2008

Online File Sharing: Resolving the Tensions Between Privacy and Property

Frances Grodzinsky
Sacred Heart University, grodzinskyf@sacredheart.edu

Herman T. Tavani
Rivier College

Online File Sharing: Resolving the Tensions between Privacy and Property Interests

Frances S. Grodzinsky
Sacred Heart University
grodzinskyf@yahoo.com

Herman T. Tavani
Rivier College
htavani@rivier.edu

Abstract
This essay expands upon an earlier work (Grodzinsky and Tavani, 2005) in which we analyzed the implications of the *Verizon v RIAA* case for P2P Networks vis-à-vis concerns affecting personal privacy and intellectual property. In the present essay we revisit some of the concerns surrounding this case by analyzing the intellectual property and privacy issues that emerged in the *MGM Studios v. Grokster* case. These two cases illustrate some of the key tensions that exist between privacy and property interests in cyberspace. In our analysis, we contrast Digital Rights Management (DRM) and Interoperability and we examine some newer distribution models of sharing over P2P networks. We also analyze some privacy implications in the two cases in light of the theory of privacy as contextual integrity (Nissenbaum, 2004).

1. Introduction

This essay[9] expands upon an earlier work (Grodzinsky and Tavani, 2005) in which we analyzed the implications of the *Verizon v RIAA* case for P2P Networks vis-à-vis concerns affecting personal privacy and intellectual property. In the present essay, we analyze some implications for intellectual property by drawing some analogies to the ruling in the *MGM Studios v. Grokster* case, which demonstrates that the debate over sharing copyrighted material in P2P systems has not been limited to copyrighted music files. In particular, we question whether the Verizon and Grokster cases advance the interests of copyright owners at the expense of preserving privacy for individual users. We also question whether the rulings in these two cases threaten new technologies in order to advance the interest of copyright owners. We then examine some privacy implications surrounding these cases in light of the theory of privacy as contextual integrity (Nissenbaum, 2004). Although we disagree with the tactics used by the recording and movie industries to track down individuals who download unauthorized proprietary content from the Internet, we do not defend copyright violation. However, we also believe that some alternative strategies need to be examined in this debate.

[9] An earlier version of this essay was presented at the *11th International Conference on the Social and Ethical Impacts of Information and Communications Technologies*, University of Mantua, Italy, September 2008, and printed in the *ETHICOMP 2008 Conference Proceedings*, 2008, pp. 373-383.

2. A Brief Review of the *Verizon v. RIAA* and the *MGM v. Grokster* Cases: Implications for the Future of P2P Systems

We begin by providing some background information in the Verizon and MGM cases, including the timeline in each. In January 2003, U.S. District Court in Washington D.C. ruled that Verizon must comply with the subpoena issued by the Recording Industry Association of America (RIAA) requesting the name of a subscriber who allegedly made available more than 600 copyrighted music files over the Internet. Subpoena power applies to all Internet service providers within the scope of the Digital Millennium Copyright Act (DMCA), not just to those service providers storing information on a system or network at the direction of a user. On December 19, 2003 the United States Court of Appeals for the District of Columbia overturned the lower court's decision alleging that the DMCA applied only to those sites hosting illegal content and not to those simply transmitting it.

The debate over sharing copyrighted material in P2P systems has not been limited to copyrighted music files (e.g., as argued in the Verizon case). The motion picture industry has also been concerned about the ease with which copyrighted movies can be freely exchanged in file-sharing systems. In 2003, Metro-Goldwyn-Mayer (MGM) sued two P2P file-sharing services, alleging that over 90% of the material exchanged on Grokster was copyrighted material and that the P2P service was legally liable. The lower district court and the Court of Appeals ruled that Grokster could not be held liable for the distribution of copyrighted material because: it lacked sufficient knowledge of the infringement; it did not materially contribute to the copyright infringement. MGM appealed the case to the U.S. Supreme Court. During the oral arguments, the justices seemed to be divided between two principles: the need to "protect new technologies" (such as P2P networks) and the need to provide "remedies against copyright infringement." The Court unanimously confirmed that using Grokster's service to trade copyrighted material is illegal (but the Court did not agree that P2P technology should be made illegal). This decision reflected the tension to protect new technologies as well as copyright holders.

What are some of the implications of the Court's decisions in these two cases for the future of P2P technology? Whereas the appeals process in the Verizon case can arguably be interpreted as favoring the privacy rights of individual users in P2P networks, we believe that the US Supreme Court in the MGM appeals tended to side with property right holders. However, the Court's ruling does not necessarily threaten innovative technologies such as P2P systems, despite the efforts of some property right holders to eliminate P2P systems altogether.

The Verizon and MGM cases illustrate ethical challenges that affect both privacy and property. The conflict between privacy and property rights in cyberspace can be understood as a tension involving "access and control" (Tavani, 2004). Whereas property-rights advocates argue for greater control over information they view to be proprietary (thereby restricting access to that information by ordinary persons), privacy advocates argue for individuals having greater control over their own personal information (thus restricting access to that information by entrepreneurs). In the next

section of this essay, we examine some property-related issues affecting the two cases. Privacy-related concerns are examined in Section 4.

3. Property-Related Issues Affecting the Verizon and MGM Cases

In an earlier essay (Grodzinsky and Tavani, 2005), we discussed Jessica Litman's concern that the extension to the Copyright Act of 1976 has contributed to the shrinking of the public domain by extending the scope of copyright to anything that is potentially copyrightable. Litman (2003) offers up a distribution model whereby the default is to share and therefore expand the public domain. Since then several other distribution models have emerged that concern online file sharing.

3.1 Distribution Models

By the year 2012, it is estimated that 40% of the global music market will be digital music (Evans, 2008). If more than 60 million users are sharing music over the Internet, and if many composers are not getting compensated adequately, then a fair distribution model that balances copyright with contextual privacy would be desirable. In an attempt to address some current inequities affecting copyright, a cluster of distribution models based on subscription fees have emerged since the publication of our last paper. In particular, many of these models are directed at servicing online music stores and portable MP3 players. The most popular of these models, iTunes is compatible with the iPod, Apple's MP3 player. On Demand Distribution (OD2) is another distribution model that is popular in Europe. Nokia purchased it in 2006 for use on mobile phones. Streaming media is yet another distribution model and is found in Internet radio.

3.1.1 The iTunes model

In the iTunes online music store, users are now downloading one and a quarter million songs per day, which is an annual run rate of almost half a billion songs per year. The contract that iTunes users sign in order to download their music strictly describes what they can or cannot do with the songs that they download. As for now, the proprietary nature of Apple software prevents downloading onto other portable devices; the distribution model is limited to iPods. However, iPods do play open format CD's not purchased from iTunes. This raises concerns about a possible "distribution monopoly."[10]

Apple has implemented a technology known as Fair Play DRM in an effort to stop illegal file sharing activities, and this technology is now active on all but the EMI music catalog. On April 3, 2007, EMI, one of the big four announced that it would sell its music without DRM on the iTunes music store. Non-DRM formatted music will cost slightly more than the $0.99 cents DRM version. This move will pave the way for others to follow suit (Felton, 2007). There will be no great loss for the big four: EMI, Sony BMG, Universal and Warner, as less than 3% of all music played on iPods is purchased from iTunes, and therefore, protected with DRM (Jobs, 2007). More than 90% of music is sold DRM free.

[10] The issue of a "distribution monopoly" is beyond the scope of this essay. However, we should point out that Apple worries that if it opens up its DRM (Digital Rights Management) algorithm to others, it would lose the ability to protect its music, which would cause it to lose its distribution rights. (DRM, and some controversies surrounding it, are briefly examined in Section 3.2 of this essay.)

Steve Jobs believes that if DRM restrictions were lifted, there might be an influx of new stores and players. (Jobs, 2007)

3.1.2 On Demand Distribution

At one time, OD2 was the primary download technology for online music stores in Europe. The European community is now looking at distribution models that work on standards that anyone could license, and so they are opposed to the monopolistic approach of Apple. Yet they are no longer satisfied with OD2 because of the interoperability problems that model has had. As noted above, Nokia purchased OD2 in 2006 in order to use it on its mobile phones. It is unclear, however, whether Nokia support will bring OD2 back as a serious contender in the digital music arena in Europe (Finlayson, 2006). Also, we should note that if Microsoft launches its own portable digital player, this product would have the potential to compete with Apple. No one has yet solved the interoperability issue, as online music stores typically service their own hardware.

3.1.3 Streaming Media

Video and audio streaming each have their own set of problems (whose details go beyond the scope of this essay). In video format, user-created content can be developed and used, but any content that is copyrighted can only be used with permission of the copyright holder. Who owns the copyright? Often there are several layers of "middlemen." We believe that Lessig's Creative Commons (CC) License would be helpful, if the goal is to broaden the public domain and make sharing easier.

The current growth rate for Internet radio is 27% per year, as compared to the 1% annual growth rate for traditional radio (Siglin, 2007). Internet radio stations that use audio streaming have been under attack by the Library of Congress Royalty Board, who issues royalty fees and who have been trying to revise the fee structure retroactive to 2006 (Siglin, 2007). How would this affect Internet Radio? "AOL Radio, LaunchCast, ClearChannel and Live365 would be billed $363 million during the same year that all 14,000 US radio stations combined would be billed $550 million" (Siglin, 2007). The tension between the Royalty Board and Internet radio was created in part by Sound Exchange, representatives of the record companies who "…sought the royalty amid a drop in compact disc sales that fell 20% from 2004-2006"(Tirrell, 2007).

It would seem that the case audio streaming can be viewed as one more instance in which proprietary interests are shrinking the public domain and thwarting new technologies from further development. Yahoo and AOL may have to shut down their Internet radio stations. In an attempt to nullify the ruling of the Copyright Royalty Board, the Internet Radio Equality Act was proposed in the Senate in May 2007.

3.2 Privately Preserving Property: DRM Vs. Interoperability

Digital Rights Management (DRM) technology can be defined as "Technology that protects a piece of intellectual digital property such as a music, video, or text file. With DRM, copyrighted material downloaded from the Web may be restricted so that it cannot be freely distributed" (http://h71036.www7.hp.com/hho/cache/281-0-0-225-121.html).

Because DRM builds a "digital fence" around a piece of copyrighted content, and allows only certain authorized access or use, it can be viewed as posing a significant obstacle to online file sharing. In the US, according to the DMCA, it is illegal to circumvent this technology for any reason; so the user has no legal recourse except to abandon his/her attempt to use the protected content. Current DRM schemes tip the balance in favor of the copyright owner who can determine how and by whom his/her content may be used. For that reason, DRM has become an obstacle to private use because it limits the user's freedom, by allowing private interests to define the parameters of the law. For users in DRM systems to preserve their fair use rights, they must be able to access material anonymously and to use content without authorization or demand for compensation (Armstrong, 2006). For more on issues affecting private use as "fair use", see Grodzinsky and Bottis (2007).

In the context of online music sharing, there is a tension between DRM and interoperability. Interoperability enables users to download and play music on a variety of devices. This ability also challenges the notion that downloadable content can and should be restricted to proprietary devices controlled by the company that owns the online store. France is perceived to have led the way in interoperability when in March, 2006 its National Assembly passed a law that would force distributors of online music in France to remove DRM so that music can be played on any device. Any company using proprietary music formats would be affected by this law, which may pave the way for other EU countries to follow (Hesseldahl, 2006). However, many distributors of music content believe that legally pushing interoperability will result in opening the door to file sharing of copyrighted material without compensation.

It is encouraging that EMI has agreed to distribute non-DRM music on the iTunes platform. On the one hand, opening up the distribution of music online might encourage other subscription services to follow suit. On the other hand, while these developments can be viewed as attempts to move in the right direction, unfortunately, the fair distribution of media might reduce but not totally eliminate unauthorized online file sharing of proprietary music. However, we do not subscribe to the recent attempts by the RIAA at lawsuits and lobbying in Congress for bills that tie penalties to online file sharing, especially those schemes that do so at the expense of personal privacy.

4. Context Based Theories of Privacy

In our earlier essay (Grodzinsky and Tavani, 2005), we described some of the difficulties one encounters when attempting to give a precise definition of privacy. There, we also distinguished between descriptive privacy and normative privacy, and we differentiated among three types of privacy: accessibility privacy, decisional privacy, and informational privacy. In our analysis of the Verizon case we also defended a theory of privacy advanced by Moor (1990, 1997) and expanded upon by Tavani and Moor (2001). Key aspects of this privacy framework, which we refer to as the RALC (Restricted Access/Limited Control) theory of privacy, are more fully explicated in Tavani (2007, 2008). So, we will not repeat the details of RALC here. However, we should note that one virtue of RALC that is crucial for our discussion of privacy in the present essay is that it is a context-based privacy theory that appeals to the notion of a "situation" in

determining whether a particular context, such as a P2P network, warrants normative privacy protection.

4.1 Privacy as Contextual Integrity

We have already noted how the RALC theory was helpful in analyzing P2P networks used in the Verizon case from the perspective of normative privacy protection. In this section, we show how a context-based theory of privacy such as Helen Nissenbaum's "contextual integrity" theory can also help us to understand the issues at stake for individual privacy in the debate about P2P environments.[11] We should note at the outset that Nissenbaum describes her privacy framework as a "benchmark theory," rather than a full-fledged theory of privacy (Nissenbaum 2004). However, we believe that her framework is sufficiently developed to inform the privacy debate in cases such as Verizon and MGM. How, exactly, does her privacy theory enable us to do this? First, we should note that Nissenbaum's theory requires that the processes used in gathering and disseminating information are "appropriate to a particular context" and that they comply with the "governing norms of distribution" for that context (Nissenbaum, 101). This insight expands upon her earlier work on the problem of "privacy in public" (Nissenbaum, 1997, 1998), where she notes that normative privacy protection does not typically apply to personal information gathered about us in what she describes as the "public sphere." For example, she points out that privacy norms (whether in the form of explicit privacy laws or informal privacy policies) protect personal information considered to be intimate and sensitive. This generally includes personal information such as medical records and financial records. However, normative privacy protection does not generally extend to personal information about us that can be gathered from our activities in public places – e.g., places where we shop, dine, recreate, and so forth.

Some of the core concerns affecting the problem of privacy in public, introduced in Nissenbaum's earlier essays, are also illustrated in her theory of privacy as contextual integrity (Nissenbaum 2004). Two key principles underlying Nissenbaum's later privacy theory are:

(i) the activities people engage in take place in a "plurality of realms" (i.e., spheres or contexts)
(ii) each realm has a distinct set of norms that govern its aspects.

These principles or norms both shape and limit or restrict our roles, behavior, and expectations by governing the flow of personal information in a given context.[12]

Additionally, Nissenbaum (2004) distinguishes between two types of informational norms: (a) norms of appropriateness, and (b) norms of distribution. The first of these determines whether a given type of personal information is either *appropriate or inappropriate* to divulge within a particular context. According to Nissenbaum, (138), these norms "circumscribe the type or nature of information about various individuals

[11] My description of Nissenbaum's privacy theory in this section closely parallels my accounts in Tavani (2008, in press).

[12] The contextual integrity model proceeds on the assumption that there are "no areas of life are not governed by norms of information flow" (Nissenbaum 2004, 137).

that, within a given context, is allowable, expected, or even demanded to be revealed." Contrast these norms with those of *distribution*, which restrict the flow of information within and across contexts. Nissenbaum (125) believes that when either of these norms is "breached," a violation of privacy occurs. On the contrary, the contextual integrity of the flow of personal information is maintained when both kinds of norms are "respected." [13]

Nissenbaum argues that her contextual integrity theory improves upon the leading alternative privacy theories in at least two key respects. For one thing, she notes that personal information that is revealed or disclosed in a particular context is always "tagged" with that context and thus is never "up for grabs." Because alternative privacy theories lack the appropriate "mechanisms" to prevent the "anything goes" approach to this kind of personal information, [14] Nissenbaum believes that those theories cannot grant normative protection to the kinds of personal information gathered in public places, A second key respect in which her theory differs from alternative accounts can be found in her claim that the "scope of informational norms" is always "internal to a given context" – i.e., the norms are "relative" or "non-universal" (Nissenbaum 125). She also points out that in her theory, "context-relative qualifications" can be "built right into the informational norms" of any given context, unlike other normative theories of privacy where these qualifications tend to be treated as "exceptions or tradeoffs" (Nissenbaum, 138).[15]

As in the case of the RALC framework mentioned above, Nissenbaum's theory illustrates why we must always attend to the context in which information flows, not the nature of the information itself, in determining whether normative protection is needed.[16] Like RALC, Nissenbaum's framework of privacy as contextual integrity can be applied to a wide range of contemporary technologies to determine whether they breach the informational privacy norms that govern specific contexts.[17]

---

[13] Nissenbaum argues that there are no information or spheres of life for which "anything goes." As Nissenbaum (2004, 128) states: "Almost everything – things that we do, events that occur, transactions that take place – happens in a context…" In her scheme, contexts include "spheres of life" such as education, politics, the marketplace, and so forth.

[14] Nissenbaum (1998) points out that when it comes to questions about how to protect personal information in public contexts, or in what she calls "spheres other than the intimate," most normative accounts of privacy have a theoretical "blind spot."

[15] In this sense, she believes that her theory allows for the possibility of "context-relative variation" as an "integral part of contextual integrity."

[16] Rather than focusing on the nature of the information included in a P2P situation – i.e., asking whether or not it should be viewed as private – we can ask whether P2P situations or contexts (in general) deserve protection as "normatively private situations" (Moor) or contexts (Nissenbaum). In the RALC framework, Moor (1997) includes a scenario involving information about faculty salaries for professors who teach at public institutions funded by tax-payers vs. small, privately owned colleges, to illustrate this point. He notes that there is nothing inherent in the information about the professors' salaries per se that is helpful in determining whether it was appropriate to protect that information. Instead, Moor argues that it is the specific "situation" or context – in particular, the norms governing the flow of information in the context of a large public university vs. a small private college – that determined whether it is appropriate to grant such information normative protection.

[17] For example, Nissenbaum's account of the problem of privacy in public, in conjunction with her framework of contextual integrity, can help us to better understand the kinds of privacy threats posed by data-mining technology (Tavani, 2007). For an interesting discussion of how Nissenbaum's theory of

5. Extending Contextual Integrity To P2P Contexts

How can Nissenbaum's account of privacy as contextual integrity be applied to P2P contexts? Before attempting to extend the theory of Contextual Integrity to P2P networks, we first respond to the challenge of whether a P2P environment can count as a context.[18] For example, some might object that P2P networks lack explicit norms for governing the behavior of its participants and thus might not qualify as a conventional "context" – at least not in a normative sense. Against such an objection, we note that P2P environments have implicit rules that govern the behavior of participants as well as explicit privacy policies in some cases. But consider that even in the absence of explicit rules governing all of our day-to-day activities, many of our cultural norms (in general) are based upon adherence to implicit rather than explicit rules. So, for our purposes, we can assume that a P2P network is an example of a context that is governed by rules.

We believe that Nissenbaum's theory of privacy as contextual integrity shows why it is inappropriate for the RIAA to have access to personal information that belongs to a P2P context. For one thing, P2P users have an expectation of privacy based in part on the privacy policies and the distributed architectures (e.g. Bit Torrent) that were created, in part, to preserve the anonymity of the clients. According to the norms of appropriateness, IP addresses that enable file sharing among clients are appropriate to those involved in the sharing process. In some highly distributed models, these address strings are further randomized to preserve anonymity, even among those sharing files. According to the norms of distribution, email accounts as well as upgrades about P2P services are available to those who choose to create accounts and subscribe to the services; these are used solely within the P2P service and are not shared with third parties. Privacy policies on the Morpheus and Bit Torrent Web sites outline the terms of distribution of personal information. Following the Napster, Grokster and Verizon cases, some "context-relevant qualifications" have emerged on these sites. For example, Bit Torrent's policy says,

> *Notwithstanding any other term of this Privacy Policy, we may release any personal information we obtain or collect when we believe its release is appropriate to comply with the law, enforce our Site policies, or protect ours or others' rights, property, or safety* (http://www.bittorrent.com/privacy?csrc=splash).

Morpheus, distributed by StreamCast Networks, makes a similar claim, when it asserts:

> *StreamCast does not condone copyright, patent or other intellectual property infringement. Due to the nature of peer-to-peer software, StreamCast Networks is unable to monitor or control the files searched for or shared using Morpheus. If you locate any material being shared by a user who you believe may be in violation of copyright or other intellectual property law, please report your concerns to that user directly. This is not intended to be legal advice or counsel. If you have any questions consult your attorney.*

---

contextual integrity can be applied to privacy issues involving "vehicle-safety communications technologies," see Zimmer (2005).

[18] For example, Richard Volkman has posed this question to us in a conversation about "P2P contexts."

This approach preserves the flow of distribution and does not assume the role of cyber police. The next part of the policy defines its "context-relevant" qualifications.

> *Morpheus® values your anonymity and privacy. Morpheus does not contain or bundle malicious spyware. Upon being served with valid subpoenas or warrants, Morpheus will cooperate with governmental agencies to eliminate and prosecute trafficking in child pornography and other similar crimes* (http://www.morpheus.com/notices.asp).

So while many of these P2P systems claim that they condemn sharing of copyrighted material, and while they say that they will cooperate with legitimate legal actions, (not requests of the entertainment industry), only Morpheus specifies that crimes on the level of child pornography will cause it to alter its norm of distribution.

Because the RIAA has been technologically thwarted in its attempt to obtain information about users from P2P networks directly, it has tried to get that information by other means. Typically, file sharers connect to P2P networks through either their ISP's or their university's networks. These two discrete contexts connect to the P2P context; however, there is also information that crosses contexts (i.e., flows from one to the other). We have argued elsewhere (Grodzinsky and Tavani, 2005) that the RIAA seems to assume that its property interests automatically trump the privacy rights of P2P users. By threatening ISP's and universities with legal action, the RIAA hopes to obtain private information that can be used to identify file sharers on the P2P networks. We believe that this kind of behavior is a violation of privacy according to Nissenbaum's theory.[19]

To see how the privacy violation occurs, consider the following scheme. In most universities in the United States, student privacy is protected. There are explicit policies in place that inform who may or may not have access to a student's personal information. In fact, on many campuses, parents may not have access to his or her child's grades or to information about the child's professors without explicit consent from the student. So, the flow of information within the university context is quite restricted. Consider that university networks are part of the university context – i.e., they are owned and operated by the university and, we believe, fall under their privacy rules. When students use the university network to connect to a P2P network to file share, they move from a private network to an openly distributed one, thus crossing contexts. The RIAA's inability to control file sharing through technology within the P2P's has led it to increase its attempts to force universities as well as ISP's to assume the role of cyber police effectively, placing the burden of enforcement on the university. This usually conflicts with the university's existing privacy policies. Thus, we believe that capitulation by the universities and ISP's based on threats from private industry would constitute a clear violation of privacy, according to Nissenbaum's theory.

In a more expansive and systematic attempt to control downloading on university campuses, the RIAA has recently tried to tie the unauthorized downloading of files by

[19] For a view that is more sympathetic to Verizon in this dispute, see Spinello (2004). We should also point out that Spinello (2008) supports a position that is more sympathetic to MGM than the one we defend in this essay.

students to a loss of financial aid. Legislation introduced in November 2007 to amend and extend the Higher Education Bill of 1965 includes the controversial Section 494, entitled Campus-based digital theft prevention. Sunny Kalara, an intellectual property attorney, explains, "Each eligible institution participating in the federal aid program shall: provide annual disclosure/warnings to the students applying for or receiving financial aid, stating that: P2P file sharing may subject them to civil and criminal liability" (Kalara, 2007). Students applying for or receiving financial aid, stating that: P2P file sharing may subject them to civil and criminal liability" (Kalara, 2007). The bill demands that the universities offer subscription services to their student bodies that will give them an alternative to illegal file sharing. The American Association of Universities has written to the proponents of the bill expressing their outrage and asking them to remove the P2P section. Otherwise, innocent students could be caught up in a sweep that would penalize them and deprive them of much needed financial aid, if universities do not comply.

6. Concluding Remarks

If we accept Nissenbaum's context-based approach to privacy controversies affecting P2P networks, in conjunction with one or more of the distribution models, that we examined, we can both protect privacy interests of individuals and help ensure that property owners' interests are also reasonably preserved. Following DeCew (1997), we believe in a "presumption in favor of privacy" as the default starting position in debates affecting privacy and other interests, such as property. We also argue that P2P networks are contextually private situations and, as such, protecting privacy in the debate involving Verizon and the RIAA is essential. In the MGM case, we believe that the Courts failed to appreciate the *contextual* aspect of P2P systems in its ruling. Even though the Court upheld the legitimacy of P2P systems and their importance to technological innovation, the majority opinion expressed by the Court did not recognize the significant implications its decision had for the privacy of users of P2P systems. We believe that if the US Supreme Court, in deciding the MGM case, had taken into consideration the contextual nature of P2P networks and the kind of privacy protection that is warranted by such contexts, the Court may have reached a different conclusion.

References

Armstrong T.K. (2006) "Digital Rights Management and the Process of Fair Use," 20(1) *Harvard Journal of Law & Technology* 49 electronic copy http://ssrn.com/abstract=885371, accessed April 2007

DeCew, J. (1997) *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, New York: Cornell University Press.

Evans, J (2008) "Forty Percent of Global Music Sales to Be Digital," http://www.pcworld.com/businesscenter/article/144392/forty_percent_of_global_music_sales_to_be_digital.html, accessed May 2008.

Felten E. (2007) "EMI to sell DRM-Free Music," available at http://www.freedom-to-tinker.com, accessed April 2007.

Finlayson, Gordon (2006) "Kia buys Loudeye/OD2 for 60 Million," http://digitalmusic.weblogsinc.com/2006/08/09/nokia-buys-loudeye-od2-for-60-million/, accessed March, 2008.

Fisher, W. (2004) " iTunes: How copyright, contract and technology shape the business of digital media: a case study", http://cyber.law.harvard.edu/media/uploads/81/iTunesWhitePaper0604.pdf, June 15, 2004, accessed March, 2006

Grodzinsky, F.S., and Bottis, M.C. (2007) "Private Use as Fair Use: Is it Fair?" *Computers and Society*, Vol. 37, No. 4, 11-24.

Grodzinsky, F. S., and Tavani, H. T. (2005) "P2P Networks and the *Verizon v. RIAA* Case: Implications for Personal Privacy and Intellectual Property," *Ethics and Information Technology*, Vol. 7, No. 4, 243-250.

Hesseldahl,A. (2006) "Apple vs. France", http://www.businessweek.com/print/technology/content/mar2006/tc20060321_144066.htm, accessed May, 2008.

HP Digital Music Glossary http://h71036.www7.hp.com/hho/cache/281-0-0-225-121.html. accessed May, 2008.

Jobs S. (2007) "Thoughts on Music," available at http://www.appled.com/hotnews/thoughtsonmusic/, accessed November, 2007.

Kalara, S. (2007) "Now the RIAA wants Universities to get campus-wide Napster subscription or 'lose all federal aid'", http://www.bizorigin.com/2007/riaa_nuclear_option, accessed March, 2008.

Litman, J. (2003) "Ethical Disobedience," *Ethics and Information Technology*, Vol. 5, No. 4, 2003, pp. 217-223.

Moor, J. H. (1990) "The Ethics of Privacy Protection," *Library Trends*, Vol. 38, Nos. 1-2, 69-82.

Moor, J. H. (1997) "Towards a Theory of Privacy for the Information Age," *Computers and Society*, Vol. 27, No. 3, 27-32.

Nissenbaum, H. (1997) "Toward an Approach to Privacy in Public: Challenges of Information Technology," *Ethics and Behavior*, Vol. 7, No. 3, 207-219.

Nissenbaum, H. (1998) "Protecting Privacy in an Information Age," *Law and Philosophy*, 559-596.

Nissenbaum, H. (2004). "Privacy as Contextual Integrity," *Washington Law Review*, Vol. 79, No. 1, 119-157.

Siglin, T. (2007) "New Royalty Schedule May Scuttle Independent Internet Radio", http://www.streamingmedia.com/article.asp?id=9527, accessed March 2007.

Spinello, R.A. (2004) "A Moral Analysis of the 'RIAA v Verizon' Case," *Journal of Information, Communication and Ethics in Society*, Vol. 4, No. 2, 203-215.

Spinello, R. A. (2008) "Intellectual Property: Legal and Moral Challenges of Online File Sharing." In K. E. Himma and H. T. Tavani, eds. *The Handbook of Information and Computer Ethics*. Hoboken, NJ: John Wiley and Sons, 553-570.

Tavani, H. T. (2004) *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Second Edition, 2007. Hoboken, NJ: John Wiley and Sons.

Tavani, H. T. (2007) "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy," *Metaphilosophy*, Vol. 38, No. 1, 1-22.

Tavani, H. T. (2008) "Informational Privacy: Concepts, Theories, and Controversies." In K. E. Himma and H. T. Tavani, eds. *The Handbook of Information and Computer Ethics*. Hoboken, NJ: John Wiley and Sons, 131-164.

Tavani, H. T. (in press) "Floridi's Ontological Theory of Informational Privacy: Some Implications and Challenges," *Ethics and Information Technology*.

Tavani, H.T. and Moor, J.H. (2001) "Privacy Protection, Control of Information, and Privacy Enhancing Technologies," *Computers and Society*, Vol. 31, No. 1, 6-11.

Tirrell, Meg (2007) "Yahoo, AOL May Abandon Web Radio After Royalties Rise (Update2)", http://www.bloomberg.com/apps/news?pid=20601103&sid=a0pKOrcpw6yE&refer=us#, accessed December 2007.

Zimmer, M. (2005). "Surveillance, Privacy and the Ethics of Vehicle Safety Communications," *Ethics and Information Technology*, Vol. 7, No. 4, 201-210.