled the development of a robust legal competence in this area. Copyright issues have been discussed for centuries and been connected to the most fundamental ideas of the Democratic state.

Second, US corporations have lobbied for both weaker and stronger legislation for centuries and have been well prepared to push intellectual property discussions in both national and international arenas.

Third, the strong international position of the US cultural industry, particularly concerning music, enabled the US to recognize potential problems at an early stage. They also could see themselves as being victimized both nationally and internationally.

Sell (1999) has described how 13 chief executive officers from US multinational corporations formed the Intellectual Property Committee (IPC) in 1986. These represented companies such as CBS, Du Pont, General Electric, Hewlett-Packard, IBM and Johnson & Johnson. They had a common interest in developing broad international property regulation concerning patent, copyright, trademarks and trade secrets. IPC recognized that the new global economy created a context in which intellectual property became a key power factor. This constituted a kind of "paradigm shift" as earlier intellectual property had been exclusive domain of international property lawyers.

It is notable that IPC only was marginally interested in digital intellectual property rights. The only entertainment company members were Warner Communications and CBS. Most of the others were concerned with traditional manufacturing industries involved in the outsourcing of industrial base to third world countries with cheaper labor resources. They were mainly focused on the problem of outsourcing having a side effect of counterfeiting. These kinds of industrial concerns led to a crude linkage between intellectual property rights and counterfeiting which has been allowed to set the frame for Internet legislation.

IPC created alliances with other actors within the private sectors of Europe and Japan. Together, they formed the "Trilateral Group" that enrolled policymakers on a global basis. It was this group that together negotiated and wrote the blueprint for the so-called Trade Related Aspects of Intellectual Property Rights (TRIPs) agreement (1994). "The US government pushed hardest for the TRIPs agreement, but the power behind the throne was this well-coordinated private sector group" (Sell & May 2001, 493).

In this all-important document, "intellectual property rights" is seen as an extremely broad concept. This is an idea that still underpins Internet legislation. This bloated concept signals no difference between, on the one hand, a systematic and commercial production of designer
clothes, watches, mobiles, prescription drugs and, on the other, a 10-year-old remixing her favorite music. This seems, however, mostly an effect of those drafting the text either not being concerned with the digital dimensions of intellectual property rights or simply not able to visualize the problems appearing half a decade later. This becomes evident in article 61 of the agreement, which deals with criminal measures appropriate for all kinds of intellectual property rights infringements. Here it is clearly stated that the target of legislation is "wilful trademark counterfeiting or copyright piracy on a commercial scale" (World Trade Organization 1994, article 61). This supplies a mandate for tracking down Pirates, but not the occasional pirate customer.

2.4 Two international policy streams become one

The TRIPs agreement created a foundation for national legislation on digital intellectual property rights. The two most influential policy streams were developed within the US (DMCA) and the EU. Both of these were initiated in the early to mid 90s and were given a foundation in 1998. While both of them were clearly positioned within the "monopoly position", they were actually two different approaches.

The DMCA positioned itself as a national implementation of two treaties signed by the World Intellectual Property Organization (WIPO) two years earlier: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. In other words, the basic ideas must have been formulated in the mid-1990s, barely a few years after the launching of the World Wide Web in 1991. The strength of the DMCA, compared to the European approach, was that it constituted an attempt to regulate digital practices, without explicitly connecting these to other marketplaces. This enabled the legislators to recognize various unique qualities of digital information. Therefore, some of the exemptions formulated, such as for libraries, were quite advanced for its time. As the European approach was much more general, such insights, and exemptions, would take time. Concepts such as "library" and "libraries" are absent in the TRIPs agreement.

The DMCA, as well as the WIPO treaties, banks on one important idea, what is commonly called Digital Rights Management (DRM). In the DMCA, it is characterized as "copyright protection systems". At the time, this must have appeared as a foolproof idea. Four new paragraphs were introduced into title 17, Chapter 12 of the US Code. The key one is paragraph 1201, a new prohibition entitled "Circumvention of copyright protection systems". This clearly prohibits the removal of any kind of copyright protection system. In paragraph 1204, criminal measures are clearly stipulated for those who have "willfully and for purposes of commercial advantage or private financial gain" removed such protection. First offenders can expect up to $500,000 in fines and/or five years imprisonment and double up for the repeat offender.

This legislation clearly focused systematic piracy for commercial profit. The ordinary user was not targeted simply because copyright protection systems (DRM) were expected to function. As long as it was illegal to remove DRM, users would be forced to consume digital products with protection software in place.
A remarkable convention came to be established in the years to come as ordinary users were systematically brought to justice for a handful of downloads. Usually, these had accessed digital products in which the protection systems already had been removed. Usually, they were confronted with fines that in the original legal text were designed for large-scale pirates.

The European Commission (1998) wrote a green paper on the theme "counterfeiting and piracy", thereby initiating this policy stream. The text begins with an outline of the general problem of counterfeiting and piracy. This was a perspective that clearly followed upon the broad all-inclusive agenda set by the IPC in the late 1980s. The paper makes a virtue of "counterfeiting" and "piracy" covering "all products, processes and services which on the subject-matter or result of an infringement of intellectual property right" (The European Commission 1998, 7, italics in original). The establishment of this "wide scope" is seen as a major benefit for the construction of a catchall legislation. The authors had clearly the manufacturing industry in mind, but as a sideline notes: "Piracy in the services sphere will cover mainly broadcast services and services linked to development of the information society" (7).

Ever since this policy document, counterfeiting and piracy have been held together as key legislative concepts within the EU and served as an umbrella for the regulation of digital practices on the Internet (The European Commission 2000; the European Council 2003; the European Parliament 2004; the European Commission 2004; the European Council 2006). In essence, this has created a policy context in which the same legislative instruments are appropriate for organized counterfeiting crimes, as for the digital practices of ordinary citizens. While the DMCA refers to WIPO-treaties from 1996, the European Union follows the track established by the TRIPs agreement.

Arguably, broad interests of multinational companies of the 1980s as well as the digital visions of the mid or early 1990s will unavoidably host simplistic images of what today are extremely complex issues. The crude connection of the gifting economy of filesharing with organized crime and counterfeiting is of little assistance in developing a sophisticated policy framework. On the one hand, the monopolizing standpoint on intellectual property rights has been given an extremely strong global position. On the other hand, technologies for free copying and distribution have never been so sophisticated and widespread. As a result, loopholes are unavoidable and since the phenomenon transforms in response to legislative efforts, policing becomes increasingly difficult and questionable.

In recent years, several countries, led by the US and Japan, have initiated a so-called "plurilateral negotiation process" on a new "Anti-Counterfeiting Trade Agreement" (ACTA). A handful of countries have joined these proceedings, including the EU. It is curious to see that these countries have come together on the old "anti-counterfeiting" umbrella, the ancient brainchild of multinational corporations in the late 1980s. This is, also, the same kind of catchall, broad legislation that the EU has pursued since late 1990s. Despite this approach being less useful for IBCC than the DMCA, which at least recognize the uniqueness of digital products, the US has seemed to switch policy stream.¹

¹ One probable cause for the reemergence of the strong anti-counterfeiting umbrella would be that the Internet has tended to renegotiate ideas on what is a sellable commodity. Cultural products easily adapted to the digital media, such as music, are slippery and, unavoidably, freely
From the perspective of this author, it is futile to construct broad policy without recognizing the complexities involved in IBCC. The three layered domains of the copygrey business that I will discuss in this article are so different from anything else that it needs to be dealt with on its own terms. Currently, we need specific regulation that not only deals with "white" IBCC, there is clearly a market where a number of actors are making money through the distribution of the same products for free. A number of diverse and urgent policy problems appear in connection with the domains surrounding copygrey services.

2.4 The fear of convergence

An important factor, in how the media in the 1990s positioned itself in relation to intellectual property legislation, was the uncertainties regarding the convergence of "old and new media" (Jenkins 2008). A widely accepted belief was that the evolution of new media would basically kill the old. As the car made the horse obsolete and the computer did away with the typewriter, so would eventually new media destroy newspapers, books, radio, cinema etc. Usually, it was thought that each home would host one all-powerful and unified media device that would control all content. The strategic and heavily subsidized game consoles of Microsoft (Xbox) have been in line with this ambition, with the aim of being the unified power device of the living room. Jenkins (2008) points out that we now find that the convergence of old and new media is ongoing, but it is much more complex than expected in the 1990s. Old media are not becoming extinct, instead there is a mixture in which the old and new are enriching each other in unpredictable ways.

However, the dominating image within media corporations of the 1990s, was that their products in the future would be exclusively active within the digital domain of a unified single media. This made it possible to think that it was:

a) vital to ensure the digital rights and
b) control the distribution of media files on the unified single media.

This actually connected to an old dream, that of reselling.

2.4 The dream of reselling

In his history of the development of filesharing, Alderman (2001) sees the idea of "reselling" as based on the practical experiences that the musical industry drew from the technological switch distributed to what otherwise could be paying customers. However, fan products that are not digital can be sold more easily. You can't download a T-shirt. As there exist distribution systems for music beyond the traditional commercial system, there is a potential for a larger fan base. This, in turn, may create a foundation for a much larger market for fan base products than within the old system. As a consequence, it becomes more important to further policy within the counterfeiting umbrella.
from vinyl records to CD in the 1980s. This was a virtual Klondike for the record business. Suddenly, it became possible to resell the same product to the same customer at a large-scale. This activated the backlog of old recordings since a huge amount of customers needed to rebuild their old record collections in the new medium. Furthermore, although the production of CD records was considerably cheaper, the market readily accepted a higher pricing than was possible for vinyl.

Similarly, the motion picture industry had in the 1980s successfully developed a model of reselling. The first sale was to the cinema, then to video, to cable and finally regular TV. Why couldn’t the music industry, with a product holding a much higher potential of repeated consumption (who wanted to see the same movie more than twice anyway?), develop a similar model?

This established a kind of exploitative customer view where future technology was seen as an instrument for tricking customers into repeat sales. If policy and innovation was handled, then new technologies would be established with regular intervals. Each time, the record companies could reap rewards of another Klondike, reselling the same music to the same customers again and again.

The prerequisite for this development was legislative control over the technological development. However, that in itself was not enough in order to optimize future profits. A secondary control idea was to hold strict control over the legal rights themselves. It was important to disrupt the symmetrical relationship between the rights holder and the user. It was a problem that the customer could buy music and then own it. In principle, this made it possible to make endless copies of owned property. The buyer could then create and format new copies for different listening devices, rather than actually buying new ones. This particular dilemma, grounded in a vision of optimizing profit, gave rise to the idea of licensed music. The customer would only be allowed to buy a license for digital music in future applications. The license would be restricted so that use was only allowed on a particular device. If the customer wanted to play the music on another device, simple, just buy another license.

This system was to be controlled with the help of technology that restricted all forms of copying. It would eventually be named Digital Rights Management (DRM). With control over legislation and technology, future Klondikes seems assured. As we have seen, the ideas of DRM were clearly inscribed into the DMCA.

2.6 The unintended consequences of the DMCA

In intermittent reviews, the Electronic Frontier Foundation has identified a number of "unintended consequences" of the DMCA. In the latest review (2010), the following are listed:

- The DMCA Chills Free Expression and Scientific Research
- The DMCA Jeopardizes Fair Use
The DMCA Impedes Competition and Innovation

The DMCA Interferes with Computer Intrusion Laws

If these are the unintended consequences, what were then the intended outcomes? This is, actually, not easy to discern in a reading of the DMCA. The document itself, which is what all discussion refers to, is not a policy document. It is not even a hybrid between a policy document and a legal document; it is a purely legal in format, constituting a revision of the outdated Copyright Act from 1976. Obviously, it becomes difficult to read without also reading the earlier text. The DMCA itself contains no clear statement of purpose, vision or aims. Instead, it is focused on articulating a set of restrictions as clearly as possible and then to set out a number of limitations, exceptions and punishments. However, a reading of the Copyright Act from 1976, gives no further guidance, it is not that kind of document. Furthermore, as it is from 1976, it couldn't possibly say anything about the Internet.

The closest to an articulation of purpose is a statement in the official summary of the DMCA, not present in the whole document (!): "... the safe and efficient exploitation of works on digital networks" (The Digital Millennium Copyright Act: Official Summary 1998, 3). The positioning of IBCC within trade and commerce policy is seemingly done without any reflection on viable alternatives. There seems to be some underlying idea that the DMCA is to create a clear set of legal guidelines for sustainable digital commerce. If this, indeed, is the intended outcome, then there has been some success in this area, but most importantly, a new significant business domain has been created that also must be seen to be part of the "unintended consequences".

In the continuation of this article, I will argue that instead of creating a context of safe and efficient commercial exploitation (eliminating the "black market" of freely circulating media files), a very strange and, seemingly, flourishing "copygrey business" has been created. In other words, what was earlier a free exchange of cultural products is now a complex and dynamic business sector.

It has taken a number of years before the trajectory of the Copyright Act/DMCA restrictions have been developed into a reasonably effective system for detection, litigation and punishment. However, at the same time, filesharing practices have been transformed and moved away from areas that legislation practices have explicitly targeted. We have entered a new phase of IBCC where the exchange of media files proceeds systematically through unavoidable loopholes and where these "grey areas" becomes the foundation for enterprising in three different domains.

3. Internet policy: economic and cultural development

3.1 Reconceptualizing filesharing

The launching of Napster in 1999 changed the landscape of policy and economy concerning cultural distribution and consumption of diverse cultural products, mainly, at the time, music. Much of the thinking on intellectual property rights on the Internet, including the DMCA,
became instantly obsolete. It became puzzling to see how legislation could deal with, and penalize, activities that were not even imagined when Bill Clinton put his pen to the paper.

In order to rejuvenate and support contemporary policy work, we also need to update some of the key concepts of Internet policy. One important starting point is that top-down concepts such as "intellectual property rights", "copyright" etc. should not be agenda setting since they do not reflect the main activities on the Internet. Instead, we need to start with policy and research concepts that reflect the activities of the Internet. These are more in line with cultural consumption, coproduction, remixing and sharing of media products. As Anderson (2009) notes, the tendency is toward free cultural content. Already, there are a number of original ways available for the commercial exploitation of "free culture". Some of this is positioned within what I call "copygrey services". These are, actually, adapted to the new structures of sharing within the Internet. They reflect the kind of convergence referred to by Jenkins (2008), but which is often disallowed by the Copyright Act and the DMCA. This must be so, since the authors of these legal principles lived in another world where these things were not possible. They could not even imagine Napster and today we are far beyond Napster.

The concept of "filesharing" was readily adapted to characterize the way that music became easily and freely available within global networks following Napster. However, in order to understand the larger phenomenon, we must realize that in recent years "filesharing" has evolved into something more complex and diverse. Legislative initiatives have targeted certain specific characteristics of filesharing. As a result, services that freely distribute media files have been transformed. The most obvious example is streaming video. Furthermore, cultural products, particularly music, were distributed in other ways before Napster.

By introducing the concept of Internet-based Cultural Consumption (IBCC), I am creating a distance to the popular concepts of "filesharing" and "peer-to-peer" to open up for a broader understanding of the way in which all types of cultural products are distributed and consumed within the commercial, black and grey marketplaces. This also makes it possible to see "illegal filesharing" as an evolving phenomenon that today can be seen as an intimate part of the regular commercial marketplace. Cultural products are distributed and consumed on a massive scale in a wide variety of legal, semi-illegal (copygrey services) and illegal genres. All these impact on each other and these effects are not one dimensional. In other words, illegal and copygrey consumption of culture will invariably have effects on the regular commercial marketplace.

Extremely broad concepts are often problematic. However, for some analytical tasks they are essential. By utilizing the concept of IBCC, it becomes possible to discuss:

- All cultural forms of expression (allowing us to be distanced from the specificities of the music industry)
- the needs of the Internet users as a starting point (rather than starting with a commercial special interest group)
- societal, political and transnational contexts
- technological, legislative and economical choices
- social relationships
IBCC, quite simply, enables broader research questions. It becomes possible to investigate the relation between all cultural consumption, cultural distribution ventures in relation to current legislative frameworks. We can ask you questions such as "how does IBCC as a whole respond to legislative pressure?" and "how does that response serve to develop Internet technology?" In other words, it becomes possible to discuss the big picture.

**3.2 The four phases of IBCC**

The development of IBCC is performed in a context of legislative pressure and technological development. It can be characterized as a kind of kind "tug of war"-pattern where legislation and technological development pull, against each other, in opposite directions.

To briefly sketch an overview of IBCC with respect to policy, technical tools and applications, one could see the first phase starting in the mid-80’s as characterized by a strong technological pull. The MP3 codec was invented in 1987, but was not the obvious choice for developers of music playing software such as RealAudio and Liquid Audio. The music industry also worked against MP3 as a standard in several ways as it was difficult to combine with fresh (and seemingly lucrative) ideas on Digital Rights Management. Ideas of reselling the same song with different licenses to the same customer, relied on legislation restricting easy copying in the way that computers now allowed. The World Wide Web was launched in 1991 and the Internet as a whole received a global public breakthrough in the mid-90s.

At the end of the first phase, the revision of the US Copyright Act (DMCA) was passed in 1998 and it has served as a global guideline for national legislation ever since. This was the start of a legislative pull to counter the technological development. However, in this tug of war, technological development is obviously a much stronger contestant. The legislators, working together with strong media anchors, seemed to never realize this. The pattern quickly becomes predictable. As the legislative team makes a concerted, strong pull, technological development quickly jerks back, gaining even more ground. It is, obviously, a losing battle for legislation. Their best option would be to simply concede defeat and ask for a rematch in another sport. The second best option is to stay as firm as possible, in this way losing ground more slowly. Still, the legislative team never catches on. They hope to one time summon enough strength to surprise technology and pull it to its knees.

The second phase started with the launching of Napster (1999) and the new possibilities of large-scale, global filesharing. MP3 emerged as the favored standard for sharing music on the Internet. The phase is characterized by heightened public interest in music, industry panic and litigation as well as quick technological development in which the defeat of the centralized filesharing model of Napster only leads to the creation of a number of decentralized clones, starting with KaZaa. The RIAA spent enormous resources, in this and the following phase, on applying the legal instruments supplied by the Copyright Act and the DMCA in order to scare filesharers into available business models. However, few business models were well functioning at the time.
The third phase is initiated in 2001 with two significant events. First, BitTorrent is created, increasing the possibilities of IBCC manyfold. Together with the continued spread of access to broadband Internet connection, cultural sharing becomes increasingly facilitated. It is now possible to access whole collections of music as easy as one earlier downloaded a song. Increasingly, movies, computer games, literature and various forms of computer software become shared through a number of different filesharing technologies. Second, iTunes is launched in January 2001, quickly developing into the first commercially successful online music store. Others would soon follow. On the policy side, the third phase is characterized by an orchestration of global legislation that serves to implement the main ideas of the DMCA.

The development of diverse systems for sharing on the Internet is today often described as "piracy". This label has also been promoted by a section of the filesharing community, most notably the BitTorrent client The Pirate Bay. However, researchers have often conceptualised sharing systems as part of a new form of economy, the gifting economy (Bays & Mowbray 1999; McGee & Skågeby, 2004; Ripeanu 2006). Although much remains to be done in this area, it is the purpose of this paper to describe the characteristics of a fourth phase which constitutes the evolution of copygrey business as response to the actual outlawing of the gifting economies.

### 3.3 Phase 4: copygrey business

One of the main problems within the legislative drive, that characterized phase 3, was the difficulties of policing millions of users within each national context. The third phase can be said to conclude with the widespread acceptance of a solution to this problem by decentralizing filesharing enforcement from the police to individual intellectual copyright holders. This was based on the popular practice of RIAA to send out massive amounts of "takedown notices" in a way endorsed by the DMCA. In the fourth phase, takedown notices becomes a business area populated by professional takedown specialists. Within the EU, the actual legislation commonly referred to as IPRED (the European Council 2004) allows a copyright holder to police the way that their intellectual property is shared on the Internet.

In the continuation of this article, I am concerned with new business domains that become established following these illegal initiatives. The law is actually saying: if you want to protect your intellectual property, you must do it yourself. At the same time, we are giving you unprecedented legal rights to pursue protective strategies and to generate considerable income this way.

A particular loophole in legislation such as IPRED I (the European Council 2004) and IPRED II (the European Commission 2006) within the European Union, is of the same kind of character as the vulnerability that Napster targeted within the US Copyright Act/DMCA. As this only recognized the problem of site owners who hosted the physical media file, it became difficult to litigate against those that only provided a link. Similarly, IPRED is based on the most popular alternatives of IBCC at the start of the decade. In other words, it is targeted against filesharing, but has little to offer against IBCC solutions where there is no clear linkage between IP address and downloaded media file. Such linking is relatively easy to detect in the earliest forms of filesharing such as Napster, Gnutella and KaZaa. In the police work, all you had to do was join
the network and identify IP numbers of downloaders and uploaders. This has been called "direct detection". As BitTorrent became fashionable, this became more difficult, still a procedure called "indirect detection" was established, made possible by the key feature within BitTorrent technology called "tracker" (Siganos 2009). IPRED is built with direct and indirect detection in mind. However, in recent years, new solutions have been created that obscures this relationship. Users downloading from YouTube, for instance, do so without making a "tracker" available to the surveillance systems. In actuality, it becomes difficult to detect and secure evidence on illegal activities of the advanced users without infringing on their privacy, which would mean breaking the law.

Detection of illegal filesharing/downloading/uploading according to this law would therefore seem to be primarily effective against individuals who lack basic information literacy concerning legislation and protective resources. Users with necessary competence and/or economic resources can easily become too complex targets. This is particularly the case since those that will be policing copyright infringement are likely to be focused on "easy targets" rather than fairness.

I argue that in this new phase/era users will renegotiate their patterns of IBCC. Consumers will be making a choice (or a mix) between three general strategies: White (legal buying); Grey (technologies built on loopholes); or, Black (illegal file sharing with protection against detection). In the remainder of this paper, we will discuss the character of the three domains of the copygrey business.

Very little research has, so far, investigated the structures of what I hear call "the copygrey business". Therefore, much of the source material for what follows consists of Internet-based news material, blogs and information from company websites.

4. The copygrey business

4.1 Three domains

It is still early to be able to fully characterize the new structures and patterns that are evolving. However, I will pursue a model of "copygrey business" that is structured in three domains that are layered upon each other.

The first domain, the core, can be conceptualized as "copygrey services" supplying media files to a large global public beyond the traditional commercial system. These services gather revenue through membership/subscription fees and/or Internet advertising.

The second domain is the "surveillance, obstruction and takedown service" that generates toward copyright holders. Within this domain, commercial actors strive to make it more difficult for the copygrey services to function. Also, it is dependent on there actually being a copygrey service. Much of it would disappear if the legislative system would once and for all defeat the activities of the first domain.
The third domain is here described as "anti-copyright and surveillance services". These are business activities that evolve as response to the existence of the second domain. As the second domain creates difficulties for the first domain, likewise, the third domain attempts to lessen the efficiency of the second domain.

In identifying the three domains of the copygrey business, I will argue that the current policy strategy, basically built on the ancient (pre-Napster) legislation of the Digital Millennium Copyright Act (DMCA) from 1998, follows a trajectory that creates dysfunctional patterns of Internet commerce.

**4.2 The first domain: copygrey service**

A number of diverse business enterprises are today exploiting the illegal copyright infringement. These are established as totally legal enterprises that only serve as intermediaries. It can be made in a number of different ways:

- hosts of uploaded streaming content (such as YouTube)
- hosting linked pages to illegal content
- USENET providers
- uploading services
- supplying recording of streaming content

Here follows a brief characterization of the copygrey service.

**4.2.1 Hosts of uploaded streaming content**

YouTube is the first and still strongest of these services, but it is by no means alone. Others are MegaVideo, Hulu, Justin TV, MySpace TV, Veoh, Yahoo TV etc. Both YouTube and Veoh have been sued and both have come up on top. However, in the case of the latter, it actually meant bankruptcy and corporate takeover. In the case of YouTube, the favorable ruling found that this activity was within "the safe harbor" of the DMCA.

This actually becomes a "safe harbor" for much copyrighted material. At the same time, most major media companies would also utilize them as important tools within marketing campaigns. YouTube is not only a host of streaming content, it is also a social media and a hot bed of fan activity and creative remixing of copyright material. Most major media companies maintain ambivalence toward much of this.

**4.2.2 Upload services**

As peer-to-peer services traditionally have created vulnerability toward detection, many users will switch to services that do not connect individual file sharers with each other. Examples are USENET service providers and uploading sites such as Rapidshare, Megaupload, SendOver, etc. Uploading sites can be utilized in a number of ways. One way is to connect the collections of several users with intermediary copygrey linked sites. Another strategy is to share collections
within a smaller circle of trusted peers, exchanging access keys. These kind of uploading services create new challenges for the practice of detecting illegal file sharing and gathering evidence. The access key serves as an identifier to the media file when uploading and downloading. It therefore becomes difficult for outside observers to grasp what the real content is.

Another alternative to peer-to-peer is the old USENET. Access is usually given through copygrey service providers, such as Giganews, NewsDemon and Supernews, creating their own copies of USENET. While this service is built on rather old technology, the current revival is based on a higher degree of privacy than BitTorrent filesharing. The communication between USENET provider and customer is usually SSL-encrypted, making attempts at detection a matter of privacy intrusion. USENET access is usually sold for about $10/month subscriptions. This is a huge business in itself. There are also satellite ventures discussing and ranking USENET services. One such site, Newsgroup Reviews, supplies information on USENET use and ranks over 100 "premium newsgroup services".

In order to actually download from USENET, it is also necessary to have a newsreader-program. While these historically have been free of charge, the advanced ones are today also business ventures within the copygrey services. The favored newsreader of market-leading USENET provider Giganews is Newsbin Pro, which is currently sold for $35. This does not include advanced searching functionality, which is an added subscription.

### 4.2.3 Link pages

Information on how to access media files in any of the above services, is systematically disseminated through a wide variety of Link pages. YouTube and other suppliers of streaming content will typically host massive databases of both legal and illegal content. However, many services stay away from the controversial area of actually hosting files, but can do well by supplying links. For instance, the popular links site "watchxonline.com" supplies a service in which a huge amount of TV series, movies and pay per view sporting events can be seen streaming at their site. However, all files are stored at other places and imported when the user clicks. The actual user experience is the same as with YouTube. There are thousands of similar sites. Many of them are specialised on a specific kind of content. In addition, there are a multitude of Link sites to Rapidshare and other uploading sites.

### 4.2.4 Copying from streaming media

The actual use of streaming media seems to be an excessively grey area on which there so far does not appear to be a clear legal position since the "fair use" provision in the Copyright Act is difficult to adapt to the complex setting of today. So far, those who have preferred their IBCC streaming have been exempt from litigation. This has made it possible for users worldwide to, for instance, watch a new Hollywood production online before it becomes available at the local cinema.

A further grey area relates to the actual downloading of streaming media. There are a number of both free and commercial products that makes it possible to either download the streaming file
directly or copy it as you watch/listen. The legal convention is currently to view such procedure as "fair use" as long as it is for personal consumption and not shared with others.

This is a crucial loophole that actually makes much of the services of the second domain quite ridiculous. Given the acceptance of "fair use", it is not a matter of the user having a nonpaying IBCC practice. It is, rather, the character of that practice that is at stake. Most clearly, streaming is okay, downloading not. However, if you download from streaming, it also seems to be okay.

This has been recognized by one of the pioneers and market leaders in digital media software: RealMedia. The heading for the homepage of the RealPlayer (Eu.real.com/realplayer) announces the following:

One button. Over 100 million videos downloaded. Download Web videos and watch them anytime, anywhere.

Soghoian (2008) argues that streaming services such as YouTube "has no way of knowing if someone is streaming or downloading a video – as it's simply a case of transferring bits over a wire. If the RIAA or MPPA ever subpoenaed YouTube’s logs, they wouldn't be able to differentiate these uses either" (4).

RealMedia actually goes a step further and also encourages the user to first "create your own video library" in this way, thereafter using RealPlayer to convert and transfer these media files to the mobile, or burn them to DVD and watch them on TV. However, RealMedia is not satisfied with that, but also crosses the conventions of "fair use", which traditionally says it is okay as long as it is for personal use. RealMedia makes the following statement:

Share with friends
Pick a downloaded video from your library and click on the icon for social network you want to share it on (on the envelope icon if you just want to e-mail it). Entertain your friends and show them what you are into!

In this way, RealMedia actually reinvents traditional filesharing.

There are also a number of services that supply "radio rippers". These business ideas exploits the notion of "fair use" in order to supply customers with free music to be saved right on their hard disks. Typically, the customer buys a software or an Internet-based service such as RadioRipper, StationRipper, The Ripper, Streamripper or Chilirec which then allows the customer to pick favorites among hundreds of Internet streaming channels. A wide variety of music is thereafter downloaded on the hard disk, free from any copy restricting features.

Streaming media is probably the key problem for DMCA implementation. It is hardly possible to outlaw streaming media. There are two reasons for this. First, it is already an important marketplace for commercial media corporations. Second, streaming media is a natural extension of the basic functionality of the Internet. Placing a ban on streaming media, would require the destruction of the Internet. That is hardly a realistic alternative.

At the same time, it will be possible to produce copies of streaming media without centralized detection. Game over.
4.3 The second domain: surveillance, obstruction and takedown

The basic services and strategies of the second domain are diverse, but can be categorized according to:

- Surveillance of copygrey services
- Surveillance of uploaders and downloaders of protected material
- Producers of surveillance technology
- Administration of takedown notices
- Producers of media blocking technology
- Providers of obstruction and/or pollution services
- Legal services

All these services need to be performed according to professional standards in order to keep the copygrey services at bay. Some of these activities are developed within large media companies as in-house competence in analyzing the way that the surveillance of copygrey services are using their media. Others are clearly promoting their business on the Internet.

4.3.1 Surveillance services

Some of the companies within the surveillance industry are specialized, such as BanPiracy, which has developed a key competence on the misuse of copyrighted audio software. The largest actor within surveillance services, was for many years MediaSentry. In 2009, this company was merged with MediaDefender, creating Peer Media Technologies. This company uses buzzwords such as: content protection, copyright enforcement and digital piracy measurement services. Peer Media Technologies work broadly within all types of second domain services.

4.3.2 The administration of takedown notices

Many companies involved in surveillance, primarily Peer Media Technologies, are also broad enough to handle the lucrative business of takedown notices. For instance, BayTSP (Tracking-Security-Protection) is a major company in the same business as Peer Media Technologies, but works broader, as "Internet detectives". They file several million takedown notices each year. Still, on the market today we also find takedown specialists.

The administration of takedown notices is actually becoming a substantial business in its own right. Naturally, this is system that gives privilege to the very large companies that are able to finance an effective takedown notice-system. The importance of working with a professional procedure for takedown notices was made clear in a 2004 court ruling. Diebold Inc., a company specializing in the manufacture of electronic voting machines, attempted to silence criticism of their technologies through DMCA takedown notices. The company was found guilty of inappropriately utilizing this legislative instrument. They were heavily fined.
The most prolific takedown specialist is DMCA.com. The company name is a bit ironic as it actually is a kind of "trademark steal" from the well-known legislation. On their website they proclaim the following:

Is someone stealing your content? For just $99 DMCA.com can get it removed. Guaranteed.

You don't need to stand idly by while your website, photos, music, videos or apps are being ripped-off. DMCA.com can get your start in material removed in no-time for just $99, or the refund your money.

While this may seem a cheap offer, these $99 covers an individual takedown notice. As I have explained above, effective takedown procedures need to be both continuous and systematic. DMCA.com offers additional services such as 10% off on additional takedowns and "protection badges" to be placed on the webpage. DMCA.com also view themselves as an alternative to expensive lawyers:

Hiring a lawyer or battling the infringer alone can be an expensive and tedious process. The time it takes for you to get in touch with a lawyer, then it negotiate the fees, and for them to start working on your case could take a few days. Meanwhile, your copyrighted content is being spread around the Internet at a rapid rate!

DMCA.com saves you both time and money. We make sure the content is removed – or you get your money back.

4.3.3 Legal services and media blocking technology

Legal action is very expensive and given the massive amounts of copygrey services involved, they must be used with a sound strategic business sense. Historically, the Recording Industry Association of America (RIAA), has been the driving force in filesharing litigation, making legal claims against a wide diversity of copyright infringements (Bowrey & Rimmer 2005). Since the early 1990s, they have engaged in more than 2000 legal actions each year (Kravets 2010). In 2003 RIAA switched from a strategy of suing filesharing services to instead targeting individual downloaders. Some 18,000 individuals were sued during the years 2004-2008. In December 2008, RIAA announced the end of this strategy. Instead, it was hoped that Internet service providers would cooperate in a new campaign in which copyright offenders would be denied Internet access.

There are interesting developments connected to YouTube, the leader of streaming media and the most obvious targets for takedown notices. At a relatively early stage of the life of this company (founded in February 2005), media giant Viacom sued in March 2007 for $1 billion in damages (Abrams 2010). This seems strange since YouTube already had responded to more than 100,000 takedown notices from Viacom. Although YouTube won the legal battle, it was costly and could even be more damaging in the future. The new YouTube strategy was to install automatic systems for identifying copyrighted music and videos. This "video content identification system" was launched in its Beta version in October 2007 (Anderson 2007). Copyright owners were instructed to feed their material into the identification system, which would then be able to correctly identify copyrighted material even when it only played in the background or constituted a small segment of a large media file. As a side effect, DMCA-critical media, such as lectures by Lawrence Lessig, became unavailable (Abrams 2010).
However, as this was a system particularly developed for and by YouTube, it supplied no universal solution for addressing the many alternative streaming sites. A workable solution would be a sophisticated standard produced by a third-party company (such as MotionDSP or ImageTracker) that supplied a video content identification system that all streaming sites owners would be forced to relate to.

In the absence of such solutions, the business of representing copyright holders in the game of takedown notices can be expected to flourish.

Despite the adaption of an automatic takedown system, Viacom chose to continue its legal battle against YouTube and appealed the earlier ruling in August 2010. This is in many ways surprising, since YouTube is not an ordinary copygrey service provider, but very much big business. As it is backed by the owner, Google, perhaps the most powerful presence on the Internet, one would think that Viacom would risk Internet visibility in this litigation. Wasko & Erickson (2009) points out that YouTube visibility may be related to Google visibility. As of this writing, a Google search on Viacom will yield very high rankings for several articles with the theme "YouTube defeated Viacom". The attempt to destroy one of the world's most popular Web services generates effects on the trademark.

It is possible to foresee the development of another, quite nasty, form of legal business within the second domain: "copytraps". Snow (2009) argues that the excessive fine stipulated in US legislation of a minimum of $750/download encourages companies to create traps for users. It is possible to make much more money in legal action against customers than actually selling to them.

**4.3.4 Obstruction and pollution**

In the third phase of IBCC (discussed earlier), filesharing networks were systematically flooded by corrupt media files (Liang et al. 2005). Pollution companies such as Overpeer and Retspan worked according to a business idea that served to overload peer-to-peer networks with corrupted files. The idea was that filesharers eventually would grow weary and simply buy the media through the legal route. Major record companies redoubled these efforts when releasing a new major record. The strategy was eventually aborted when filesharing services became increasingly adapt in filtering corrupt files as well as developing trust-based systems.

However, with the evolution of BitTorrent, the context of filesharing changed and pollution strategies returned. This time, pollution is performed through what is called "interdiction" companies (Dhungel et al. 2008). MediaDefender, SafeNet and Macrovision emerged as the most prolific business actor in dealing with BitTorrent through a wide range of obstruction strategies. The term that the company itself used was "Internet-piracy-prevention technologies" (mediadefender.com 2007). One successful venture was to create a sabotaging BitTorrent client, ZipTorrent, that sent out false data and registered IP-addresses. Dhungel et al. (2009) identified two different "attack types":

- **Fake-block attack:** fake information was exchanged for an authentic block. The user would only notice this after downloading the entire piece. It was enough to introduce one damaged block in order to corrupt the whole download.

- **Uncooperative-peer attack:** there are many variations of this where certain peers refuses to cooperate with the structure of the protocol, creating delays. One common version is the *chatty peer attack* in which the peer repeatedly engages in the initial handshake procedure so that the download is not initiated. The strategy is to engage the client continuously with the handshaking ritual, but never offer any block for uploading. Another variation is to simply refuse the handshake.

In experiments of downloading a new music album from *Foo Fighters*, Dhungel et al. (2009) found that only 10% were regular "benevolent peers". 18% were "chatty peers" and another 17% refused handshake. In addition, 53% of the peers were not connectable at all. This test supplies an image of a filesharing environment populated to a higher degree by obstructing peers, than benevolent peers.

Another strategy was the so-called "seed attack" which served to attack the seed at an early stage so that it could never gather any momentum (Dhungel et al. 2008). This can be done either by flooding the bandwidth, preventing the legitimate seeds from making requests, or by occupying the majority of the connection slots.

One side effect of these obstructions is that filesharers will increasingly test more files before attaining a playable media. This may lead to increases in the spread of various forms of malicious code. Grizzard et al. (2007) could observe a dramatic rise of malicious botnets that targeted peer-to-peer networks during recent years. Naturally, media files from filesharing networks as well as from copygrey posting services, are ideal vehicles for computer virus.

A strategy that is similar to the methods of producers of malicious code, is to mark up media files through fingerprinting and/or watermarks (Biddle et al 2002). It then becomes possible to identify the originators of the files that were circulating on the Internet. It is, seemingly, an effective instrument. However, as is the case with all copyright protection technology, the advanced users will be able to "wash" media files before sharing and only the less informed will be caught.

### 4.4 Domain three: anti-copyright and surveillance services

Arguably, the growths of domain three services rely on the expansion of the second domain. Given the increasingly aggressive surveillance services on the market, people will react by hiding more effectively. In the following, I will deal with a diverse range of third domain services:

- Proxies
- SSL encryption
- anonymization networks
- Network Address Translation and Virtual Private Network
4.4.1 Proxies
There are large amount of proxy site services available that allows the user to browse the Internet and download content, while seemingly coming from some other place. Many of these are free, but will earn the money through advertisement. Popular services are: The Proxy Bay, Maximum Proxy, BetterUnblock, Proxy 108 and Proxy24.

The obvious problem with proxies are that the user will still leave information with the proxy, making that company a trusted party.

4.4.2 SSL encryption
Copygrey services may offer encryption, as is basically standard for USENET services. However, basic SSL-encryption is vulnerable at the endpoints. There therefore exists a market for strong encryption and software with encrypted data stream. There is a future for freeware such as MEO Encryption Software or Comodo Disk Encryption, and shareware such as High Power Encryption.

4.4.3 Anonymization networks
There are, broadly speaking, two kinds of anonymization networks. First, there are those that provide a higher degree of anonymity to the surfing experience. The most obvious example is Tor. Second, there are anonymous P2P, which are the ones that are particularly relevant in the context of this article.

Examples of anonymization networks are Freenet, MUTE, Entropy, Share and OneSwarm. Many of these are built on a friend to friend expansion, only trusting peers that are already well-known. A number of increasingly advanced network ideas are being developed, such as Crowds and Phantom. There is also a potential of developing this idea for wireless networks which are not built upon fixed Internet connections and Internet service providers.

4.4.4 Network Address Translation and Virtual Private Network
It is possible to masquerade the network address information through network address translation. To the outsider, it may seem that all traffic originates from the Gateway. The potential of building a closed private network for privacy purposes was extended with the development of the Virtual Private Network (VPN). With this system it is possible to create a tunnel between two endpoints. The technology is utilized by a group of filesharers in their development of the commercial application TorrentPrivacy. There are other similar services such as Relakks and Ipredicate, the latter developed by The Pirate Bay.

USENET provider Giganews offers their premium customers VyprVPN, which is billed as a revolutionary and advanced form of VPN.

The diverse services within the third domain are a mixture of commercial business ventures and freely available support. There exist a long-standing popular movement that works to counter all kinds of surveillance, censorship and restrictions to free cultural and political expressions on the
Internet. These movements, including actors such as The Electronic Frontier Foundation, Creative Commons, Free Software Foundation and GNU Project. These actors are usually opposed to the activities within the second domain of copygrey business and will offer various types of support for individuals and institutions.

It is also important to point out that a number of research projects are aimed at developing peer-to-peer services. For instance the BitTorrent client TRIBLER, sponsored by the European Union research system, is a social-based peer-to-peer system with advanced functionality related to social trust which would serve to counter pollution (Pouwelse et al. 2007). Credence, an object reputation and ranking system for filesharing networks, allows users to filter untrustworthy peers (Walsh & Sirer 2006). Others have researched blacklisting strategies and a combination of peer and object reputation systems (Costa & Almeida 2007).

Obviously, these are initiatives that can serve to counter pollution strategies. At the same time, they can function as remedies against viruses, troyans, bots, etc. There have even been research on utilizing peer-to-peer systems as effective instruments for early warning of virus attacks (Janakiraman 2003).

Beyond these institutions and these diverse research initiatives, there is a large amount of commercial enterprises established with the purpose of protecting the Internet user from surveillance. Some of these are mainstream protection instruments, while others are specialized at shielding the first the domain from the enterprises of the second domain.

Anonymizing and cryptology software are beginning to flourish as a response to the expansion of privacy infringing strategies. As surveillance technology is likely to pick up much more than illegal downloading/uploading, large portions of the mainstream Internet users will find it quite rational to utilize services that would obstruct the activities generated by the services of the second domain. This is also a result of the failure of the producers of Web browsers to give priority to sophisticated privacy settings at the cost of restricting information to advertising companies and third-party information data miners, such as DoubleClick. This conflict became evident at the launching of Internet Explorer 8, where the advanced privacy settings of the Beta version – a competitive edge against Mozilla Firefox – were removed for the finished product.

### 4.5 A fourth domain?

I have attempted to demonstrate interconnectedness between the different domains, arguing that the business opportunities within one will occur due to sophisticated developments within another. Within all three domains, sophisticated professional services are developed that require a high degree of specialization.

It is also possible to identify a fourth domain, with the earmarks of "white business". These are a number of businesses that has been able to expand on a massive scale due to the emergence of filesharing services. I refer to those producing and selling personal computers, broadband connection, CD/DVD burners, hard discs and similar products. Historically, the need for
extensive bandwidth, high speed, sophisticated copying equipment and huge hard disc capacities have to a large extent been motivated by illegal filesharing.

5. Closing discussion

As Sell & May (2001) argues, every settlement within intellectual property rights changes the rules of the game. In a sense, "reality kicks back" against heavy-handed and one-sided legislation. Initiatives such as TRIPs and the DMCA are, in addition, ancient by today's standards. The three domains of the copygrey business are their responsibility, their offsprings. The actors within the second domain are fond of portraying themselves as "the good guys" hunting down criminals. However, the copygrey services are a response to that mismatch between ancient legislative ideas and the technologies and practices of the new millennium. It must be the task of the creators of media to adapt to the technology of the times and build commercial ventures in that context. They should not be allowed to force the consumers into the business models of the old millennium.

It is not surprising that multinational companies will attempt to monopolize. However, these demands clearly stifle the creativity and entrepreneurialism of the new generations. That is bad for any country. Policymakers should take the long view and circumvent the current trend of strong intellectual property on the Internet.

In addition, this is legislation that is currently monopolizing Internet policy and therefore restricting the strategies of other policy actors. The current development of the copygrey business domains is very troubling for all concerned parties. Within all three domains, the natural patterns of Internet behavior are being skewed. In addition, all domains are seemingly expanding. This means that the instruments of surveillance are likely to become more sophisticated which in turn will increase the paranoia within the customers of the copygrey services. This would in turn lead to an expansion of the third domain. Increasingly, the Internet appears to become a place where it is okay for some private individuals/companies to track the information behaviors of other users. As "information is slippery" and as many corporations tend to renegotiate privacy agreements (see for instance the AOL search data scandal and the release of personal identification data to advertisers from Facebook (Prater 2010)), many users will start to establish Internet patterns according to the idea that their information behavior is in the public, rather than the private, domain.

The current article has been aimed at describing the three domains of the expanding copygrey business. It is a business sector that really didn't exist a few years ago. As it stands, the sophisticated user will be able to utilize a wealth of instruments from the third domain in order to make both tracking infringement and collecting evidence very difficult. Similarly, users with a lesser degree of competence will become easy prey for the services of the second domain. As the legal situation today is interpreted differently by various actors, the situation for ordinary citizens is very confusing. On the one hand, we are told that consuming culture without paying is like stealing. The most extreme standpoint is that it is criminal to make copies of music that you have bought (Bangeman 2007). On the other hand, mainstream companies, such as RealMedia, encourages massive downloading.
References


DMCA.com (2010).


European Commission, the. (2004). The EU strategy for enforcement of intellectual property rights in third countries. Available at: The EU strategy for enforcement of intellectual property rights in third countries. Available at:


Real Media (2010). Eu.real.com/realplayer


