Ethics and Information Technology (2005) 7:243–250
DOI 10.1007/s10676-006-0012-4

P2P networks and the *Verizon v. RIAA* case: Implications for personal privacy and intellectual property

Frances S. Grodzinsky[1] and Herman T. Tavani[2]
[1]*Department of Computer Science and Information Technology, Sacred Heart University, 5151 Park Avenue, Fairfield, CT 06825, USA*
[2]*Department of Philosophy, Rivier College, 420 Main St., Nashua, NH 03060, USA*
E-mails: grodzinskyf@sacredheart.edu; htavani@rivier.edu

Abstract. In this paper, we examine some ethical implications of a controversial court decision in the United States involving Verizon (an Internet Service Provider or ISP) and the Recording Industry Association of America (RIAA). In particular, we analyze the impacts this decision has for personal privacy and intellectual property. We begin with a brief description of the controversies and rulings in this case. This is followed by a look at some of the challenges that peer-to-peer (P2P) systems, used to share digital information, pose for our legal and moral systems. We then examine the concept of privacy to better understand how the privacy of Internet users participating in P2P file-sharing practices is threatened under certain interpretations of the Digital Millennium Copyright Act (DMCA) in the United States. In particular, we examine the implications of this act for a new form of "panoptic surveillance" that can be carried out by organizations such as the RIAA. We next consider the tension between privacy and property-right interests that emerges in the Verizon case, and we examine a model proposed by Jessica Litman for distributing information over the Internet in a way that respects both privacy and property rights. We conclude by arguing that in the Verizon case, we should presume in favor of privacy as the default position, and we defend the view that a presumption should be made in favor of sharing (rather than hoarding) digital information. We also conclude that in the Verizon case, a presumption in favor of property would have undesirable effects and would further legitimize the commodification of digital information – a recent trend that is reinforced by certain interpretations of the DMCA on the part of lawmakers and by aggressive tactics used by the RIAA.

Key words: DMCA, intellectual property, Panopticon, privacy, RIAA, surveillance, Verizon

VERIZON v. RIAA: Background issues

In January 2003, a US district court, the Court of Appeals for the District of Columbia, ruled that Verizon (an Internet service provider) must comply with a subpoena by the Recording Industry Association of America (RIAA), a trade group representing the interests of the recording industry, requesting the name of a subscriber who allegedly made available more than 600 copyrighted music files over the Internet. This ruling sent shock waves throughout the Internet community, especially for those who saw the court's decision as one that advanced the interests of copyright owners at the expense of broader values such as freedom of speech and privacy in cyberspace.

The move on the part of the RIAA was part of its attempt to stop file sharing of copyrighted music over the Internet. Many Internet Service Providers (ISPs), such as Comcast, and many universities eventually complied with subpoenas issued on behalf of the RIAA. However, Verizon refused to hand over the names of its subscribers to the RIAA on the grounds that doing so violated specific articles of the U.S. Constitution. The RIAA contended that the Digital Millennium Copyright Act (DMCA) supported its demand. Verizon refused to comply with the subpoena, arguing that no illicit music was stored on its servers and that as an ISP, Verizon fell outside the scope of the subpoena. However, the District Court ruled that "the subpoena power ... applies to all Internet service providers within the scope of the DMCA, not just to those service providers storing information on a system or network at the direction of a user."[1]

In an appeals ruling on December 19, 2003, the United States Court of Appeals for the District of Columbia overturned the lower court's decision. The Appeals Court also noted that while it was

[1] R. Mark, "Court: Verizon Must Reveal Name of Alleged Online Pirate," http://dc.internet.com/news/article.php/1572591 accessed 10/9/03.

sympathetic to those who hold music copyrights, it was not in the court's purview to "rewrite the DMCA." Only Congress, the Court argued, could amend the DMCA to carry out the kind of enforcement measures requested by the RIAA.

Although we do not dispute the RIAA's claim that the copying and distribution of proprietary music has cost the recording industry millions of dollars, we believe that other important ethical issues also need to be examined in the *RIAA v. Verizon* dispute. Among those issues are the impacts that the RIAA's actions have for individual privacy, anonymous speech, and civil liberties in on-line activities. We also believe that in order to appreciate many of the controversial issues at stake in the *Verizon v. RIAA* dispute, it is important to understand certain aspects of the Peer-to-Peer (P2P) architecture used in the sharing of files over the Internet. Hence, we begin our analysis with some brief remarks about the P2P architecture that facilitates file sharing across computer networks.

P2P networks

The P2P architecture is a network of "peer machines," each identified with an IP (Internet Protocol) address. In this scheme, there are no fixed clients and servers. Thus all nodes on the network are equal, and they can both send and receive packets, lending themselves to a peer-to-peer distribution model of exchanging and sharing information. While P2P networks facilitate person-to-person communication and file sharing, they also open the door to abuse as the hierarchical constraint of one server overseeing the network has been removed.

P2P networks like KaZaA and Grokster use software to facilitate the sharing of music. Their applications identify all nodes on their networks by their IP addresses, which are unique identifiers. The P2P infrastructure facilitates this transfer, as any node can theoretically "talk" to any other node on the network, but it also opens the network up to snooping. Unlike Napster, which used a centralized database, creating a centralized point of vulnerability for attack by the RIAA, later P2P models sought to preserve node anonymity as much as possible by eliminating this hierarchical configuration. Most current implementations of the P2P architecture work on a *distributed* network structure. In these networks, each node maintains its own local database and each "talks" to a set of neighboring nodes when requesting a particular musical recording (e.g., a specific song) by a particular artist. The distributed algorithm of the network determines how this communication occurs. Generally, a responding node that has the requested song replies and the file is sent. The main point is that no one node knows about all the other nodes on the network, making surveillance of the network difficult but not impossible.

Newer versions of P2P networks go one step further in trying to protect the privacy of the individual by not using identifiable IP addresses; instead, random address strings are used. For example, Jason Rohrer developed a system of this type called MUTE. Each time a node connects, a new address is generated, making it extremely difficult to track. When a node requests a particular song, for instance, it sends the request to nearby nodes. If the song is not found, then those computers send out the request to the next set of nodes, etc. When the file is found, it is passed back through the network until it reaches the requestor. Thus the privacy and anonymity of the user is protected.

In order for RIAA to find out the identity of a node, it would have to track the entire network. "It's a scary environment to be living in when an organization like the RIAA can just snoop on what you're doing online," says Rohrer. "I've created a piece of software that helps people protect their privacy."[2] His response is reminiscent of that by Philip Zimmerman, who created Pretty Good Privacy (PGP), an email encryption program that was designed to help users protect the privacy of their email communications. A recent development, emerging from Freenet, is an ad-hoc network that connects computers via software, so there is "no corporate body that can be slapped with a court order."[3]

RIAA's attempt to use the DMCA to its advantage in its lawsuit focuses our attention on whether P2P architecture itself could conceivably fall under the restrictions of the law, thus opening the door for further legal actions. The United States Congress passed the DMCA in October of 1998, and it was enacted into law in 2000. DMCA was supported in large part by the software and entertainment industries, but it was opposed by many academics.[4] Two areas of the bill are problematic: Section 1201 and Section 512. An examination of Section 1201, which deals with circumvention of copyright protection systems, reveals that violations in this area fall into

[2] P. Eng, "Of Ants and Online Pirates: Insects Inspire 'Untraceable' Online File-sharing Network," Available at ABCNEWS.com, accessed 1/18/04.

[3] D. Briscoe, "On the Darknet", *Newsweek*, October 17, Vol. CXLVI, No. 16, 2005, p. E2.

[4] UCLA Online Institute for Cyberspace Law and Policy, "The Digital Millennium Copyright Act," http://www.gseis.ucla.edu/iclp/dcma1.htm, accessed 7/7/04.

the category of "deliberately working around technological measures" that are in place to protect copyright and do not deal with infrastructure at all. Furthermore, this subsection clearly states the "Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications or computing products."[5] So while this act limits ISPs from copyright infringement liability for transmission of material, as we have seen in the Verizon verdict, the RIAA expects these ISP's to: (1) take the responsibility of removing material from a user's website that would seem to violate copyright laws and (2) share the identity of copyright infringers. However, the latter action would also remove the protection of anonymity guaranteed under the First Amendment of the US Constitution. According to Section 512, however, once an ISP is informed about a possible infringement, it is up to the ISP, in order to protect its immunity, to disable access to the offending material.[6]

Arguably, the P2P distribution model seems to favor individual choice over social control. On one hand, it facilitates both open communication and freedom of speech because no one node in the network dominates; on the other hand, it opens up nodes to issues of trespass by other nodes, which can also disrupt service.[7] Individuals have the opportunity to join P2P networks; in fact, there are many communities of users associated with file-sharing networks. P2P networks became embroiled in the privacy vs. property controversy once those networks began to be used to download digitized versions of copyrighted music files.

Personal privacy

Privacy is a difficult concept to define. Often, privacy is closely associated with concepts such as liberty and autonomy. In the context of cyberspace, privacy is also frequently associated with concepts such as anonymity and security. The notion of privacy in the US has evolved during the past two centuries from one that initially was concerned with governmental intrusion (as expressed in the Fourth Amendment to the US Constitution), to worries about governmental interference involving one's personal decisions (expressed in important court decisions in the 1960s), to current concerns about access to and control of personal information.

Privacy is still sometimes defined in terms of *non-intrusion* into one's personal space[8], a view that traces its roots to a definition of privacy in a classic article by Warren and Brandeis.[9] At other times, privacy is defined in terms of *non-interference* into one's personal affairs.[10] And, more commonly today, privacy is viewed from the perspective of concerns having to do with access to and control over personal *information*.[11] On the whole, courts have seemed more comfortable ruling in cases involving issues of decisional privacy than with those of accessibility or informational privacy. This may be due to the fact that applying privacy laws designed for physical space to cyberspace has often been problematic. The problems arise, in part, because determining what counts as private space vs. public space in a networked infrastructure is not always easy. In addition, in cyberspace, the legal interpretation of what is afforded privacy protection is not always consistent with the public's perception of what those norms should be.

Privacy in P2P networks

While a user might think that working from her computer entitles her to an expectation that information stored on that computer is private, this is not necessarily the case. As soon as that computer becomes a node in a P2P network, it opens itself up to anything embedded in a message or file that is passed from node to node. This can also include viruses, and the problem can be exacerbated by the naivety of users, as well as their inexperience with file sharing programs. A user's privacy is preserved in these networks in part by the ISPs that provide Internet access, and by the infrastructure of the P2P networks themselves.

Later, we will see how the Verizon case brings into focus the need to reassess the interpretation of privacy and property law as it applies to the networked infrastructure and the Internet in general. We will also see that the lawsuits advanced by the RIAA, which attempt to place enforcement of copyright laws

[5] Digital Millennium Copyright Act, Available at http://Thomas.loc.gov. Accessed 6/21/04.

[6] S. Katyal, "The New Surveillance," *Case Western Law Review*, Vol. 54, 2004. Also available at http://islandia.law.yale.edu.

[7] For example, P2P networks can be used to launch distributed denial-of-service attacks.

[8] This view of privacy is sometimes called "accessibility privacy."

[9] S. Warren and L. Brandeis, "The Right to Privacy," *Harvard Law Review*, Vol. 14, No. 5, 1890.

[10] This view is sometimes described as "decisional privacy."

[11] Some refer to this view of privacy as "informational privacy."

into the hands of service providers, are based on laws that are, as Jessica Litman[12] suggests, at best murky – and perhaps even "made-up rules."

Distinguishing between naturally private and normatively private situations

We defend a definition of privacy introduced by James Moor,[13] which incorporates key elements of the non-intrusion, non-interference, and informational views of privacy into a unified theory. According to Moor, an individual "has privacy in a *situation* if in that particular situation the individual is *protected from intrusion, interference, and information access* by others." [Italics Added] An important aspect in this definition is Moor's notion of a "situation." His definition of a *situation* is left deliberately broad so that it can apply to a range of contexts or "zones" that can be "declared private" in a normative sense. In other words, a situation can be an "activity," a "relationship," or the "storage and access of information" in a computer or on the Internet. For example, a P2P context in cyberspace fits Moor's notion of a situation. Should such a situation receive privacy protection?

Central to Moor's theory is a distinction between *naturally private* and *normatively private* situations. Moor's distinction enables us to differentiate between the conditions required for: (a) having privacy, and (b) having a right to privacy. This distinction, in turn, enables us to differentiate between a loss of privacy and a violation of privacy. Privacy can be violated only in "normatively private situation" because it is only in those kinds of situations that zones or contexts that merit some kind of normative protection have been *formally* established. Implicit in this definition is that if you own something like a house, you have the right to privacy within that house. Does that also apply to a computer connected to a network? The problem for cyberspace is that it is difficult to expand the metaphor of a zone to an infrastructure of networks. Yet, the perception of users is that if they own their computers they are entitled to a zone of privacy around them even when they are connected, for example, to a university network. So, for example, if we declare a P2P context to be normatively private, then organizations like the RIAA violate the privacy of individuals whenever they succeed in identifying the names of users via subpoenas directed at ISPs. Should P2P contexts, in particular, be declared normatively private situations and should ISPs be required to enforce surveillance policies of private–sector organizations like the RIAA? If so, should we presume in favor of protecting privacy as a starting point in negotiations, as DeCew[14] suggests? Perhaps the answer to this question presupposes an answer to a larger question: Why do/should we value privacy?

Some have argued that privacy is valuable because it is essential for individual autonomy. James Rachels[15] notes that having privacy enables us to control how much personal information we wish to disclose to others and how much we elect not to divulge. Thus one important value of privacy is that it enables us to form relationships with individuals, ranging from intimate to casual, by being able to control how much information about ourselves we elect to grant to or withhold from others. Because privacy enables us to form a diversity of relationships, Rachels suggest that privacy is essential for friendship and trust.

James Moor believes that privacy is the articulation or expression of a "core value," viz., *security*, which he further argues is essential for human flourishing in all societies. Implicit in Moor's definition of privacy is the notion of freedom from surveillance. If one is being constantly watched, all expectations of privacy disappear. Many privacy advocates also worry that surveillance stifles creativity and human flourishing, and they note that people who are constantly watched tend to alter their behavior.

Panoptic surveillance and P2P networks

Some privacy analysts compare the kind of surveillance made possible by contemporary information technology to the classical Panopticon. The Panopticon, a prison designed by Jeremy Bentham and discussed extensively by Michel Foucault in the twentieth century, was more than just a building. Its central tower enabled guards to watch prisoners constantly and for prisoners to know, by the presence of the tower that they were watched. Power and control were instilled through constant surveillance. The metaphor of the Panopticon in cybertechnology

[12] J. Litman, "Ethical Disobedience," *Ethics and Information Technology*, Vol. 5, No. 4, 2003, pp. 217–223.

[13] J. H. Moor, "Towards a Theory of Privacy for the Information Age." In R. A. Spinello and H. T. Tavani, editors. *Readings in CyberEthics*. 2nd ed. Sudbury, MA: Jones and Bartlett, 2004, pp. 407–417.

[14] J. W. DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, New York: Cornell University Press, 1997.

[15] J. Rachels, "Why Privacy Is Important." In D.G. Johnson and H. Nissenbaum, editors. *Computing, Ethics and Social Values*. Upper Saddle River, NJ: Prentice Hall, 1995, pp. 351–357.

has come to represent surveillance that is ever-present but not necessarily verifiable. For example, students know that they are working on university-owned networks, but they can never be sure when someone controlling the network is snooping around to see who is downloading files or sending suspicious email. This can create a state of anxiety for the user, e.g., a fear that someone is watching.

In the past, users of P2P networks assumed that they were immune to surveillance because of the decentralized and distributive nature of the network. Sonia Katyal points out

> a transformation has taken place. Panoptic control has just begun in the peer-to-peer realm...it involves a level of intangible invasion and technological surveillance that seemingly escapes legal regulation.[16]

Earlier, we noted that many ISPs responded to RIAA lawsuits by revealing the names of their subscribers – i.e., subscribers who were forced to share their personal information in order to join the ISP. Arguably, these subscribers lost autonomy and privacy based on the accusations of an organization that does not have clear or unambiguous legal status. The mere threat of litigation based on liability was sufficient to shut down web sites and to violate anonymity.

Why has surveillance taken on such a prominent role in the privacy vs. property debate? Katyal suggests that when the court presiding in the Napster case placed the burden on copyright owners to identify the infringers, it opened up an entire new industry that has content owners searching the Internet for potential infringers.[17]

Intellectual property rights and P2P networks: The conflict between privacy and property

The emergence of file sharing over P2P networks has raised the question about where the presumption, or default view, should be when competing interests such as privacy and property are at stake. We will defend the view for a presumption in favor of privacy; advocates for strong property protection, however, would no doubt argue for a presumption in favor of property rights. The conflict between privacy and property rights in cyberspace can be understood as a tension involving issues of *access and control*.[18] Consider that property-rights advocates argue for greater control over information that they view to be proprietary, thus denying ordinary individuals free access to that information; at the same time, however, these advocates want unfettered access to information about individuals, such as in the case involving the RIAA demands on Verizon for the names of customers. Privacy advocates, on the other hand, argue for individuals having greater control over their own personal information and space. Yet many who advocate for stronger control over their personal information also desire greater access to digital information, including on-line music.

We next examine the application and the relevance of some traditional copyright schemes in cyberspace and their relationship to surveillance. In doing so, we look at how the rules designed to protect proprietary information play out in the public domain of cyberspace, where it is estimated that more than 60 million people share music files. In particular, we examine a model that we believe strikes a fairer balance between property and privacy interests, because it both rewards the composers of digital music and preserves the privacy of individual users who share files via P2P networks. First, however, we examine some arguments used to justify copyright protection.

Copyright law and the rationale for according legal protection to information

According to Jessica Litman,[19] the original purpose of the copyright law in the U.S. was to encourage the production and dissemination of works of authorship. It was a model that encouraged sharing because it required authors who wanted copyright protection to request it. It also made it relatively easy to obtain permission to use copyrighted material because people knew whom to ask. The essential point here is that it forced everything else into the public domain. Litman points out that this began to change with the passage of the Copyright Revision Act in 1976, when:

> ...we abolished the rule that publication without notice or with inaccurate notice sent the work into the public domain and in 1989...[when]...we abolished the notice requirement entirely.[20]

The result of these changes was to reverse the default rule and to extend the scope of copyright to anything that is *potentially* copyrightable whether or not authors themselves seek copyright protection. In

[16] S. Katyal, op. cit., p. 24.
[17] Ibid., p. 34.
[18] H.T. Tavani, *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Hoboken, NJ: John Wiley and Sons, 2004.
[19] J. Litman, *Sharing and Stealing*, 2004. Available at http://www.law.wayne.edu/litman/papers/sharing&stealing.pdf, accessed 4/22/05, p. 2.
[20] Ibid., p. 17.

effect, these changes have contributed to the "shrinking" of the public domain. This plays out in a very unfortunate way in cyberspace where, until recently, information traditionally had been shared, used, and reused. According to the modifications in the current U.S. Copyright Law, neither digital music nor any other kind of copyrighted information can be used without permission. However, it is not always obvious where to go to obtain these rights. In addition, any distribution, reproduction, or performance of this copyrighted material also needs proper authorization. Because organizations like the RIAA are trying to make the mere possession of a copy of a digital work that may possibly used for distribution a crime, a new "conceptual muddle" may be emerging with respect to current copyright laws.

The U.S. Congress has also weighed in on copyright issues involving digital information. Litman reports that the Author, Consumer and Computer Owner Protection and Security Act, proposed by Congressman Conyers, would make it a crime to put any copyrighted material on a computer network that is accessible to the public unless one had the permission of the copyright owner. This law would extend to home, as well as to commercial, networks. One problem in applying this law to cases involving digital music, however, is that ownership rights involving this kind of information are often uncertain, unknown, or vague. Often times, it would take a rigorous examination of legal contracts to determine who had the authority to give permission, and it is not altogether clear that "electronic rights" are even included in the contracts.

Katyal believes that "copyright owners now undertake a widening degree of control over cultural products through the guise of piracy detection."[21] She also notes that copyright owners, in their attempts to catch copiers of intellectual property online, have "trespassed on a person's expectations of informational privacy and anonymity"[22] by taking surveillance into their own hands. Katyal makes the point that by allowing extra-judicial enforcement of copyright, legal proof of piracy gives way to schemes where everyone is under suspicion. For example, universities have responded to the threat of RIAA lawsuits by monitoring downloading activities at their institutions, and web-crawlers are moving through P2P networks looking for suspicious activities. The excuse to protect property has exposed all of us to unwanted and often unwarranted surveillance, which also has implications for fair use as well as for creativity when people are monitored as potential violators. It also sets up ISPs as a defacto governance tool, as they are being asked not only to oversee their network connections but also to monitor them. As Katyal aptly states:

> ...the premise of piracy surveillance suggests the need to revisit the importance of recognizing the cost of technologies of invasion on consumer autonomy and access to information.[23]

Digital information and digital music in the public domain of cyberspace

If both digitized information and digitized music can be easily shared in cyberspace, why is the sharing of one acceptable and the sharing of the other not? Scholars, who have tried to differentiate between digital information and digital music, have generally concluded that a principal or key distinguishing feature is that digital music is proprietary and ordinary information is not. One might argue that publishers are equally protective of journal articles and books as the RIAA is of music. One major difference, however, is that digitized music does not usually fall under the rubric of "fair use" or inclusion in scholarly works. In addition, it is easier to find and obtain permissions from publishers of this kind of material, when necessary. Digital information in the public domain – i.e., non-proprietary digital information – is shared for a variety of ways and for a variety of uses. For example, some people post and respond to material, and others write open source programs that are available for use and extended development. This process of information sharing provides a low cost model of distributing information without many difficulties. However, critics of this model argue that, with respect to digitized music, someone typically has legal ownership rights and claims. Yet, according to Litman, some scholars have "deconstructed" the rationales for giving different treatment to music and facts; some have concluded that because the differences cannot be defended, we should seek legal mechanisms for protecting facts as well. However, she dismisses this argument, pointing out that it is "backwards." Litman writes:

> If facts and music are equivalent in the respects that matter, and we have an ample readily accessible and diverse supply of facts when the law gives them no protection, shouldn't we at least investigate what sort of musical smorgasbord we might develop if we treated music comparably?[24]

[21] S. Katyal, op. cit., p. 1.
[22] Ibid., p. 4.
[23] Ibid., p. 79.
[24] J. Litman, *Sharing and Stealing*, op. cit., p. 24.

Katyal, writing from the perspective of surveillance, tends to agree with Litman when she points out that the law "has opted to expand property rights, rather than to create a comprehensive scheme to protect individuals from unwanted surveillance."[25] Both Litman and Katyal also suggest that there should be a way of balancing the protection of property with privacy.

One serious flaw in current P2P schemes used to share music is that the creator of the music does not typically receive any monetary compensation. So to extend to music the same openness that we do to facts, we also would have to find a way to ensure that creators of music were fairly and justly compensated. Doing so would keep the production line open; that is, musicians would be encouraged to compose new music because of financial incentives that are clearly and explicitly articulated, and they would be free to market their musical compositions over the Internet. The RIAA, of course, would have no interest in such a solution, because, as a "middleman," it would be virtually eliminated; the current copyright status quo is clearly in the RIAA's best interest. Musicians, on the other hand, would have more autonomy, including a greater say about the decisions as to how and where to distribute their music. If the estimate that while 60 million people are currently sharing music via P2P networks musicians receive no monetary compensation is correct, then we agree with Litman and others that a different kind of distribution model is needed.

Litman's distribution model

Various models have recently emerged in response to the problem of music distribution over P2P networks. One feature common in all of these models is that the default practice should be *to share* and not to hoard information.[26] Models by Lessig, Ku, Gervais and Fisher, among others, suggest schemes for supporting "consumer to consumer distribution"[27] that compensate the creators of music rather than the "middlemen." Some models and schemes suggest extending licenses to fans to allow them to share music for a small fee; others suggest that levies be attached to Internet services involving audio and video equipment.

Litman's model expands upon ideas suggested in some of these earlier proposals; it also responds to her concern that as more and more people embrace P2P file sharing, more and more legislation that maintains the "asymmetrical power structure" of private interests over those of the consumers will be enacted. For this reason, Litman believes that by sheer numbers alone, those engaged in P2P network sharing have a right, if not an obligation, to weigh in on the discussion. Her vision of a "music space" is one that contains a wide spectrum of music that can be easily shared, either through blanket fees or by way of levies that would fairly compensate the composers of the music. In other words, *the default should be sharing*! However, composers would also have the choice of opting out of this system by withholding their music from distribution mechanisms designed to share music.

We believe that composers should be encouraged to participate in file-sharing models. One way to encourage their participation is to demonstrate to them that the proposed licensing models actually work – i.e., these models would ensure a system of compensation for the composers that is fair and just. Litman also points out that in her scheme, if any other "intermediaries" were currently contractually bound to receive fees, they would still receive those fees.

Concluding remarks

We have chosen privacy and property concerns as two key topics on which to focus our discussion of moral implications in the *Verizon v. RIAA* case. Elsewhere, we have examined some implications that this case has for democracy and freedom[28] and civil liberties[29] in cyberspace. Clearly, property-right issues are very much at the heart of the Verizon case, especially from the point of view of the RIAA, which is interested in protecting its proprietary information from being exchanged freely over the Internet via P2P networks. Because of this concern, some might argue that the "presumption in favor of privacy" that we have defended can be counterbalanced by a presumption in favor of protecting intellectual property rights.

However, we believe that another presumptive principle can be brought into play here. In particular, we defend the principle "Information Wants to Be Shared," which presumes against the "fencing off" or

[25] S. Katyal, op. cit., p. 13.

[26] Here, the presumption is that we should preserve and possibly expand, not shrink, the public domain.

[27] See J. Litman, *Sharing and Stealing* (op. cit.) for a detailed discussion of these models.

[28] F.S. Grodzinsky and H.T. Tavani. "The *Verizon v. RIAA* Case: Implications for Privacy and Democracy in Cyberspace." In *Proceedings of the 2004 International Symposium on Technology and Society*. New York: IEEE Press, 2004, pp. 49–53.

[29] See H.T. Tavani and F.S. Grodzinsky. "Threat to Democratic Ideals in Cyberspace: Lessons Learned From the *Verizon v. RIAA* Case," *IEEE Technology and Society Magazine*, Vol. 24, No. 3, Fall, 2005, pp. 40–44.

enclosing of information in favor of a view of information as something that should be communicated and shared.[30] We further believe that this presumptive principle could help to reverse the recent trend to turn all digitized information into a "commodity" that can be hoarded and thus made more exclusive. We also believe that when our presumptive principle – advocating for the *sharing* of information as a default position – is combined with the interests at stake for protecting values such as privacy and anonymity in the current debate involving Verizon and the RIAA, we can justify a policy that tilts in favor of defending the position articulated by Verizon rather the one advanced by the RIAA.

In defense of a presumptive principle of sharing as our default position, we briefly examined a proposal for a distribution model advocated by Jessica Litman, which both rewards the creator of digital music (and of other forms of proprietary information in digitized form) and protects the interests of file sharers using P2P networks. In such a scheme, it would seem that the only ones who are disadvantaged monetarily are the "middlemen" (e.g., the RIAA). It would also seem that if a model similar to the one advocated by Litman were adopted, many of the privacy conflicts currently surrounding P2P networks (such as those in the *Verizon v. RIAA* dispute), could be resolved easily and fairly, and the perceived need for surveillance reduced or eliminated.

Acknowledgments

An earlier version of this paper was presented at CEPE 2005, Twente University, July 17–19, 2005. We are grateful for comments received from conference participants. In composing this paper, we drew from material in two previously published works: Grodzinsky and Tavani (2004) and Tavani and Grodzinsky (2005).

References

D. Briscoe. On the Darknet. *Newsweek*, October 17, Vol. CXLVI, No. 16, 2005, p. E2.

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

Digital Millennium Copyright Act. Available at: http://Thomas.loc.gov., accessed 6/21/04.

P. Eng. Of Ants and Online Pirates: Insects Inspire 'Untraceable' Online File-sharing Network., Available at: ABCNEWS.com, accessed 1/18/04.

F.S. Grodzinsky and H.T. Tavani. The *Verizon v. RIAA* Case: Implications for Privacy and Democracy in Cyberspace. In *Proceedings of the 2004 International Symposium on Technology and Society*. pp. 49–53. IEEE Press, New York, 2004.

S.K. Katyal. The New Surveillance. *Case Western Law Review*, Vol. 54, 297, 2004. Also available at: http://islandia.law.yale.edu.

J. Litman. Ethical Disobedience. *Ethics and Information Technology*, 5(4): 217–223, 2003.

J. Litman. *Sharing and Stealing*, 2004. Available at http://www.law.wayne.edu/litman/papers/sharing&stealing.pdf, accessed 4/22/05.

R. Mark. Court: Verizon Must Reveal Name of Alleged Online Pirate. Available at: http://dc.internet.com/news/article.php/1572591, accessed 10/9/03.

J.H. Moor. Towards a Theory of Privacy for the Information Age. In R.A. Spinello and H.T. Tavani, editors, Readings in CyberEthics 2 ed., pp. 407–417. Jones and Bartlett, Sudbury, MA, 2004.

J. Rachels. Why Privacy is Important. In D.G. Johnson and H. Nissenbaum, editors, Computing, Ethics and Social Values, pp. 351–357. Prentice Hall, Upper Saddle River, NJ, 1995.

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

H.T. Tavani and F.S. Grodzinsky. Threat to Democratic Ideals in Cyberspace: Lessons Learned From the *Verizon v. RIAA* Case. *IEEE Technology and Society Magazine*, 24(3): 40–44, Fall 2005.

UCLA Online Institute for Cyberspace Law and Policy. The Digital Millennium Copyright Act. http://www.gseis.ucla.edu/iclp/dcma1.htm, accessed 7/7/04.

S. Warren and L. Brandeis. The Right to Privacy. *Harvard Law Review*, 14(5): 1980.

[30] H.T. Tavani, *Ethics and Technology*, op. cit.