

# Vicarious Infringement Creates a Privacy Ceiling

Janice Y. Tsai  
Carnegie Mellon University  
jytsai@andrew.cmu.edu

Lorrie Faith Cranor  
Carnegie Mellon University  
lorrie@cs.cmu.edu

Scott Craver  
Binghamton University  
scraver@binghamton.edu

## ABSTRACT

In high-tech businesses ranging from Internet service providers to e-commerce websites and music stores like Apple iTunes, there is considerable potential for collecting personal information about customers, monitoring their usage habits, or even exerting control over their behavior - for example, restricting what can be done with a purchased song. A privacy ceiling is an effective limit to these privacy intrusions, created by the perceived or actual legal liability of possessing too much information or control. As we show in this paper, the risk is not simply that of customer backlash, but liability for a customer's actions, owing to the ability to identify, report, or prevent them from taking those actions. In some cases high-tech businesses have been obligated to divulge their store of personal information or to police their customers at the demand of third parties; this unwanted result derives from the possession of too much information or control for the company's own good. We argue that vicarious infringement liability in particular creates a privacy ceiling, a point beyond which there is no economic incentive to intrude on a user's privacy; and, indeed, there is an incentive to architect one's business so that such intrusions are difficult or impossible.

## Categories and Subject Descriptors

K.4.1 [Computers and Society]: Public Policy Issues—*Intellectual property rights*; K.5.1 [Legal Aspects of Computing]: Hardware/Software Protection—*Copyrights*

## General Terms

Privacy, Digital Rights Management

## 1. INTRODUCTION

A privacy ceiling is a practical limit to privacy intrusions, such as monitoring and the collecting of personal information, created by the perceived legal liability of possessing that information. As we show in this paper, the risk is not

simply that of customer lawsuits, but liability for customer actions, owing to the ability to identify, report, or prevent those actions. The temptation to collect as much information as possible is an easily implemented (and profitable) one to which to succumb. A privacy ceiling can be created by several hazards, one of which is the liability associated with being sued for vicarious infringement of copyright. Many technologies deal with digital content, and the ways the technology providers monitor and control the usage of digital material may subject them to vicarious liability. The economic disincentive posed by legal liability provides a significant reason for technology providers to be cognizant of the levels of privacy they afford in their products. We examine these issues of privacy in the context of digital rights management (DRM) technologies and expand our observations to include all content-related technologies.

Due to the ability to easily transfer and copy digital materials, copyright holders and data owners try to protect their content by restricting the unauthorized use and dissemination of their work by implementing various technologies for digital rights management (DRM). To be effective, these DRM methods sometimes track personal information and the usage of the media that they protect, as well as enforce usage rules. The use of DRM technologies has several privacy implications, and these technologies “represent an effort to reshape the practices and spaces of intellectual consumption” [28]. Since these technologies restrict the use of content, they may restrict legally permitted use of that content as allowed by copyright law. Businesses may apply their own usage regime on top of the existing legal framework; one common example is that of user operation (UOP) blocking on DVDs, which can prevent a user from fast-forwarding during movie previews by temporarily disabling that feature on the DVD player itself.<sup>1</sup> This DRM restriction, which helps fulfill the advertising agreements made with the movie studio, is not related to preventing copyright infringement or any other illegal act.

Ironically, the monitoring and control exerted by DRM technologies may open companies to lawsuits based on al-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

DRM'06, October 30, 2006, Alexandria, Virginia, USA.  
Copyright 2006 ACM 1-59593-555-X/06/0010 ...\$5.00.

<sup>1</sup>UOP blocking is detailed by Gwen Hinze in “Post-Hearing comments of The Electronic Frontier Foundation” (<http://www.copyright.gov/1201/2003/post-hearing/post10.pdf>). Hinze observes that UOP blocking is apparently a requirement for licensing the official DVD logo. The official requirements are only available under a non-disclosure agreement, but test specifications available online show tests for UOP blocking ([http://www.dvdfllc.co.jp/forms/TS\\_Video\\_plyr\\_V114\\_June2005.zip](http://www.dvdfllc.co.jp/forms/TS_Video_plyr_V114_June2005.zip)).

legations of the vicarious infringement of copyright. If a company has information on users, it could be compelled not only to surrender that information, but also to periodically act on it to prevent or report certain behavior. If a company exerts control over users, a third party could reasonably demand more or different controls on the grounds that the company has the machinery already in place to enforce them. This challenges the idea of a consumer-friendly DRM system that seeks to strike a balance between content providers and customer rights; if such a DRM system is in place, a content provider can simply demand that it be made stricter lest the company face the specter of litigation. This liability may be an economic incentive for businesses to adopt more privacy-friendly technologies. Technology providers need to take into account that “turning a blind eye” or failing to do anything at all when implementing systems of control is not a viable defense. The threat of vicarious liability suggests concrete standards for the architecture and design applicable to technologies beyond DRM technologies.

Beyond DRM, companies may simply monitor their customers’ behavior for purposes of market research, or simply because their business architecture naturally incorporates the possession of private information or usage behavior. A centralized music store, for example, may naturally archive its transactions with its customers. This information, if too detailed, may also make a company liable on the grounds that it could identify and report infringers if only it simply processed that information. Finally, companies which neither restrict users nor collect much information could still face liability if it is easy to do so, given their architecture.

We discuss privacy intrusions and the privacy ceiling in the next section. Vicarious infringement, as defined by recent court decisions, is examined in detail in Section 3. Finally, we recommend design principles based on the privacy ceiling in Section 4, and conclude in Section 5.

## 2. PRIVACY INTRUSIONS

One definition of privacy relates to personal autonomy, or the “freedom from official regulation” [37]. This zone of privacy “consists of ‘personal rights’ that can be deemed ‘fundamental,’ that are implicit in the concept of ordered liberty.” With the ability to decide one’s actions for one’s self, people retain a certain amount of freedom from intrusion. This freedom from regulation deals with both the monitoring and surveillance of actions as well as the control or restriction of those actions. These are the two intrusions of privacy that we focus on below.

### 2.1 Types of Privacy Intrusions

#### 2.1.1 *Intrusion 1: Usage restrictions*

Individuals have an expectation of privacy in their own homes. Whether it be reading a book or tearing that book to shreds, the “rules and traditions about freedom within private spaces ... [provide] guarantees of breathing space for individual behavior” and “privacy rights” in the “breathing space for thought” [28]. This philosophical view of privacy is concerned with **intellectual consumption** and **intellectual exploration**, or the freedom to think and act in one’s own space.

Usage restrictions imposed by technology intrude into this private space by forcing a consumer to change how they be-

have with their media content [29]. This may include purchasing a music disc only to find that one is unable to access the music due to hardware restrictions, or unable to transfer that music onto a music player. These usage restrictions “shift the baseline conditions of user autonomy to determine the circumstances of the use and enjoyment of intellectual goods” [29]. The limiting of private behavior, or how one acts in a private space, is a means to restrict personal freedoms, even if those freedoms may have been permissible with the content in a different format or in a previous iteration of the content.

#### 2.1.2 *Intrusion 2: Monitoring*

Monitoring encompasses both the collection of personal information, and the observation of customer’s behavior as he or she uses a product. It is difficult to “act naturally” knowing that this physical monitoring is taking place. Technology, unfortunately, makes it easier to forget that the same type of monitoring is occurring digitally. Websites and e-commerce sites also seek to collect as much information as possible about a consumer. In general, monitoring raises “troubling privacy concerns” and creates “opportunities to police and limit behavior occurring in private spaces” as well as “subtly shap[ing] behavior, expression, and, ultimately, identity” [28].

Technology can track consumers’ actions in very fine and precise detail. For example, DRM technologies can record “the content used, the time of use, the frequency of use, and the location of use” [45]. This level of surveillance can be used to create profiles about the habits and preferences of users, leaving them with no control over any of the information that has been collected about them or what is done with that information. Based on how this information is used (by the content supervisor and, potentially, third-parties), these systems “have the potential to change, dramatically, the way people experience intellectual goods” [28].

Apple iTunes provides an interesting example of pervasive monitoring. iTunes 6.0.2 introduced the iTunes MiniStore. When the MiniStore is open, it makes recommendations on similar music available for purchase from iTunes based on the songs initiated with a “double-click” [43]. To make this recommendation, iTunes sends data back to Apple about the song as well as “a string of data that is linked to a computer user’s unique [Apple] account ID” [25]. This Apple ID is the ID used for the iTunes Music store and other Apple accounts and services. “The Apple ID can therefore be linked to your credit card, your address, and your purchasing habits with Apple” [25]. Due to customer concerns about their privacy, Apple added a notification in the iTunes software stating, “As you select items in your library, information about that item is sent to Apple, and the MiniStore will show you related songs or videos” [26]. Additionally, they inform customers that it will not “keep any information related to the contents of your music library,” and it redesigned the iTunes interface to make it easier to turn off the MiniStore, making the MiniStore an “opt-in” feature [26].

### 2.2 DRM Technologies

An example of technology that incorporates the previously mentioned privacy intrusions is digital rights management (DRM). DRM typically refers to technologies that are used to “manage consumer uses of copyrighted content” [13]. Music, movies, and art can be easily copied and shared when

they are available in digital form, making it difficult for the artists or creators to retain control over their work. Due to these concerns, DRM technologies typically favor the content or copyright owners who are seeking to limit the unauthorized use of data or the infringement of content. These technologies enforce or oversee data usage in several ways, typically employing the functions of constraint and monitoring [28]. Technologies that focus on constraint “impose direct restrictions” [28] on consumers’ use of digital content. For example, the technology included on a music compact disc (CD) may not allow purchasers to play that CD on their computers, or it may prohibit them from uploading the music onto their portable music storage devices [48]. Other DRM technologies may be designed to “report back to the copyright owner on the activities of individual users” [29], monitoring the use of that content and the user. An example of monitoring would be an application for downloading digital music from a music service where the DRM software reads information about “cookies or browsing history,” and transmits this information to the music service even when the application is idle, suggesting that the music service is monitoring user browsing habits [45] in addition to tracking the music downloaded by the user. DRM systems are specifically engaged in “detailed surveillance of content consumption by consumers within private spaces” [28].

Constraint and monitoring are accomplished in several technological manners: with DRM metadata for digital content, by tying content to a device, and by tying the rights of the digital content to the user [33]. In the DRM metadata method, the digital content is formatted so that it may be accessed only with a specific application or software program. Monitoring may occur when the user goes to a website to obtain or download the content. That software may even be designed to continually monitor general operations on that computer and send that information back to the digital content provider. By tying content to a device, content owners make digital content inoperable with other devices. In this scenario, users may have to provide the serial number of the device to the content provider in order to obtain permissions or authorization to use the content. Constraint and monitoring are both functions of this type of technology. To use the content with the device, “ongoing, periodic contact” is required between the user and the content provider [33]. This contact may be monitored or tracked, connecting the user to both the device and the content. If this contact cannot be initiated, the device will constrain the use of the content. Due to its monitoring capabilities, DRM technologies may collect information on other infringing practices, even if that DRM technology is restricting the use of other content. The privacy implications of DRM applications “weigh heavily against expectations of personal use” [45].

## 2.3 Risks and Consequences of Privacy Intrusions

The types of privacy intrusions listed above can incur several negative consequences, which we argue create a privacy ceiling. These include consumer backlash, the reduction of the value of the product, and legal liability for the technology vendor or provider. We describe some examples of risks and penalties from privacy intrusions. We will discuss the liability of vicarious infringement in detail in Section 3.

### 2.3.1 *The Sony Rootkit Controversy*

A recent example of a technology company running afoul of the privacy ceiling involves the Sony BMG Music Entertainment group in what has become known as the “Sony CD copy protection controversy” or the “Sony DRM Rootkit controversy.” Sony BMG employs two DRM systems, XCP and MediaMax, to control the playing, copying, and transferring of music from their CDs [36]. Just prior to the controversy, these systems led to the reduction of value of Sony BMG products when consumers realized that they were unable to transfer music from their CDs onto their iPods. The complaints of consumers and the recording artists led Sony BMG to provide consumers with instructions on how to work around their XCP technology to remedy the iPod incompatibility [9]. These grumblings about the DRM technologies became a roar in the fall of 2005.

In October 2005, a software engineer was running a security scan on his computer and discovered that a CD released by Sony BMG had installed a “rootkit” onto his computer [47]. Rootkits are computer programs “designed to hide evidence of a system intrusion” [34]. Once the rootkit is installed, malicious agents can deploy computer viruses to take advantage of this introduced vulnerability on music listeners’ computers. To make the copy protection strong enough to deter copying, First4Internet (XCP) and SunnComm (MediaMax) employed techniques that acted in ways that would classify them as spyware. Upon further investigation, computer scientists discovered that both types of DRM systems monitored the CD-playing habits of users when the software is installed, contacting the vendor when protected discs were inserted. While the purpose of this contact was to obtain “images or banner ads to display, ... these connections allow[ed] the servers to log the user’s IP address, the date and time, and the identity of the album” [36]. First4Internet and SunnComm do not mention the intended usage of this information nor do they mention the collection and control policies for this information. Sony’s use of DRM technologies allowed its DRM vendors to install software without the informed consent of the consumer, and it also compromised the security of its users’ computers.

As a result of the consumer backlash over the privacy and security risks introduced by their music purchases, Sony BMG halted the production of all CDs employing XCP copy protection [32], and recalled the 4.7 million XCP-protected CDs [24]. Sony BMG’s privacy disruptions were alleged to have violated laws in several states regulating spyware and data collection, and this legal liability led to lawsuits in Texas, California, New York, and Italy [14]. Sony BMG settled the class action lawsuit at a cost in the “single-digit millions of dollars” [53], and the settlement requires them to cease manufacturing “Sony BMG CDs with XCP or MediaMax ... software” [23].

### 2.3.2 *Google - Search and Seizure*

The risk of user monitoring was highlighted by a trial in November 2005, illustrating potential consequences should a technology company monitor and store information that may later be used against a user. In a murder trial in North Carolina, prosecutors presented a man’s Google search history containing the words “neck snap break” and “hold” as digital evidence in the killing of his wife [38]. While the evidence did not come directly from his Google search his-

tory, it would have been entirely possible for prosecutors to request that information from Google, and within Google's legal obligation to provide that information to law enforcement officials. This scenario implies that if a technology company or service can collect information from and about its users, that information may be used against users in the future.

### 2.3.3 *Verizon and Disney*

In September 2005, Verizon Communications and the Walt Disney Company reached an agreement by which Disney will license its television and broadband services and content to Verizon in exchange for Verizon's assistance in cracking down on copyright infringement for Disney [8]. When Verizon broadband customers are identified by Disney as "unauthorized copiers of Disney content," Verizon will "forward and track notices" to the alleged infringers [8]. It may also terminate the service of Verizon customers who continue to infringe despite multiple notices. To protect the privacy of its customers, Verizon will not identify the subscribers to Disney unless they have been served with a subpoena.

This agreement between Verizon and Disney sets an interesting precedent. Verizon's primary purpose is to provide Internet services rather than act as copyright enforcement agents. But, since they monitor their users, they have become responsible for tracking their subscribers and serving them with notices of infringement. These actions may require additional costs to maintain their server and traffic logs for an unspecified amount of time as well as keeping records of users to whom they have served notices.

The situation also raises other questions. If Verizon will help Disney to stop the infringement of their works, will it be obligated to help the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), or other content owners notify potential infringers to cease and desist? Based on the cost to Verizon and the response by its consumers, Verizon will need to decide how to best deal with preserving its customers' privacy despite the constant monitoring implied in the agreement reached by Verizon and Disney. It is an interesting turnaround in events since Verizon fought the RIAA in releasing subscriber information, with the U.S. Court of Appeals for the District ruling that subpoenas cannot be issued without judicial consent [30]. Verizon and Disney's agreement also raises doubts about the "safe harbor" provision of the Digital Millennium Copyright Act, that allows an Internet Service Provider (ISP) to avoid copyright infringement liability [4]. Many ISPs (Verizon, Comcast, AOL) are becoming entire media conglomerates, providing Internet connectivity, telecommunications functionality, and even media delivery services; it is not clear if safe harbor provisions apply to them.

In the remainder of this paper, we focus on the legal liability for vicarious infringement and its role in creating a privacy ceiling.

## 2.4 The Privacy Ceiling

The privacy ceiling is defined as the point beyond which it is no longer profitable for companies to monitor or control their users. The following considerations discussed previously create a privacy ceiling:

- The cost of monitoring or control;

- The reduction in value of a product;
- Consumer backlash; and
- Legal liability, including that of vicarious infringement.

## 2.5 Examples of Privacy Ceilings

Government policy has resulted in several examples of privacy ceilings. In these cases, the technology or information vendors seek to not have private information of its users so that they are not put into positions of liability.

### 2.5.1 *Don't Ask, Don't Tell*

"Don't Ask, Don't Tell" is the name of the policy established by Congress in the FY 1994 Defense Authorization Act that allowed people with homosexual sexual orientations to serve in the armed forces. While the United States military prohibits homosexual conduct, and anyone who is found to have "engaged in, attempted to engage in, or solicited another to engage in a homosexual act" or "stated that he or she is a homosexual or bisexual"<sup>2</sup> will be separated from the armed forces. The "Don't Ask, Don't Tell" policy allows homosexuals to serve in the military as long as they do not disclose or act upon their homosexual orientation.

This policy is an example of a privacy ceiling. Commanders are expected not to inquire about sexual orientation, and as long as servicemen do not openly display or disclose their sexual orientation, the military will make no effort to monitor or to discover evidence of homosexual acts [46].

### 2.5.2 *Children's Online Privacy Protection Act*

Similarly, the Children's Online Privacy Protection Act of 1998 (COPPA) is applicable to operators of websites or online services directed at children or "any operator that has actual knowledge that it is collecting personal information from a child" under the age of 13.<sup>3</sup> To comply with COPPA, website operators must first do the following before collecting information from children under 13:

- Provide a privacy policy on the website detailing what information is collected and the operator's intended use and disclosure practices;
- Obtain verifiable parental consent;
- Allow parents to review the information provided and prohibit its further use;
- Prohibit the use of a game or incentive to gather "more personal information than is necessary;" and
- Create procedures to protect the information that is collected.

To avoid determining the ages of all of the individuals visiting a site or "knowingly" collecting information from children, some website operators have instituted a policy of not collecting information from children.<sup>4</sup> This self-imposed privacy ceiling allows them to avoid the expense of compliance with COPPA.

<sup>2</sup>Title 10, U.S.C. Sec. 654, "Policy concerning homosexuality in the armed forces."

<sup>3</sup>15 U.S.C. 6501-6506, P.L. No. 105-277, 112 Stat. 2681-728.

<sup>4</sup>For example, the Privacy Policy of the Food Network states, "Our websites are not designed for use by chil-

### 2.5.3 Libraries and the USA PATRIOT Act

Another policy-instituted privacy ceiling deals with the data retention polices of libraries and the USA PATRIOT Act. According to the Library Bill of Rights enacted by the American Library Association (ALA), libraries have a “responsibility to provide information and enlightenment” by providing access to “materials and information presenting all points of view” [17]. The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) was enacted in 2001 following the September 11, 2001, terrorist attacks in the United States. It altered the “scope of subpoenas for records of electronic communications” and access to records and other items under the Foreign Intelligence Surveillance Act” [15]. The Act had the effect of expanding the authority of government officials and law enforcement to gain access to electronic evidence and communications, including library records [18]. The ALA was concerned that this access to library records was a “present danger to the constitutional rights and privacy rights of library users” [20] and recommended that libraries adopt a privacy ceiling.

The ALA recommended that the collection of information “only be a matter of routine or policy when necessary for the fulfillment of the mission of the library” [19]. To fulfill this recommendation and to avoid the monitoring of patrons, many libraries keep a “minimum number of records necessary for maintaining records” [41], deleting records after materials have been returned. By expunging these records, libraries do not have knowledge of what information is being sought by patrons, and they reduce the burden of having to monitor or control access to information.

### 2.5.4 Google in China

Google has created a privacy ceiling for itself in its deployment of technology to China. In January 2005, Google announced that it would provide a censored version of its Google search engine for China [10]. Other competitors such as Yahoo! and Microsoft already have a technology presence in China, obeying the rules and regulations of the Chinese government. Microsoft has been criticized for censoring Chinese bloggers who use the words “freedom,” “democracy,” and “demonstration” in their entries on its blogging service MSN Spaces [12]. Yahoo! has been criticized for being responsible for the imprisonment of a Chinese dissident after it provided email information to the Chinese government [40]. Due to Google’s concerns about the “privacy and security of users’ sensitive information,”<sup>5</sup> Google decided not to offer its Gmail e-mail or Blogger blog services when it launched Google.cn [44]. In this way, their privacy ceiling prevents them from monitoring users’ emails or blog posts, and therefore, Google is unable to provide any e-mail or blog informa-

tion without their parent’s supervision. We ask that anyone under the age of thirteen not submit any personal information through our websites. We do not knowingly collect any personal information from children under the age of thirteen, and therefore we do not knowingly distribute such information to third parties.” [http://www.foodnetwork.com/food/privacy\\_policy](http://www.foodnetwork.com/food/privacy_policy).

<sup>5</sup>These concerns were voiced by Elliot Schrage, Google’s vice president of communications and public affairs before the Committee on International Relations, United States House of Representatives on February 15, 2006. <http://googleblog.blogspot.com/2006/02/testimony-internet-in-china.html>.

tion when asked. In addition, they have moved the servers that store search records out of China to reduce the possibility of being required to hand the records over to the Chinese government [11].

## 3. THIRD PARTY COPYRIGHT LIABILITY

Third parties may be held liable for copyright infringement based on their relationships and interactions with the infringers. The main causes of this liability are vicarious infringement, contributory infringement, and inducement. To be liable for contributory infringement, an entity must have knowledge of and provide some direct assistance for the infringing act [54]. Specifically, “one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable” [1]. Additionally, secondary liability is assigned if an entity induces infringement by “distributing a device with the object of promoting its use to infringe copyright” [50].

In this paper, we specifically focus on the impact of vicarious infringement; however, it is worth pointing out that contributory and vicarious infringement claims are often made together.

### 3.1 Vicarious Infringement

Vicarious copyright liability is based on the principle of *respondeat superior*, Latin for “let the superior answer” [3]. It indicates that an employer (principal) is “liable for the wrong of an employee or agent if it was committed within the scope of employment or agency” [3]. The landmark case that “provides the modern definition of the doctrine” [54] is *Shapiro Bernstein and Co. v. H.L. Green Co.*, 316 F.2d 304 (2d Cir. 1963) [49]. Here, vicarious infringement dealt with the liability of the owner of a department store whose employee, a concessionaire, was selling counterfeit recordings. The court found that the department store owner Green was liable for infringement even though he had been unaware of the selling of the counterfeit recordings. It reasoned that the “imposition of vicarious liability” was “neither unduly harsh nor unfair because the store proprietor had the power to cease the conduct of the concessionaire, and because the proprietor derived an obvious and direct financial benefit from the infringement” [49].

Another case that has expanded the scope of third party liability was *Fonovisa v. Cherry Action*, where Cherry Auction was found liable for both contributory and vicarious infringement. At the Cherry Auction swap meets, some vendors rented booths to sell copyright infringing music recordings. The court found the requirement of contributory infringement met once Cherry Auction provided the “means” to infringe by holding the swap meet. Additionally, the indirect financial benefit to Cherry Auction from having infringing vendors and its ability to terminate a vendor was enough control for vicarious liability to be established. It is this more stringent evaluation of secondary liability that is now applied to current copyright cases involving technology vendors.

### 3.2 Legal Requirements

Vicarious liability has evolved from an employee infringing on copyright while using employer resources to include consumers using technology at home to infringe on copyright. While the circumstances may have changed, the rulings of

the courts continue to be based on the following requirements:

- **Direct Infringement:** someone has infringed on copyright in some manner;
- **Supervision:** the accused has the “right and ability to control and supervise the underlying direct infringement” [22]; and
- **Direct Financial Benefit:** the accused has or receives a “direct financial benefit” from the infringement [42].

### 3.3 Court Cases

Peer-to-peer file sharing services have been brought to court for charges of vicarious infringement, and the decisions in these cases have set the precedent for digital copyright liability. The major court cases that have defined the scope of the guidelines for digital content in this context include the following:

- *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 57 U.S.P.Q.2d (BNA) 1729 (9th Cir. 2001);
- *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003); and
- *Metro-Goldwyn-Mayers Studios Inc. v. Grokster, Ltd.*, 75 U.S.P.Q.2d (BNA) 1001, 2005 WL 1499402 (U.S. 2005).

#### 3.3.1 Napster

Originally released in 1999, Napster was an online music sharing service that changed the way that people were able to share music with others, signaling the “emergence of a new Internet distribution channel” not controlled by the music industry [27]. Instead of going to a music store and buying a physical Compact Disc (CD), consumers could make digital copies of individual tracks and compress and encode the music into what is known as an MP3 file. Napster facilitated a peer-to-peer (P2P) computer network which allowed users to do the following:

- Make files stored on individual computers available for copying by other Napster users;
- Search for files on other users’ computers; and
- Transfer copies of files to their own personal computers [22].

In a P2P network, the computers connect directly to each other, so that each computer is both a server and a client. When users logged into the Napster system, the Napster software uploaded the names of that user’s MP3 files to a central server to allow for indexing of the files and searching. In this way, users of Napster’s software could share copyrighted music files with other users or allow other users to “pirate” copyrighted music. Before it was brought to court, Napster was a free service that supported itself solely on venture capital [16].

In the *Napster* case, record companies filed suit against Napster, alleging violations of copyright law pertaining to the contributory and vicarious infringement of music. The Ninth Circuit Court of Appeals upheld the lower court’s

analysis of the vicarious infringement charges against Napster, finding Napster vicariously liable because the following requirements were met:

- **Direct Infringement:** Users were, in fact, downloading copyrighted music files;
- **Supervision:** Since Napster had the ability to block users from particular environments and the right to refuse service and terminate accounts as noted in their Terms and Conditions, they had the “right and ability to supervise its users’ conduct.” Due to its “search function” and the “file name indices,” Napster had the “ability to police” its systems and to detect infringers [22]; and
- **Direct Financial Benefit:** Despite the fact that Napster was not generating revenues, a financial benefit existed when the availability of infringing material “acted as a ‘draw’ for customers,” and evidence showed that Napster’s [future] revenue was dependent on “increases in userbase” [22].

The most significant, far-reaching, yet ambiguous portion of the Ninth Court’s decision stated that “Napster... bears the burden of policing the system within the limits of the system” [22]. We will examine the implications of this provision on other technologies in Section 4, Recommended Design Principles.

#### 3.3.2 Aimster

Aimster (renamed Madster during the court proceedings) was another P2P service that allowed users to share files over an “instant messaging” (IM) service. The “Aim” in Aimster is a reference to the AOL Instant Messenger service. Users can add others to their “Buddy Lists” and share files with each other when both users are connected to the IM service at the same time [2]. Aimster encrypted the communications between “Buddies,” allowing the developers of Aimster to state that they had no knowledge of what files were being shared between users.

The record companies filed suit against Aimster, alleging charges of contributory and vicarious infringement of copyrighted music [42]. The Seventh Circuit of Appeals found that Aimster was liable for copyright infringement. The analysis of the case focused mainly on the charges of contributory infringement, finding the following: Aimster did not have any noninfringing uses; and Aimster encouraged the downloading of copyrighted music, thereby having specific knowledge of specific infringing uses.

The Court also implied in their decision that “One can be liable for vicarious copyright infringement even without knowledge of the infringement” [31]. Again, the three requirements for vicarious infringement must be met, and the “lack of knowledge” of infringement is not a sufficient defense against liability.

#### 3.3.3 Grokster

Grokster, Morpheus, and KaZaA are other P2P software companies with products that allowed users to share music and movie files with others by connecting them to the FastTrack and Gnutella P2P networks. These services did not contain a central server to index the files on the network and advertised themselves as post-Napster alternatives. The

entertainment industry sued the makers of these P2P products for contributory and vicarious infringement. While the P2P companies did not receive any revenue from users, they did generate income by selling advertisements that they displayed to their users.

The Ninth Circuit Court concluded that *Grokster* could not be held liable for vicarious infringement, but the Supreme Court reversed the Ninth Court’s judgment, defining an additional standard for infringement related to the *inducement* of copyright violations.

The Ninth Circuit originally found *Grokster* not liable for vicarious infringement based on the following:

- **Supervision:** *Grokster* did not have the “ability to block access to individual users,” and that there was not a “point of access for filtering or searching for infringing files” [51].

While the entertainment companies argued that *Grokster* should not escape their vicarious liability by turning a “blind eye” to the infringing practices of its users, the Ninth Court found that the “possibilities for upgrading software located on another person’s computer are irrelevant to determining whether vicarious liability exists” [51]. Thus, the Court emphasized that the defendants were not liable for vicarious infringement and had no obligations to redesign their technologies so that they could supervise their users.

In June 2005, the Supreme Court reversed the Ninth Court’s judgment, finding *Grokster* liable for copyright infringement. The *Grokster* court re-emphasized the legitimacy of secondary liability. The Supreme Court also included another standard with which to determine copyright infringement. This is the *inducement rule*, where “one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties” [50]. This “inducement” overwhelmed the other charges of secondary liability, and *Grokster*’s use of advertisements and solicitations [31] for its service indicated that they intended for the infringement to occur.

### 3.4 Privacy and Vicarious Liability

The disruption of privacy by surveillance may subject technology providers to charges of vicarious infringement. Vicarious infringement does not only effect vendors of DRM technologies alone; any other technology that also monitors users or the data that they access may have collected information about user’s infringing tendencies, even if that is not their primary purpose. If technology vendors do not have the intent to infringe, nor do they advertise or imply any infringing purposes, the decisions in the previously mentioned court cases can still apply to that technology’s use. If a technology is deployed to control and monitor consumers, it may make the distributor liable for vicarious infringement under the definitions set forth in the law.

The Recording Industry of America (RIAA) has shown that they are ready and eager to pursue lawsuits. Serving lawsuits to alleged infringers (individuals) has become the chief method by which the RIAA seeks to reduce the infringement of music files. As of June 2006, the RIAA had filed over 18,000 lawsuits [39], against individuals for illegally downloading and distributing copyrighted music on the Internet. Thousands of these cases have been settled

outside of court, and the fines that individuals are required to pay in the settlement range from \$4,000 to \$5,000 [21], substantially reduced from the maximum fine based on \$750 per song infringed. The RIAA has created an environment ripe for lawsuits against larger and richer entities. With the *Grokster* decision, “legal clarity has decreased, and the risk of litigation has increased,” said Michael Petricone, vice president of technology policy for the Consumer Electronics Association [35].

As mentioned in the Supreme Court *Grokster* ruling, “when a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement” [50]. The court has framed vicarious infringement in such a way that it is possible that organizations, such as the RIAA, could begin to target technology providers or designers, rather than only going after the individual infringers. Technology companies are already subject to significant amount of legal arbitration for matters related to copyright. Based on the 2005 Fulbright Litigation Trends Survey [6], technology/communications companies were the “most frequent subjects of arbitration filing.” Technology/communications companies were more likely to have a legal budget of 2-5% of their company’s gross revenues. Mid-sized companies, including technology/communications companies, “rated intellectual property matters as their most expensive on average.” Thirty-three percent of technology companies listed intellectual property as their biggest concern in the future. The average cost per intellectual property matter resolved by a technology company was \$151,000 dollars. On average, it took a technology company 324 days to resolve an intellectual property dispute.

Litigation has a significant effect in the development and deployment of technologies and services. Since the recent *Grokster* decision added liability via *inducement* to consider when making copyright claims, it “increased the legal uncertainty around innovation substantially and created great opportunities to defeat legitimate competition” [7]. Designers of technology must consider the legal ramifications of their products before they can even go about producing a product out of fear of excessive litigation.

## 4. RECOMMENDED DESIGN PRINCIPLES

We have focused on the privacy ceiling as a limit that arises naturally from economic pressure. Companies may encounter liability from excessive privacy intrusions, and then collectively respond to these penalties by moderating their behavior. However, this is a costly way for a business to converge to a balanced privacy policy; indeed, those who are sued and forced into deeper intrusions might not be able to reverse their trajectory. Instead, technology providers are better off designing their business architecture with a safe privacy policy from the start. Based on the circumstances that can create a privacy ceiling, we suggest several general design principles for businesses that wish to monitor or control users without making themselves liable.

Note that these recommendations assume there is no additional liability for contributory infringement. If there is substantial liability for contributory infringement, it is probably not helpful to split hairs over vicarious liability. In fact, if

a company participates so directly in a user's infringement, it will be very difficult to design against monitoring and control in the first place.

#### 4.1 Do not make it easy to monitor or control users

*Be aware of the architecture of your technology. Design an architecture so that it is not possible for a third party to force you to monitor and control your users.*

Even if a company does not monitor or restrict its users, it should be aware of the ease with which such measures might be put in place. If it can be argued that monitoring is easy and cheap to implement, then a company might be compelled to do so despite its existing policy. Keep in mind that courts will not be sympathetic to a "head in the sand" design approach. Instead, the inability to monitor or control users should be a natural consequence of the architecture rather than an apparently contrived property specifically engineered to avoid liability.

For example, a core feature of the Napster software led judges to order the monitoring of all content passing through the P2P network. While Napster claimed that they were unable to monitor their users due to the lack of access to user's MP3s, the Court ruled that Napster was capable of policing its system because it had the "ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system" [22] As a result, Napster was ordered to install a filtering mechanism to remove all content violating copyright.

In contrast, the makers of ReplayTV were not required to provide information about its users. In 2001, ReplayTV and its vendor SonicBlue were sued by Paramount Pictures Corporation for contributory infringement, vicarious infringement, violations of the Communication Acts, and for unfair business practices [5]. ReplayTV's technology allowed subscribers to record and time-shift television programming; features included the ability to skip commercials with the technology's "AutoSkip" feature as well as to record and distribute digital content to other users with the technology's "Send Show" feature. In the decision by the magistrate judge of the Central Court of California, Replay TV was initially ordered to provide information relating to how the "users of ReplayTV employ the devices" [52] during the discovery process. The Central District Court reversed the lower court's decision finding that the order impermissibly requires defendants to create new data which does not exist. A party cannot be compelled to create, or cause to be created, new documents solely for their production. Federal Rule of Civil Procedure Rule 34 requires only that a party produce documents that are already in existence" [52]. This case supports our recommendation that an architecture should be designed so that it would be impossible for the data collection to occur.

A possible remedy is a system in which tracking or control is inherently difficult. This may not be possible for some business models; for example, a file sharing service may be engineered to be difficult to track, but for an Internet service provider or online store, a user's personal information is naturally acquired in a financial transaction. For some technology companies, they either license copyrighted materials or patents controlled by entities who want strict monitoring

and control. In that case there will not be as much freedom to choose a limited architecture.

Fred von Lohmann [42] recommends that companies do not sell both software and services. The advice against "bundling" is architectural because a large end-to-end system allows more monitoring and control. Following his recommendation may also help to prevent being subject to licensing restrictions - for example, if a company sells music-playing software and also runs an online music store, they may not be allowed to distribute the copyrighted music unless they yield to demands to put controls in the software.

#### 4.2 Monitor and control to the extent that is capable in the architecture

*To minimize liability, make some effort to exercise control is that allowed by the architecture.*

This may seem contradictory, but we are assuming that if any monitoring and control is practically possible, then a company can be compelled to exert it. Indeed, it is this principle that suggests the existence of a privacy ceiling. In the worst case, we will assume that a company will be obligated to inflict privacy intrusions that the architecture realistically allows. *Reliable privacy safeguards must be systemic, intrinsic in the architecture.*

But, why would we then suggest that people monitor and control to the extent their architecture *does* allow? This is an effort to reduce liability: a court may be unsympathetic to someone that exerts virtually no effort, even if by design there is little one can do to stop infringement. The *Grokster* court stated that someone "infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it." Doing nothing or turning a "blind eye" to infringement may be seen as declining to exercise that right. On the other hand, the *Grokster* "formulation does not hold the defendant liable even if she exercises control", where "a defendant is not at fault if she takes reasonable precaution against the possibility of harm to the plaintiff" [54].

In other words, architectural limits will set the privacy level that protects the user; beneath this threshold, we should not only assume that the remaining controls will be forced into use, but that their use can reduce liability.

#### 4.3 Do not attempt to 'strike a balance'

*Do not try to design a system that tries to please everyone. Legal attacks like the ones described above will negate the consumer-friendly protocols that have been designed in such a system.*

This recommendation is less obvious than the previous two. Researchers have attempted to design DRM systems that balance the desires of consumers with those of content providers, incorporating privacy and usage policies to satisfy everyone.<sup>6</sup> However, a technology company is not in any position of authority to decide where the balance will lie. As

<sup>6</sup>A recent example proposes a buyer-seller protocol with a third party to balance customer rights with copyrights (F. Frattolillo et al. "A web oriented and interactive buyer-seller watermarking protocol." In *Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents VIII*, 6072-67.) The third party collects user tracking information, but keeps it from a copyright owner unless certain requirements are met.

long as end users are committing what is arguably infringement, a content provider may still demand the surrender of personal information - or demand that the company abandon “balance” and tighten its rules.

In fact, a company puts itself at greater risk by attempting to strike a balance, because in doing so it establishes some framework for data collection or usage control. Thus, the company cannot easily argue that it is unable to meet the content provider’s demands. Rather, a content provider can argue that the existing system can simply be changed to be made more strict: the architecture of control is already in place, and needs only be amended.

We find this result very interesting, because it suggests that the whole idea of a “balanced” DRM system is risky and counterproductive. The alternative is to avoid any architecture that could be extended to an undesirable extreme, if compelled by a court to do so. If a company wishes to employ a DRM system, it should only be capable of the minimum control necessary to achieve the desired ends, and be difficult to amend.

## 5. CONCLUSION

In this paper, we define the privacy ceiling and the design principles that arise from this practical limit to privacy disruptions. While initially attractive, it is counterproductive for technology companies to excessively monitor or control their users. Significantly reducing the user’s privacy is not economically feasible for the reason that companies incur various kinds of legal risk in the process, beyond mere consumer backlash. This risk should reduce the benefit of collecting information about users, until diminishing returns place an effective ceiling on companies’ behavior. This ceiling places a limit on the magnitude of privacy disruptions or violations that technologies should be permissible in taking due to a desire to remain profitable. The risk of litigation should make technology providers aware of the legal hurdles that they should seek to avoid, and thus, help them to design their products accordingly.

Of the circumstances that create a privacy ceiling, the liability for vicarious infringement lends itself to concrete design principles to avoid the “right and ability to control” defined in the *Napster* ruling. While the Supreme Court did not comment on the Ninth Circuit Court’s ruling on vicarious infringement for *Grokster* due to their focus on the inducement rule, technology providers must continue to make a special effort to preserve privacy so that they are not and do not have the ability to monitor all actions of consumers. Additionally, technology entities should design technologies according to the Fair Information Practice Principles, and they should seek to minimize the amounts of privacy intrusions as much as possible. They must be aware of their privacy ceiling and examine their architectures and design them so that it is not possible to capture privacy-invasive data, lest they wish to take on the expense of litigation. Finally, based on their privacy-protective architectures, they must show that they are attempting to be a “good actor” providing implementations of control as much as their architectures will allow.

## 6. ACKNOWLEDGMENTS

We would like to thank Michael Madison for his valuable comments and input.

## 7. REFERENCES

- [1] *Gershwin Pub. Co. v. Columbia Artists Management, Inc.* 443 F.2d 1159 (2d Cir.1971).
- [2] In re *Aimster* copyright legislation. 334 F.3d 643 (7th Cir. 2003).
- [3] *Respondeat superior.* *Merriam-Webster Dictionary of Law*, 1996.
- [4] *Digital Millennium Copyright Act of 1998.* Pub L. 105-304, 1998. <http://thomas.loc.gov/cgi-bin/toGPO/> [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105\\_cong\\_public\\_laws&docid=f:publ304.105.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.pdf).
- [5] *Paramount Pictures Corp. v ReplayTV & SonicBlue* complaint. October 30 2001. [http://www.eff.org/IP/Video/Paramount\\_v\\_ReplayTV/20011031\\_complaint.pdf](http://www.eff.org/IP/Video/Paramount_v_ReplayTV/20011031_complaint.pdf).
- [6] Second annual litigation trends survey findings. *Fulbright & Jaworski LLP*, 2005.
- [7] Ten years of chilled innovation. *BusinessWeek*, June 29 2005. [http://www.businessweek.com/technology/content/jun2005/tc20050629\\_2928.tc057.htm](http://www.businessweek.com/technology/content/jun2005/tc20050629_2928.tc057.htm).
- [8] Verizon and the Walt Disney Company sign long-term programming agreement. *Verizon Communications*, September 21 2005. <http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=92857>.
- [9] Musicians tell fans how to beat the system. *Financial Express*, 2005, October 8. [http://www.financialexpress-bd.com/index3.asp?cnd=10/8/2005&section\\_id=4&newsid=3114&spcl=no](http://www.financialexpress-bd.com/index3.asp?cnd=10/8/2005&section_id=4&newsid=3114&spcl=no).
- [10] Google censors itself for China. *BBC News*, January 25 2006. <http://news.bbc.co.uk/2/hi/technology/4645596.stm>.
- [11] Google moves files to China. *Red Herring*, March 2 2006. <http://www.redherring.com/Article.aspx?a=15927&hed=Google+Moves+Files+from+China&sector=Industries&subsector=InternetAndServices>.
- [12] Microsoft opens up censored blogs. *BBC News*, February 2 2006. <http://news.bbc.co.uk/2/hi/technology/4671284.stm>.
- [13] USACM policy recommendations on digital rights management, February 2006. <http://www.acm.org/usacm/weblog/wp-content/DRM.pdf>.
- [14] Sony sued over copy-protected CDs. *BBC News*, 2006, November 10. <http://news.bbc.co.uk/1/hi/technology/4424254.stm>.
- [15] 107th Congress. Hr 3162, October 24 2001.
- [16] S. E. Ante. Inside *napster*. *BusinessWeek*, August 14 2000. [http://www.businessweek.com/2000/00\\_33/b3694001.htm](http://www.businessweek.com/2000/00_33/b3694001.htm).
- [17] A. L. Association. Library bill of rights. June 18 1948. <http://www.ala.org/ala/oif/statementspols/statementsif/librarybillofrights.pdf>.
- [18] A. L. Association. The USA PATRIOT Act in the library, 2001. <http://www.ala.org/template.cfm/?Section=issues&Template=/ContentManagement/ContentDisplay.cfm&ContentID=76289>.
- [19] A. L. Association. Privacy: An Interpretation of the Library Bill of Rights. June 19 2002. <http://www.ala.org/ala/oif/statementspols/statementsif/interpretations/privacy.htm>.
- [20] A. L. Association. Resolution on the USA PATRIOT Act and related measures that infringe on the rights of library users. January 23 2003. <http://www.ala.org/alaorg/oif/usapatriotresolution.html>.
- [21] T. Baldas. Music piracy defendants fighting back. *National Law Journal*, October 10, 2005. <http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1128675912177>.
- [22] R. Beezer. A&M Records v Napster opinion. *U.S. Court of Appeals for the Ninth Circuit*, (00-16401), 2001. <http://www.ce9.uscourts.gov/web/newopinions.nsf/0c4f204f69c2538f6882569f100616b06?OpenDocument>.
- [23] S. BMG. Sony BMG music entertainment. 2005. <http://cp.sonybmg.com/xcp/english/home.html>.
- [24] J. Borland. Sony recalls risky 'rootkit' CDs. *CNET news*, 2005, November 15. <http://news.com.com/Sony+recalls+risky+rootkit+CDs/2100-7349.3-5954154.html?tag=nl>.
- [25] J. Borland. Apple iTunes raises privacy concerns. *CNET news*, 2006, January 12. <http://news.com.com/Apples+iTunes+raises+privacy+concerns/2100-1029.3-6026542.html?tag=nl>.
- [26] J. Borland. Apple tweaks iTunes following privacy concerns. *CNET news*, 2006, January 18. <http://news.com.com/Apple+tweaks+iTunes+following+privacy+concerns/2100-1027.3-6028085.html>.

- [27] K. M. L. Calvin and B. C. Y. Tan. The Internet is changing the music industry. *Communications of the ACM*, 44(8):68–68, August 2001.
- [28] J. Cohen. DRM and Privacy. *Berkeley Technology Law Journal*, 18, 2003. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=372741](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=372741).
- [29] J. Cohen. DRM and Privacy. *Communications of the ACM*, 46(4):47–49, April 2003.
- [30] K. M. Dames. Verizon backtracking on privacy? *CopyCense*, October 3 2005. [http://www.copycense.com/2005/10/verizon\\_backtra.html](http://www.copycense.com/2005/10/verizon_backtra.html).
- [31] R. P. Eclavea. Liability as "Vicarious" or "Contributory" infringer under Federal Copyright Act. *14 A.L.R. Fed. 825*, 1999.
- [32] J. Evers. Sony halts production of 'rootkit' CDs. *CNET news*, 2005, November 11. <http://news.com.com/Sony+halts+production+of+rootkit+CDs/2100-1029-3-5946825.html?tag=nl>.
- [33] J. F. Feigenbaum, T. Sander, and A. Shostack. Privacy engineering for digital rights management systems. In *ACM Workshop on Security and Privacy in Digital Rights Management*, pages 76–105, 2001.
- [34] E. Felten and J. A. Halderman. Digital rights management, spyware, and security. *IEEE Security and Privacy*, pages 19–23, January/February 2006.
- [35] I. Fried. Grokster case: Winners and losers. *CNET news*, June 27 2005. <http://news.com.com/Grokster+case+Winners+and+losers/2100-1030-3-5764743.html>.
- [36] J. A. Halderman and E. Felten. Lessons from the Sony CD DRM episode. In *Proceedings of the 15th USENIX Security Symposium*, August 2006.
- [37] L. Henkin. Privacy and Autonomy. *Columbia Law Review*, 74:1410–33, 1974.
- [38] K. C. Jones. Murder suspect's Google searches spotlighted in trial. *InformationWeek*, November 11 2005. <http://www.informationweek.com/story/showArticle.jhtml?articleID=173602206>.
- [39] J. LeClaire. RIAA says illegal file sharing has been contained. *TechNewsWorld.com*, June 14 2006. <http://www.technewsworld.com/story/hEHHahas2xn91U/RIAA-Says-Illegal-File-Swapping-Has-Been-Contained.xhtml>.
- [40] J. Leyden. Yahoo! in second Chinese dissident rumpus. *The Register*, February 10 2006. [http://www.theregister.co.uk/2006/02/10/yahoo\\_china\\_cyber-dissident\\_flak/](http://www.theregister.co.uk/2006/02/10/yahoo_china_cyber-dissident_flak/).
- [41] S. P. Library. The Seattle Pubic Library: Confidentiality and the PATRIOT Act. 2001. [http://www.spl.org/default.asp?pageID=privacy\\_patriot](http://www.spl.org/default.asp?pageID=privacy_patriot).
- [42] F. v. Lohmann. IAAL: What peer-to-peer developers need to know about copyright law. *Electronic Freedom Foundation*, January 2006. [http://www.eff.org/IP/P2P/p2p\\_copyright\\_wp.php](http://www.eff.org/IP/P2P/p2p_copyright_wp.php).
- [43] K. McElhearn. The iTunes MiniStore: Fact and Fiction. *Kirkville*, 2006, January 14. <http://www.mcelhearn.com/article.php?story=20060113123710770>.
- [44] A. McLaughlin. Google in China. *Google*, January 27, 2006. <http://googleblog.blogspot.com/2006/01/google-in-china.html>.
- [45] D. Mulligan, J. Han, and A. Burstein. How DRM-based content delivery systems disrupt expectations of "personal use". *DRM'03*, pages 77–89, 2003.
- [46] S. L. D. Network. About don't ask, don't tell. 2005. <http://www.sldn.org/templates/dont/record.html?section=42&record=749>.
- [47] M. Russinovich. Sony, rootkits and digital rights management gone too far. October 31 2005. <http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>.
- [48] B. Schneier. Musicians tell fans how to beat copy protection. *Schneier on Security*, October 10 2005. [http://www.schneier.com/blog/archives/2005/10/musicians\\_tell.html](http://www.schneier.com/blog/archives/2005/10/musicians_tell.html).
- [49] M. Schroeder. *Fonovisa v. Cherry Auction*. *U.S. Court of Appeals for the Ninth Circuit*, (76 F.3d 259 (9th Cir. 1996)), 1996.
- [50] D. Souter. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, LTD*. *Supreme Court of the United States*, (04-480), 2005.
- [51] S. R. Thomas. *Metro-Goldwyn-Mayer v. Grokster*. *U.S. Court of Appeals for the Ninth Circuit*, (03-55894), 2004.
- [52] C. D. o. C. US District Court. Order on parties' motions for review of magistrate judge's discovery order on april 26, 2002. May 30 2002. [http://www.eff.org/IP/Video/Paramount\\_v\\_ReplayTV20020531\\_replay\\_discovery\\_reversal.pdf](http://www.eff.org/IP/Video/Paramount_v_ReplayTV20020531_replay_discovery_reversal.pdf).
- [53] L. Woellert. Sony BMG ends a legal nightmare. *BusinessWeek*, 2005, December 30. [http://www.businessweek.com/technology/content/dec2005/tc20051230\\_658336.htm](http://www.businessweek.com/technology/content/dec2005/tc20051230_658336.htm).
- [54] A. Yen. Third party copyright after Grokster. *Forthcoming in the Minnesota Law Review*.