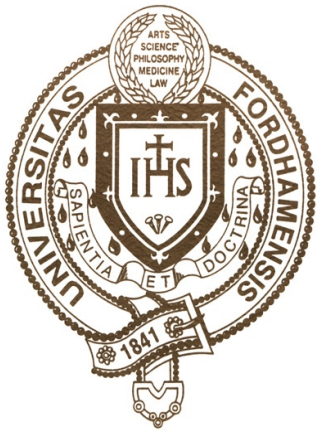
Fordham University School of Law



May 2005

Privacy vs. Piracy

By

Sonia K. Katyal
Professor

7 Yale J. Law & Tech. 222 (2004)

ARTICLE

PRIVACY VS. PIRACY

SONIA K. KATYAL*

This article was jointly reviewed and edited by YALE JOURNAL OF LAW & TECHNOLOGY and INTERNATIONAL JOURNAL OF COMMUNICATIONS LAW & POLICY

* Associate Professor, Fordham University School of Law. Another version of this paper, titled The New Surveillance, was published in the Case Western Law Review in Winter 2003.

For helpful comments, the author thanks the participants at the Yale Cybercrime and Digital Law Enforcement Conference, as well as the editors of the Yale Journal of Law and Technology, along with Ann Bartow, Jonathan Barnett, Dan Capra, George Conk, Robin Feldman, Jill Fisch, Eric Goldman, Ellen Goodman, Hugh Hansen, Jennifer Higgins, Justin Hughes, Jacqueline Lipton, Robert Kaczorowski, Neal Katyal, Orin Kerr, Thomas Lee, Mark Lemley, Laura Heymann, Howard Knopf, Esther Lucero, Glynn Lunney, Peter Menell, Joel Reidenberg, Peter Siegelman, Damien Stolarz, Kim Taipale, Rebecca Tushnet, Polk Wagner, Fred Von Lohmann, Peter Yu, Tal Zarsky and Benjamin Zipursky. John Farmer, Allison Schilling, and Jayson Mallie all provided excellent research assistance.

PRIVACY VS. PIRACY

SONIA K. KATYAL

A few years ago, it was fanciful to imagine a world where intellectual property owners – such as record companies, software owners, and publishers – were capable of invading the most sacred areas of the home in order to track, deter, and control uses of their products. Yet, today, strategies of copyright enforcement have rapidly multiplied, each strategy more invasive than the last. This new surveillance exposes the paradoxical nature of the Internet: It offers both the consumer and creator a seemingly endless capacity for human expression – a virtual marketplace of ideas – alongside an insurmountable array of capacities for panoptic surveillance. As a result, the Internet both enables and silences speech, often simultaneously.

This paradox, in turn, leads to the tension between privacy and intellectual property. Both areas of law face significant challenges because of technology's ever-increasing pace of development. Yet courts often exacerbate these challenges by sacrificing one area of law for the other, by eroding principles of informational privacy for the sake of unlimited control over intellectual property. Laws developed to address the problem of online piracy – in particular, the DMCA – have been unwittingly misplaced, inviting intellectual property owners to create private systems of copyright monitoring that I refer to as piracy surveillance. Piracy surveillance comprises extrajudicial methods of copyright enforcement that detect, deter, and control acts of consumer infringement.

In the past, legislators and scholars have focused their attention on other, more visible methods of surveillance, namely those relating to employment, marketing, and national security. Piracy surveillance, however, represents an overlooked fourth area that is completely distinct from these other types, yet incompletely theorized, technologically unbounded, and, potentially, legally unrestrained. The goals of this Article are threefold: first, to trace the origins of piracy surveillance through recent jurisprudence involving copyright; second, to provide an analysis of the tradeoffs between public and private

enforcement of copyright; and third, to suggest some ways in which the law can restore a balance between the protection of copyright and civil liberties in cyberspace.

This paper was selected as the winning entry for the 2004 Yale Law School Cybercrime and Digital Law Enforcement Conference writing competition, sponsored by the Yale Law School Information Society Project and the Yale Journal of Law and Technology.

Nearly twenty years ago, in a casual footnote at the end of an important essay, renowned property scholar Charles Donahue drew a distinction between "property as a sword," and "property as a shield."[1] Donahue's distinction symbolized an important difference between two facets of the institution—as well as the execution—of property rights; suggesting that property rights can be used for both defensive and offensive purposes in relationships with third parties.

Today, Donahue's distinction offers us a rich metaphor for understanding the transformation that has taken place in the digital era, particularly with respect to the relationship between intellectual property and privacy in cyberspace. As is now clear, the Internet is no longer a smooth-functioning patchwork of anonymous communication between peers. Instead, lurking behind the façade of such potential connections lies an increasing and subtle host of opportunities for legal accountability and detection, particularly where the use (or misuse) of intellectual property is concerned. The result, this paper argues, heralds an important shift in property rights in the digital era: compared to real space, where property rights tended to serve as a shield from harm, property rights in cyberspace serve to form the basis for a host of potentially offensive strategies that have deleterious implications for privacy, anonymity, and freedom of expression.

In recent months, strategies of copyright enforcement have rapidly multiplied, each strategy more invasive than the last. Today, the Recording Industry Association of America

---

1 Charles Donahue, Jr., *The Future of the Concept of Property Predicated From its Past*, *in* PROPERTY 28, 67-8 n.104 (J. Roland Pennock & John W. Chapman eds., 1980).

(RIAA) and other copyright owners maintain automated Web crawlers that regularly survey and record the Internet Protocol addresses of computers that trade files on peer-to-peer networks.[2] After the RIAA's initial victories, hundreds of subpoenas were issued—sometimes numbering seventy-five per day—each unveiling the digital identities of various Internet subscribers.[3] Schools, responding to threats from the recording industry, have implemented programs that track and report the exchange of copyrighted files.[4] A few have even decided to audit and actively monitor files traded by their students, at the RIAA's request.[5] And in recent sessions, there were proposals

---

2 *See infra* Part II.

3 Ted Bridis, *Music Lawsuits Amass 75 Subpoenas Per Day*, AP ONLINE, July 19, 2003; Katie Dean, *RIAA Legal Landslide Begins*, WIRED NEWS, Sept. 8, 2003, *at* http://www.wired.com/news/digiwood/0,1412,60345,00.html.

4 *See, e.g.*, Leonie Lamont, *Firms Ask to Scan University Files*, SYDNEY MORNING HERALD, Feb. 19, 2003, at 3 (reporting that recording companies asked for permission to scan all computers at the University of Melbourne for sound files, in order to gather evidence of alleged breaches of copyright); *see also* VIRGINIA E. REZMIERSKI & NATHANIEL ST. CLAIR II, FINAL REPORT NSF-LAMP PROJECT: IDENTIFYING WHERE TECHNOLOGY LOGGING AND MONITORING FOR INCREASED SECURITY END AND VIOLATIONS OF PERSONAL PRIVACY AND STUDENT RECORDS BEGIN (2001), *available at* http://www.nacua.org/documents/NSF_LAMP.pdf (on file with the Yale Journal of Law and Technology); Electronic Frontier Foundation, *Universities Should Resist Network Monitoring Demands*, *at* http://www.eff.org/IP/P2P/university-monitoring.pdf (on file with the Yale Journal of Law and Technology) (last visited Dec. 6, 2004); Letter from Electronic Privacy Information Center on P2P Monitoring to Colleges and Universities, Nov. 6, 2002, *at* http://www.epic.org/privacy/student/p2pletter.html (on file with the Yale Journal of Law and Technology); Kristen Philipkoski, *University Snoops for MP3s*, WIRED NEWS, Nov. 13, 1999, *at* http://www.wired.com/news/ technology/0,1282,32478,00.html.

5 *See* Lamont, *supra* note 4, at 3; Kelly McCullom, *How Forcefully Should Universities Enforce Copyright Law on Audio Files?*, CHRONICLE OF HIGHER EDUCATION (Nov. 19, 1999). In April 2003, the RIAA also filed suits directly against four college students accused of operating file sharing networks for the purposes of copyright infringement. *See RIAA Sues College File Traders*, WIRED NEWS, Apr. 3, 2003, *at* http://www.wired.com/news/technology/0,1282,58340,00.html. Many more suits have followed since. *See* Recording Industry Association of America, *Illegal File Sharing Targeted in Wave of New Lawuits*, Nov. 18, 2004, *at* http://www.riaa.com/news/newsletter/111804.asp (describing suits against peer-to-peer network users on college and university campuses in Massachusetts, Iowa, Virginia, and Washington D.C.); Electronic Frontier Foundation, *RIAA v. The People*, *at* http://www.eff.org/IP/P2P/riaa-v-thepeople.php (last accessed Dec. 6, 2004) (comprehensive list of suits brought by RIAA and member companies) (on file with the Yale Journal of

before Congress that placed intellectual property owners in a virtually unrestrained position of authority over ordinary consumers and intermediaries.[6] The latest of these, the Protecting Intellectual Property Rights Against Theft and Expropriation (PIRATE) Act, sought to lower the burden of proof to impose criminal penalties on individuals that engaged in acts of file-sharing, including sentences of up to 10 years.[7]

Law and Technology).

6 In 2002, Rep. Howard Berman introduced the Peer-to-Peer Piracy Prevention Act (2002), which would have protected copyright owners who engaged in acts of self-help to protect their works, H.R. 5211, 107th Cong. (2002), 18 U.S.C.A. § 1030; *see also* Howard L. Berman, *The Truth About the Peer to Peer Piracy Prevention Act: Why Copyright Owner Self-help Must Be Part of the P2P Piracy Solution*, FIND LAW, Oct. 1, 2002, *at* http://writ.news.findlaw.com/commentary/20021001_berman.html. During the summer of 2003, Senator Orrin Hatch proposed destroying the computers of individuals who illegally download material, pointing out that damaging someone's computer "may be the only way you can teach somebody about copyrights." *Senator Takes Aim at Illegal Downloads*, AP ONLINE, June 18, 2003 (on file with the Yale Journal of Law and Technology). Representative John Carter (R-TX) also suggested that jailing college students for piracy would deter other infringers. Katie Dean, *Marking File Traders as Felons*, WIRED NEWS, Mar. 19, 2003, *at* http://www.wired.com/news/business/0,1367,58081,00.html. In 2004, Congress considered the Inducing Infringement of Copyright Act of 2004, which aimed to hold software creators liable for the infringing activities of their consumers. *See* 2003 CONG US S. 2560, introduced June 22, 2004; Xeni Jardin, *Induce Act Draws Support, Venom*, WIRED NEWS, Aug. 26, 2004, *at* http://www.wired.com/news/print/0,1294,64723,00.html; Katie Dean, *Copyright Proposal Induces Worry*, WIRED NEWS, Sept. 11, 2004, *at* http://www.wired.com/news/politics/0,1283,64870,00.html; Katie Dean, *Big Anti-Induce Campaign Planned*, WIRED NEWS, Sept. 14, 2004, *at* http://www.wired.com/news/politics/0,1283,64935,00.html. Eventually the Induce Act was shelved, ostensibly due to the outcry among technology companies. See Katie Dean, *Senate Shelves Induce Review*, WIRED NEWS, Oct. 7, 2004, *at* http://www.wired.com/ news/politics/0,1283,65255,00.html. Just a week later, however, former Attorney General John Ashcroft vowed to "build the strongest, most aggressive legal assault against intellectual property crime in our nation's history," see Katie Dean, *Ashcroft Vows Piracy Assault*, WIRED NEWS, Oct. 14, 2004, *at* http://www.wired.com/news/politics/0,1283,65331,00.html.

7 *See* Xeni Jardin, *Congress Moves to Criminalize P2P*, WIRED NEWS, Mar. 26, 2004, *at* http://www.wired.com/news/digiwood/0,1412,62830,00.html; Xeni Jardin, *Feds Crank up Heat on P2P*, WIRED NEWS, Mar. 31, 2004, *at* http://www.wired.com/news/digiwood/0,1412,62895,00.html; Declan McCullogh, *'Pirate Act' Raises Civil Rights Concerns*, May 26, 2004, *at* http://news.com.com/'Pirate+Act'+raises+civil+rights+concerns/2100-1027_3-5220480.html; Roy Mark, *Conservatives Aim to Sink Pirate Act*, INTERNETNEWS, Nov. 12, 2004, *at* http://www.internetnews.com/bus-news/article.php/3435421. *See also* the

All of these different strategies share one thing in common: they rely on, invariably, private mechanisms of surveillance for their execution and control. And these techniques of surveillance—whether instituted by private entities, or public law enforcement—demonstrate copyright's increasingly tenuous relationship with information privacy. In the past, legislators and scholars have focused their attention on other, more visible methods of surveillance relating to employment, marketing, and national security.[8] This paper, however, explores the phenomenon of "piracy surveillance," an emerging area that is completely distinct from these other modes of consumer monitoring, and is incompletely theorized, technologically unbounded, and, potentially, legally unrestrained. As I will show, recent developments in copyright law– in particular, the DMCA – have invited intellectual property owners to create extrajudicial systems of monitoring and enforcement that detect, deter, and control acts of consumer infringement. As a result, this paper argues that intellectual property rights have been fundamentally altered—from a defensive shield into an offensively oriented type of weapon that can be used by intellectual property creators to record the activities of their consumers, and also to enforce particular standards of use and expression, proscribing activities that they deem unacceptable.

This outcome is not solely attributable to the development of peer-to-peer technologies, or the explosion of piracy in cyberspace, as some might suggest. Rather, the outcome involves the comparatively more subtle failure of law to resolve the troubling and often rivalrous relationship between the protection of intellectual property and privacy in cyberspace. The irony, of course, is that both areas of law are facing enormous challenges because of technology's ever-expanding pace of development. Yet, while both areas of law have enormously rich and well-developed areas of scholarly work and

---

Protecting Intellectual Rights Against Theft and Expropriation Act of 2004, S. 2237 (108th Congress); John P. Mello, Jr., *Proposed Bill Would Criminalize File Sharing*, TECHNEWSWORLD, Mar. 30, 2004, *at* http://www.technewsworld.com/ story/33262.html (on file with the Yale Journal of Law and Technology).

8 David Lyon, *The World Wide Web of Surveillance: The Internet and Off-World Power Flows*, *in* THE MEDIA READER: CONTINUITY AND TRANSFORMATION 353, 355 (Hugh MacKay & Tim O'Sullivan eds., 2000) (asserting the proliferation of three main categories of cyberspace surveillance relating to employment, security and policing, and marketing).

analysis, their interactions, particularly across the Internet, have been underappreciated by scholars. Today, however, they are on a collision course that cannot be overlooked much longer, sparked by two major developments in digital space: the rise of consumer surveillance, and the problem of rampant piracy.

The motivation behind piracy surveillance may lie in the protection of copyrighted works, a laudable goal, but the end result, I shall argue, sacrifices the most valuable aspects of cyberspace itself, eviscerating principles of informational privacy for the sake of unlimited control over intellectual property. While some intellectual property owners might herald the development of protective frameworks for intellectual property owners, I argue that it destabilizes a critical balance between privacy, property, and expression. For the new piracy surveillance exposes the paradoxical nature of the Internet: it offers both the consumer and creator a seemingly endless capacity for human expression—a virtual marketplace of ideas—alongside an insurmountable array of capacities for panoptic surveillance. As a result, the Internet both enables and silences speech, often simultaneously.

The goals of this paper are threefold: first, to trace the origins of piracy surveillance though recent jurisprudence involving copyright; second, to provide an analysis of the tradeoffs between public and private modes of piracy surveillance; and third, to suggest the necessity for the law to restore a balance between the protection of copyright and civil liberties in cyberspace. As I will show, piracy surveillance has inverted the relationship between privacy and property, subordinating the protection of privacy to the protection of property. This has occurred in two basic ways: first, piracy surveillance enables copyright owners to utilize a type of monitoring that demonstrably trespasses on a person's expectations of informational privacy and anonymity; and second, the use of piracy surveillance strategies, without conventional substantive and procedural due process constraints, has a harmful tendency to chill free expression in cyberspace.

In the first section of this paper, I review some basic principles of the relationship between privacy and property in real space, and then apply them to cyberspace. I begin by surmising some of the basic assumptions that are both descriptively and aspirationally present in property ownership,

and then argue that the architecture of cyberspace has destabilized the preexisting balance between privacy and property by eliminating the material conditions that permit the exercise of spatial privacy. Unlike property ownership in real space, which presupposes a degree of privacy by virtue of material seclusion, the public and private nature of property in cyberspace—coupled with its immense digital mobility and decentralization—often come into conflict with one another, interacting within a sphere of confusing uncertainty. Instead of material seclusion, individuals operate under an assumption of anonymity, which significantly expands their expressive potential in cyberspace. At the same time, however, information harvesting is rampant, a factor which alters any presumption of balance between privacy and property in cyberspace.

Nowhere is this better illustrated than in the context of peer-to-peer transmissions. Here, I describe how peer-to-peer transmissions have enabled the rapid transmission of content, such as music, film and other types of copyrighted material, facilitating a crisis of intellectual property. But it has also created a sort of crisis for privacy and security, as well. By making one's online activities, identities, and preferences transparently visible, peer-to-peer frameworks create a culture of panopticism by other individuals. This culture of panopticism, in turn, enables a variety of entities—government, private individuals, and copyright owners—to exploit the power of peer-to-peer frameworks to develop an increasingly invasive system of surveillance to guard against piracy.

In the second section, I turn to the origins of piracy surveillance, and describe the myriad ways in which private entities have successfully monitored transmissions in cyberspace to control uses of their copyrighted materials. Following the DMCA, I argue, court opinions have unwittingly facilitated the creation of a private regime wherein copyright owners and intermediaries engage in self-help surveillance of consumers. Piracy surveillance regimes take on three basic types, each displaying varying degrees of unilateral aggression: *monitoring*, which involves the use of automated systems to search for protected material; *management*, which involves a host of actions taken in real space and cyberspace to limit certain uses of cultural products; and *interference*, which involves a degree of preventative actions taken to prevent peer-to-peer file-sharing from occurring.

In the third section, I assess the costs and benefits of such regimes, and argue that current, private regimes of copyright enforcement carry significant disadvantages, among them the potential to transform copyright law into a regime of "panoptic publication," where future creators are essentially monitored by third parties for the infringing potential of their activities. Regimes of panoptic publication have especially deleterious (indeed chilling) effects on creations that rely on fair use for their validity, particularly transformative works.[9] As I will show, piracy surveillance carries the potential to transform the nature of copyright from a liability-based regime into a regime that governs the creation of *all* cultural products in cyberspace, both illegitimate and legitimate. This affects both speaker and audience in three primary ways: first, piracy surveillance enables ISPs to monitor and record the activities of their subscribers, thereby affecting the autonomy, anonymity, and privacy individuals enjoy in cyberspace; second, piracy surveillance overdeters copyright infringement, affecting both the expression and fair use of non-offenders; and third, piracy surveillance affects the audience's ability to access information without interference.

This paper takes the view that this conflict between privacy and piracy is important not just because it showcases a new, overlooked mode of surveillance, but also because it demonstrates the need to resolve conflicts between them in ways that are reflective—and protective—of the relationship between modern technology and personal freedoms. I conclude, therefore, by pointing out the need for greater public oversight over these private realms of surveillance, and suggest a number of ways in which we can envision a more protective sphere for individual autonomy in cyberspace. Towards that end, Part IV argues for greater judicial supervision over the DMCA and offers a potential solution that is derived from the Privacy Protection Act and that balances protections for freedom of speech and privacy with the interests of law enforcement.

---

9 *See, e.g.,* recent discussions concerning fan fiction, Rebecca Tushnet, *Legal Fictions: Copyright, Fan Fiction, and a New Common Law*, 17 LOY. L.A. ENT. L.J. 651 (1997) (arguing for applicability of fair use defense to fan fiction, insofar as it adds value and does not displace the commercial viability of the underlying rights).

I. COMPETING FRAMEWORKS OF PRIVACY AND PROPERTY

As Professor Jonathan Zittrain has pointed out, both intellectual property and privacy have something significant in common: "both are about balancing a creator's desire to control a particular set of data with consumers' desires to access and redistribute that data."[10] This Article is concerned primarily with "informational privacy," the details about our lives that we would most often like to keep free from public view.[11] Although a detailed study of the right to informational privacy—in all of its emanations—is beyond the scope of this Article, it is important to introduce a few major points regarding the conceptions of privacy law itself before progressing to its tensions with intellectual property and speech in the digital age. Informational privacy is rooted in the Fourth Amendment's protection from unreasonable searches and seizures, as well as the conception of privacy outlined by Samuel Warren and Louis Brandeis in their famous 1890 article in the *Harvard Law Review*,[12] where they used the phrase "right to privacy" to denote a constellation of different interests, most of which involved the right not to have personal information exposed to the general public.[13]

---

10 Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1201 (abstract) (2000).

11 This type of privacy is distinguishable in source and in form from "substantive privacy," which generally can be thought of as a freedom from state interference into matters of marriage, procreation, and child-rearing . Substantive privacy is thought to be a "right held against the state's power to legislate." *See* Adam Hickey, *Between Two Spheres: Comparing State and Federal Approaches to the Right to Privacy and Prohibitions Against Sodomy*, 111 YALE L. J. 993, 994 n.8 (2002); and Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 749 (1989). At the same time, however, much of the justification for substantive privacy overlaps with the ones often used to justify informational privacy. *Id.*, citing *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and his intellect. . . .They sought to protect Americans in their beliefs, their emotions, and their sensations. They conferred, as against the Government, the right to be left alone—the most comprehensive of rights and the right most valued by civilized men.").

12 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

13 *See* Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291

Today, over 100 years after Warren and Brandeis' critical formulation, informational privacy entitlements derive their force from a panoply of federal, state, and regulatory guidelines,[14] many of which emerged from the Code of Fair Information Practices over twenty years ago.[15] Despite the lingering confusion about the definition of informational privacy itself, these guidelines, along with other decisions, have created a set of norms of entitlements and expectations of informational privacy. Perhaps as a result of this patchwork of protections, informational privacy has been besought with complications regarding its scope.[16] These complications—both definitional and functional—have only been exacerbated as technology has grown more complex, revealing the law's utter inability to keep

---

(1983).

14 *See*, *e.g.*, The Privacy Act of 1974, (codified as amended at 5 U.S.C. § 552a (2004)); *see also* the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 (2004) (encompassing the Wiretap act and the Stored Communications Act); The Freedom of Information Act of 1966, 5 U.S.C. § 522; The Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §1232(g); The Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-02; The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2002); The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub. L. No. 104-191 (1996). In the state context see ROBERT E. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1992).

15 *See* Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens,* July 1973, *at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm. The Code is considered to be the governing principles of modern, informational privacy, and include the following directives: (1) Personal data record-keeping practices should not be kept secret; (2) An individual should have the ability to find out what information about him or her is on record and how it is disclosed, and should have the ability to correct it; (3) An individual should have the ability to correct or amend a record of identifiable information about him or her; (4) An individual should have the ability to limit the disclosure of information about her or him that was obtained for one purpose from being disclosed for other unrelated purposes; and (5) An organization creating, maintaining, using, or disseminating records of identifiable personal data must guarantee the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

16 Others contend that the concept of informational privacy involves a much broader formulation. For example, Robert Ellis Smith, editor of the Privacy Journal, has defined privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves." Electronic Privacy Information Center, *Privacy & Human Rights 2002*, at 2, citing ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE 6 (2000).

pace with technology to ensure the protection of privacy, property, and identity, particularly in cyberspace.

As the first section will argue, in real space, property rights coupled with architecture serve as a defensive shield to protect privacy. In contrast, as the second section will argue, the nature of cyberspace decouples the relationship between property and privacy, creating a host of challenges for the protection of privacy. Unlike real space, which is characterized by reified boundaries between private and public space, boundaries in digital space are largely permeable and transparent, engendering a nearly limitless potential for consumer surveillance.

A. A SYMBIOTIC VIEW FROM REAL SPACE

While property and privacy protect different interests, they enjoy a mutually reinforcing relationship that has been historically validated by the law—and architecture—governing real space. Historically, some scholars argue that at least one source of the right to privacy actually originated through property rights themselves.[17] In his treatise *Of Property*, written in the last decade of the seventeenth century, John Locke observed that, "every Man has a Property in his own Person. This no Body has any right to but himself."[18] Lockean notions of property in one's person are inextricably linked to the protection of privacy. Because they presuppose the ability to exclude others from bodily invasion, they suggest that protection of bodily privacy also involves a metaphor of ownership.[19]

Adding to this, Locke also powerfully recognized that property rights should extend to the products of one's labor;

---

17 Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BER. L. TECH. J. 1, 26 (1996).

18 *Id.* at 14, quoting JOHN LOCKE, TWO TREATISES ON GOVERNMENT 328-29 (Peter Laslett, ed. 1965). For a substantive due process analysis of Locke's work, *see* Jeffrey S. Koehlinger, *Substantive Due Process Analysis and the Lockean Liberal Tradition: Rethinking the Modern Privacy Cases*, 65 IND. L. J. 723 (1990) (observing that Locke's emphasis on the interests of society are "key pillars in the Lockean framework against which modern assertions of fundamental privacy rights under the Constitution must be judged").

19 *See* Radhika Rao, *Property, Privacy, and the Human Body*, 80 B.U. L. REV. 359, 422 (2000).

"that which he mixes his labor becomes 'his property.'" As Professor Wendy Gordon has explained, this linkage between labor and personality is a key principle justifying much of contemporary and historical property law.[20] The basic structure of Locke's reasoning is that labor belongs to a particular person and that when a person uses her labor to appropriate objects from the public commons, she attaches an ownership right to the objects in question.[21] Because of the intermingling of her labor with these objects, she may be said to have obtained a "property right" in the objects themselves.[22] In turn, others have a duty to restrain themselves from gathering the fruits of her labor and to leave these objects alone.[23]

Therefore, the notion of a property right, as Gordon explains, means two different things: a vested entitlement, or a complex collection of rights associated with the nature of ownership.[24] These rights usually mean that a property owner

---

20 *See* Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533, 1608 (1993). *See also* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002-03 (1984) (citing Locke in holding that intangible products of one's "labour and invention" can be considered "property" subject to the Takings clause); Peter Halewood, *Law's Bodies: Disembodiment and the Structure of Liberal Property Rights*, 81 IOWA L. REV. 1331, 1350-51 (1996) ("The core of Locke's argument is that one has a property right in one's person, thus in one's labor, and by extension, in the objects of one's labor.").

21 Gordon, *supra* note 20, at 1544-45.

22 *Id.*

23 *Id.* Indeed, according to Jeremy Waldron, Locke used the term 'property' in a broad sense to cover a wider range of possible rights, which encompassed a much wider swath than property rights alone—for example, Locke included personal rights of life, liberty, and security, as well as other rights in relation to the use of resources. This observation suggests that Locke may have even viewed personal information—whether the product of historical record or fanciful creation—to be one's personal property, because he viewed it as an extension of one's personality. JEREMY WALDRON, THE RIGHT TO PRIVATE PROPERTY 158 (1988). Locke's observations about property—as the fruit of labor and as an extension of self—greatly affected early philosophical justifications for intellectual property rights. Intellectual property law developed around the conception of the "'romantic author,'" the author that "mixes her unique personality with ideas," and who displays novelty and creativity in her expressions. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1112 (2002) (quoting JAMES BOYLE, SHAMANS, SOFTWARE AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INTERNET SOCIETY 54 (1996)). This central facet of intellectual property, according to Dan Solove, "embodies Locke's idea that one gains a property right in something when it emanates from one's self." *Id.*

24 Gordon, *supra* note 20, at 1547.

has the power to consume the property and use it harmlessly, to transfer the property, and to exclude anyone from entering, infringing, or interfering with her use and enjoyment of the property.[25] In this manner, property rights confer a certain amount of sovereignty and separation in the property owned. In turn, the right of ownership directly translates into the right to be left alone, or, put a different way, the right to exclude others from the object owned.

Just as the term private property suggests, the two enjoy a symbiotic relationship stemming from Blackstonian ideals of "sole and despotic dominion."[26] For, just as every person enjoys a property right in her person, she enjoys the right to exclude others from treading or trespassing on her privately owned property.[27] By creating a boundary between private and public ownership, the law permits an owner, by virtue of the right of exclusion, to confer a certain level of privacy on those objects. Consider, for example, the significance of the home in constructing a boundary between private and public space. The core of the private sphere lies in the home, deemed by the Court as "the most private of places,"[28] a world where an individual may safely retreat from others' gaze and scrutiny. The private sphere, according to Edward Shils, involves a sphere where a person "is not bound by the rules that govern public life…The 'private life' is a secluded life, a life separated by the compelling burdens of public authority."[29] Similarly, as Hannah Arendt points out:

> "…[T]he four walls of one's private property offer the only reliable hiding place from the common public world, not only from everything that goes on in it but also from its very publicity, from being seen and being heard. A life spent entirely in public, in the presence of others, becomes, as we would say, shallow. While it retains visibility, it loses the quality of rising into sight from some

---

25 *Id.* at 1550.

26 2 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND at 2 quoted in Julie Cohen, *Does Copyright Trump Privacy?*, 2002 U. ILL. J. LAW, TECH. & POL'Y 375, 383 n.14.

27 *See* WALDRON, *supra* note 23, at 158.

28 Lawrence v. Texas, 539 U.S. 558, 567 (2003).

29 *See* Edward Shils, *Privacy: Its Constructions and Vicissitudes*, 31 L. & CONTEMP. PROBS. 281, 283 (1966).

> darker ground which must remain hidden if it is not to lose its depth in a very real, non-subjective sense. . . ."[30]

Arendt's metaphors of visibility and depth help us to understand the functions of spatial privacy in constructing a deeper, more self-actualized existence for individuals. Ownership of private property constructs, and underpins, notions of privacy and autonomy by ensuring a degree of solitude that is necessary for true human self-actualization.

In this way, property and privacy are each grounded in territorial metaphors which construct boundaries that define realms of physical or social immunity from state interference.[31] Property rights confer a certain amount of spatial sovereignty in the property owned,[32] a factor which directly complements the right to be left alone. This is why the Supreme Court, at various points, has emphasized that "one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude."[33] As Professor Charles Reich has echoed:

> "Property draws a circle around the activities of each private individual or organization. Within that circle, the owner has a greater degree of freedom than without. Outside, he must justify or explain his actions, and show his authority. Within, he is master, and the state must explain and justify any interference. Thus, property . . . creates zones within which the majority has to yield to the owner."[34]

Citing this passage, Professor Radhika Rao has asserted that precisely the same observation could be made regarding the right of privacy.[35] She observes that the right to property, like

---

30 HANNAH ARENDT, THE HUMAN CONDITION (1958), quoted in DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 26 (2003).

31 *See* Rao, *supra* note 19, at 425. Scholars also cite this passage for the concept of defining the body as property. *See, e.g.*, RUSSELL SCOTT, THE BODY AS PROPERTY (1981).

32 *Id.*

33 Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

34 Charles A. Reich, *The New Property*, 73 YALE L.J. 733, 771 (1964).

35 Rao, *supra* note 19, at 423.

privacy, decentralizes decision-making power by placing it into the hands of owners, thereby policing "the fragile boundary between individual autonomy and government authority."[36]

This brief discussion illustrates that privacy and property are inextricably entwined with one another, even if they take on different degrees of relative importance depending on the property in question. The law, too, has embraced this view, noting that both entitlements are equally necessary in the law: one cannot exist without the other.[37] In real space, for example, property law, architecture, and the strong protections afforded by the Fourth Amendment are able to strike an important balance between privacy and property, as reflected in the substantial jurisprudence stemming from the Fourth Amendment that required some evidence of a trespassory invasion. This tendency also reflected the traditional, oft-repeated presumption that "a man's house is his castle,"[38] which formed a critical cornerstone in the development of the unreasonable search and seizure jurisprudence.[39] In the early eighteenth century, for example, the protection of property rights served as a reasonable proxy for privacy interests: Proof of trespass on one's private property, for example, was necessary to establish the search and seizure liability of government agents.[40] Early Fourth Amendment jurisprudence further

---

36 *Id.*

37 *See* Rakas v. Illinois, 439 U.S. 128 at 159-160, observing, "Though the Amendment protects one's liberty and property interests against unreasonable searches of self and effects, 'the primary object of the Fourth Amendment […] the protection of privacy.'" (quoting Cardwell v. Lewis, 417 U.S. 583, 589 (1974))

38 Miller v. United States, 357 U.S. 301, 307 (1958).

39 Part of this conception was attributable to the presence of limited technologies of surveillance. *See* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 871 (1996).

40 One English case cited often by the Supreme Court, *Entick v. Carrington*, 19 HOW. ST. TR. 1029 (C.P. 1765), involved the search of a person's home and papers. The plaintiff had been suspected of authoring several seditious publications, and the government searched and seized his private papers (some unrelated to the charges at issue). The plaintiff sued under a trespass theory, and the court agreed with him, observing that property rights played a fundamental and determinative role in modern society. The court concluded that "every invasion of private property, be it ever so minute," could be considered to be a trespass. *Id.* at 1066. Lord Camden stated:

> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that

emphasized property-based conceptions of privacy, producing an indelibly trespass-based construction of this right.[41] More recently, however, the Supreme Court has relaxed this requirement, and embraced a much more protective version of the Fourth Amendment within the home and other 'private' places.[42]

Nevertheless, while our loyalty to property remains stated—and has even expanded—through the law, our commitment to privacy in American law is far less apparent when we move outside of the boundaries of real property.[43] Without a brick-and-mortar architecture, the very concept of privacy law is replete with both theoretical and practical conflicts—between agencies, statutes, and popular expectation.[44] For example, there is no specific constitutional right to privacy, informational or otherwise.[45] Cases like *Griswold* and *Roe*

> they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. *Id.*

The court also stated that because the government had no right to seize one's private papers, such acts would be considered tantamount to a government taking. *Id.* at 1044. Commenting on this section in Entick, William C. Heffernan has observed that property rhetoric served as the primary category of analysis for the inviolability of a person's privacy. Even though the doctrine of privacy was not well-developed at this point, Lord Camden's treatment of trespass, according to Heffernan, "evinced a profound respect for informational privacy," further demonstrating that property rights served as an adequate, though awkward, proxy for privacy interests where government searches were concerned. William C. Heffernan, Fourth Amendment Privacy Interests, 92 J. CRIM. L. & CRIMINOLOGY 1, 13-14 (2002).

41 *See* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 308 (1998). For a very interesting discussion of the relationship between privacy, property and the Fourth Amendment, see Orin Kerr, *The Fourth Amendment and New Technologies*, 102 MICH L. REV. 801 (2004); Sherry Colb, A World Without Privacy, 102 MICH. L. REV. 889 (2004); Peter P. Swire, *Katz is Dead, Long Live Katz*, 102 MICH. L. REV. 904 (2004).

42 *See generally* Kyllo v. United States, 533 U.S. 27 (2001)

43 PAUL SCHWARTZ & JOEL REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996); *see also* Joel Reidenberg, Setting Standards for Fair Information Practices in the U.S. Private Sector, 80 Iowa L. Rev. 497, 545-48 (1995); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH, L. REV. 119 (2004).

44 *See* Robert Post, *Three Concepts of Privacy*, 89 GEORGETOWN L. J. 2087 (2001).

45 For example, the Supreme Court has developed a limited,

postulated a substantive type of privacy that is thought to be a "right held against the state's power to legislate,"[46] thereby honoring strands of personhood in protecting the deliberative choices of individuals in areas like marriage, conception, and child-rearing. But the Supreme Court has traditionally been quite reluctant to extend the same rationale to the protection of informational privacy, drawing a firm line between informational and substantive privacy.[47]

Consider the 1977 case of *Whalen v. Roe*, where the Supreme Court dealt with a New York law that required the government to collect and store the names and addresses of patients whose doctors prescribed drugs that could potentially be abused. The question was whether this storage and dissemination in government databases implicated a constitutional right to privacy.[48] In an insightful opinion, Justice Stevens deftly characterized the growing case law concerning privacy into two different kinds of interests, one informational and one substantive. The first, he points out, involves the individual interest in avoiding disclosure of certain

---

"penumbral" conception of this right flowing from a variety of constitutional sources—the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments, and a host of later decisions that outline (and often complicate) the borders of this right. *See* U.S. CONST. amend. I, III, IV, V, IX, XIV. *See* Planned Parenthood v. Casey, 505 U.S. 833 (1992); Cruzan v. Director, Miss. Dept. of Health, 497 U.S. 261 (1990); Bowers v. Hardwick, 478 U.S. 186 (1986); Whalen v. Roe, 429 U.S. 589 (1977); Moore v. East Cleveland, 431 U.S. 494 (1977); Roe v. Wade, 410 U.S. 113 (1973); Eisenstadt v. Baird, 405 U.S. 438 (1972); Stanley v. Georgia, 394 U.S. 557 (1969); Loving v. Virginia; 388 U.S. 1 (1967); Griswold v. Connecticut, 381 U.S. 479 (1965). In addition, numerous federal and state enactments affect the enforcement of privacy rights in various ways. *See e.g.,* 5 U.S.C. § 552a (2000); CAL. PENAL CODE § 630 (Deering 2003); MASS. ANN. LAWS ch. 214, § 1B (Law. Co-op 2002); N.Y. CIV. RIGHTS LAW § 50 (McKinney 2002); R.I. GEN. LAWS § 9-1-28.1 (2002); WIS. STAT § 895.50 (2002).

46 Adam Hickey, Note, *Between Two Spheres: Comparing State and Federal Approaches to the Right to Privacy and Prohibitions Against Sodomy*, 111 YALE L.J. 993, n.8 (2002); Jed Rubenfeld *The Right to Privacy*, 102 HARV. L. REV. 737, 748-50 (1989).

47 *Whalen*, 429 U.S. at 605.

48 *See* Francis S. Chalpowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 145-50 (1991) (noting that the balancing test outlined in *Whalen* has created a split in interpretations of the right to informational privacy); Lisa Jane McGuire, Comment, *Banking on Biometrics: Your Bank's New High Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV. 441, 460-61 (2000) (calling *Whalen* the "closest the Court came to identifying a right to information privacy").

matters; and the second involves the "interest in independence in making certain kinds of important decisions." Both of these interests were implicated in this case, Stevens observed, because the patients, rightfully so, feared disclosure of the information and its reputational effects just as much as the risk of public disclosure impaired their ability to make decisions independently.

Yet despite the Court's insightful recognition of the various types of interests that illuminated the protection of sensitive information, the Court upheld the program, finding that neither the immediate nor threatened impact of disclosure was sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment's guarantees. Nevertheless, in an interesting observation, the Court noted that, "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." [49] It then observed that the right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures, and "in some circumstances, that duty arguably has its roots in the Constitution," the Court observed.[50] However, since the New York statutory scheme (in its view) evinced a proper respect for an individual's privacy, it declined to consider the effects of an unwarranted disclosure, preferring instead to limit its holding under the Fourteenth Amendment to the facts before it, holding that neither the immediate nor threatened impact of disclosure was sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment's guarantees.[51]

Indeed, *Whalen*'s distinction between informational and substantive privacy heralded the development of two different regimes to protect privacy: one statutory and one constitutional. As the following section will point out, the unanswered question the Court left open in *Whalen*—that is, whether there is a

---

49 *Whalen*, 429 U.S. at 605.

50 *Id at 605; see also* SOLOVE AND ROTENBERG, *supra* note 30, at 189 (2002) (expressing confusion as to whether Whalen suggests a broad constitutional right to information privacy, or a narrow constitutional right that pertains to a personal information involving one's health, family, children and other interests protected by the Court's substantive due process right to privacy decisions).

51 *Whalen*, 429 U.S. at 605.

constitutionally protected right to informational privacy—is the very question that informs the relationship between intellectual property and privacy in the digital age.[52] Instead of definitively providing an answer to this question, the law has opted to expand property rights to third parties, rather than to create a comprehensive scheme to protect individuals from unwanted surveillance.[53] Moreover, the relationship between property and privacy becomes even more complicated by the concomitant rise of piracy in cyberspace, a factor which sets the stage for conflicts between them.

B. A HIERARCHICAL VIEW FROM CYBERSPACE

Property in cyberspace is largely intangible, thus, the architectural conditions that support the "private" nature of ownership in real space—locks, borders, territorial space and seclusion—are widely varying in their power and efficacy. Initially, writing on the future of the Internet, John Perry Barlow triumphantly declared, "legal concepts of property, expression, identity, movement and context do not apply to us. They are based on matter. There is no matter here."[54] As Barlow's powerful rhetoric suggests, the nature of both property and identity have been transformed by their intangible, evanescent character in cyberspace. And yet, at the same time, several scholars have observed the prevailing tendency of individuals to behave as if cyberspace is a "place" like any other.[55] Cyberspace is often characterized in terms of "private"

---

52 After *Whalen*, the Court affirmed a related notion of privacy in *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977), in which the Court concluded that President Richard M. Nixon enjoyed a constitutional privacy interest in private communications with his family, but not in records that involved his official duties. After these cases, however, the notion of a constitutional right to informational privacy has remained distinctly unclear. As a result, some courts have drawn analysis from other types of privacy law. *See* SOLOVE & ROTENBERG, *supra* note 30, 189 (2003) (observing the right to information privacy's resemblance to common law prohibition against unreasonable publicity) (citing Smith v. City of Artesia, 772 P.2d 373, 376 (N.M. Ct. App. 1989)).

53 For a helpful treatment of these issues, see Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000), along with the other articles in the symposium.

54 John Perry Parlow, *A Declaration of the Independence of Cyberspace*, *in* CRYPTOANARCHY, CYBERSTATES, AND PIRATE UTOPIAS 27, 29 (Ludlow ed., 2001).

55 *See* Dan Hunter, C*yberspace as Place and the Tragedy of the*

and "public" spaces: some parts of the Web are public, as are many chatrooms, whereas email is private.[56] The law, too, has embraced this approach: recent case law is replete with examples of territorial metaphor, as well.[57]

Nevertheless, the preexisting balance between property and privacy in real space dramatically changes when one enters the intangible domain of cyberspace. For the intangibility of digital space underlies many of the current debates facing digital intellectual property, and creates the opportunity for tradeoffs between the protection of privacy and property that ordinarily do not exist in real space.[58] Cyberspace changes the symbolic equation of privacy and property: the absence of physical boundaries in cyberspace enables others to regularly invade the privacy of others "with greater ease, efficiency, and power than has been experienced in the physical world." [59]

Since the law confers property rights over profiles of consumer information to collectors, rather than the individual

---

Digital AntiCommons, 91 CAL. L. REV. 439, 453-54 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003). Hunter observes:

> At its most fundamental, think of the term WEB, an allusion to the 'web-like' connections between computers. Then there is the NET, referring to the network of connections as well as the net-like character of the material caught in the network. We SURF this WEB, MOVING from one site to the next, ENTERING or VISITING the site, or, in the slightly old-fashioned nomenclature, we access someone's HOMEPAGE. We HANG OUT IN CHATROOMS communicating with our ONLINE buddies. We ROAM AROUND Multiple User DUNGEONS and DOMAINS ("MUDs") and MUDs Object Oriented ("MOOs"). Software programs called ROBOTS, AGENTS, or SPIDERS are allowed to CRAWL over websites unless they are barred by terms and conditions of ENTRY or ACCESS, or by the robot EXCLUSION standard. We NAVIGATE the WEB using computer programs with names like NAVIGATOR and EXPLORER.. . .We log INTO or log ONTO our Internet Service Provider ("ISP"). Malignant wrongdoers ACCESS our accounts by hacking INTO the system using BACKDOORS, TRAPDOORS, or stolen KEYS, and engage in computer TRESPASSES.

56 Hunter, *supra* note 55, at 456.

57 *Id.* at 480-493.

58 *See* Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135 (2004).

59 Natalie L. Regoli, *A Tort for Prying Eyes*, 2001 J.L. TECH. & POL'Y 267, 269 (2001).

subject herself, it creates substantial incentives for surreptitious monitoring of consumer activity.[60] And this, in turn, alters the fragile balance of privacy and property by permitting accumulation of data that is often enabled by careless consumers who unwittingly consent to such collections, but who continue to retain expectations of informational privacy. This transition towards third-party ownership, in turn, has radically altered the preexisting balance between privacy and property contemplated in real space by subordinating the protection of informational privacy to the accumulation of database property.[61]

Some of these changes are attributable to an innate transformation in the value of information itself. Although information has always served as a resource, it was always "relegated to the position of supporting other resources."[62] Today, however, since the advent of digital technology, information has become a valuable commodity in and of itself, leading to a shift towards its commercialization. As a result, the economic base of society has shifted from industry to information, giving rise to such labels as the "Information Revolution" or the "Information Society."[63] Vast amounts of personal information are now primed for harvest, distribution, and disclosure to third parties on the Internet, often without the individual's knowledge.[64] Use of this information allows companies to perfect the creation of a "virtual persona," or "electronic persona"[65] that comprises a profile of an individual user's tastes, purchasing habits, Web sites visited, and other identifying information. And, in perhaps the most ironic result of the informational privacy debate, intellectual property rights in such information are granted to the gatherer of the information, instead of to the subject herself.[66] As a result,

---

60 *See, e.g.,* Shibley v. Time, 341 N.E. 2d 337 (1975); *In re* DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d 497 (S.D.N.Y. 2001).

61 *See* J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51 (1997); Jacqueline Lipton, Information Wants to Be Property, 16 Int'l Rev. L. Computers & Tech 53 (2002).

62 Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 12 (1996).

63 *Id.* at 18.

64 *Id.* at 3.

65 *Id.*

66 *Id.*

property and privacy have developed a hierarchical relationship to one another, a factor which enables tradeoffs between them.

1. PLACE AND PANOPTICISM

Our persistent tendency towards territorial metaphor is certainly understandable; after all, both property and privacy are inextricably linked to concepts of spatiality and exclusion. Yet these tendencies pose troubling questions when we apply them to cyberspace, because they often assume that the architecture of cyberspace, like real space, adequately balances protections for both privacy and property. Unlike real space, where architecture and simple geography precluded neighbors and the government from peering in on each other's activities, today, the architecture of the Internet (quite unlike its brick and mortar counterpart) *facilitates*, rather than prevents, informational invasions.[67]

To begin with, the changing architecture of cyberspace plays a vital and active role in facilitating consumer surveillance—architectural elements like borders and fences have extremely different capabilities when they are protecting information, rather than tangible goods.[68] For example, most content on the Internet—music, text, video, and other fixed media—tends to be "served" from a central system that responds to requests from a user. The user, or "client" requests information, or content, from a server; the server then transmits the information to the user.[69] In this model, visitors to a Web site do not interact with each other.[70] Information simply passes from one entity to another, and the recipients of the information do not connect.[71] Consumers connect to the Web

---

67 *See* Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-64 (1999); Natalie L. Regoli, *A Tort for Prying Eyes*, 2001 U. ILL. J.L. TECH. & POL'Y 267, 269 (2001) (the absence of physical boundaries enables others to regularly invade the privacy—and property—of others "with greater ease, efficiency and power than has been experienced in the physical world.").

68 Wendy J. Gordon, *An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory*, 41 STAN. L. REV. 1343, 1378-84 (1989).

69 William W. Fisher III & Christopher Yang, *Peer-to-Peer Copying*, at Introduction, *at* http://cyber.law.harvard.edu/ilaw/P2P.html (Nov. 18, 2001).

70 *Id.*

71 *Id.*

sites from intermittently connected personal computers ("PCs"), which are usually at the edges of a network.[72]

This form of client-server Web architecture, predicated on hierarchical principles, has yielded extremely successful Internet Service Providers ("ISPs"), which provide information to clients from servers always connected to the Internet.[73] Over time, a few of these privileged servers, serving millions of clients, have increasingly dominated the Internet.[74] This model works for almost all content, from streaming videos to interactive games to online shopping.[75] As a result, ISPs have developed into a private form of governance in cyberspace because they maintain a substantial amount of consumer information regarding users' online activities, and because they often control the transmission and distribution of requested information.[76] For these reasons, many consider the ISP the principal repository for all identifying information regarding individual users and their Web activities.

In contrast, a peer-to-peer framework essentially erases the hierarchical division between client and server, thus turning the idea of a network of Internet governance on its head.[77] A peer-to-peer model creates a mode of communication that treats each machine as a separate and equal entity in the sharing of

---

72 Clay Shirky, *Listening to Napster*, *in* PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 21, 35 (Andy Oram ed., 2001) [hereinafter PEER-TO-PEER].

73 ISPs can further be broken down into two separate groups: Online Service Providers—such as America Online, Prodigy and Compuserve, who provide both Internet access as well as a system for posting and exchanging content—and Internet Access Providers, who simply provide direct access to the Internet.

74 Nelson Minar & Marc Hedlund, *A Network of Peers*, *in* PEER-TO-PEER, *supra* note 72, at 3-9.

75 *Id.* at 9.

76 *See* SOFTWARE & INFO. INDUS. ASS'N, STRETCHING THE FABRIC OF THE NET: EXAMINING THE PRESENT AND POTENTIAL OF PEER-TO-PEER TECHNOLOGIES 3 (2001) [hereinafter SIIA].

77 *See* Minar & Hedlund, *supra* note 74, at 3. There are three main categories of peer-to-peer systems: centrally coordinated, hierarchical, and decentralized. *Id.* at 4-8. In a *centrally coordinated* system, a central server, like Napster, mediates coordination between peers. *Id.* A *hierarchical* peer-to-peer system organizes peers into different levels, and a local coordinator mediates communication among peers in the same group. *Id.* at 7-8. In a *decentralized* system (a true peer-to-peer framework), the program provides users with a virtual underground railroad to exchange and share files, and to evade direct, centralized control. *Id.* at 5-7.

information.[78] This model enables individual computers to interact with one another by making it possible for one computer to "ask" other computers directly for a specified type of file.[79] Each computer then forwards the request to a second tier of computers, which in turn forwards the request to a third tier, and so on.[80] When the requested file is located, it is automatically transmitted to the original user.[81] In this manner, peer-to-peer fragments transform each node on the network into *both* client and server, allowing a file transfer (or download) to be performed by a direct connection between both users, instead of through a single channel.[82]

Although peer-to-peer frameworks seem deceptively simple, their implications, both legally and socially, are extraordinarily complex. They signal, for some, the end to the power of censorship, copyright, and other types of legal governance. Because these networks are extremely difficult to control, it is possible for individuals to store and exchange information freely without government intervention, even if the information has been censored in some manner.[83] True peer-to-peer networks are also extremely difficult to shut down because the nature of the technology makes it nearly impossible to track the movement of information.[84]

Peer-to-peer networks, however, also potentially transform the boundaries between public and private. Since property in cyberspace is almost always wholly intangible in nature, the material conditions that support the "private"

---

78 *Id.* at 4.

79 Fisher & Yang, *supra* note 69, at Introduction. These peer-to-peer "nodes" operate outside of the traditional registry of domain names and with significant autonomy from central servers. Shirky, *supra* note 72 at 22.

80 Fisher & Yang, *supra* note 69, at Introduction.

81 *Id.*

82 Kathy Bowrey & Matthew Rimmer, *Rip, Mix, Burn: The Politics of Peer to Peer and Copyright Law*, 7 FIRST MONDAY 8, (Aug. 2002), *at* http://www.firstmonday.dk/issues/issue7_8/bowrey/index.html; *see also* Gene Kan, *Gnutella*, *in* PEER-TO-PEER, *supra* note 72, at 94, 94-95 (describing how Gnutella, which uses a decentralized framework, transfers files from one user to another); Minar & Hedlund, *supra* note 74, at 17 (describing how Napster operates).

83 Damien A. Riehl, *Peer-to-Peer Distribution Systems: Will Napster, Gnutella and Freenet Create a Copyright Nirvana or Gehanna?*, 27 WM. MITCHELL L. REV. 1761, 1763-66 (2001); *see also* PEER TO PEER, *supra* note 72, at 35.

84 Fisher & Yang, *supra* note 69, at Introduction.

nature of ownership in real space—locks, borders, territorial space, and seclusion—vary widely in their power and efficacy.[85] Actual seclusion is effectively impossible, since everything is linked through networks, software, and hardware. As a result, privacy and security in cyberspace depend most often on consumer sophistication and technical knowledge, rather than a simple preference for seclusion.

Consider the implications of a program called "Desk Swap." Desk Swap is a program that makes a person's online desktop visible to others across the Internet. When the software begins, it takes a photograph of whatever is on a person's desktop and sends it to the developer's computer, where it then joins a host of other images that are then made visible to others. Given the extent to which individuals often place personal information on their desktops, the possibility of unintended exposure is enormous. Yet the point of the program is not to reveal others' personal information; there is another objective. The programmer's purpose is to enable its users "to feel anew this sense of panic about the loss of privacy and control in the digital age, which may inspire them to be more cautious about protecting their digital selves."[86] Likewise, since peer-to-peer systems reconfigure the boundaries of private and public space, they necessarily raise concerns about security, as well as trust between peers. As one study notes on peer-to-peer systems:

---

85 *See* Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217. For excellent background reading on this topic, see HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER (1993); David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Timothy Wu, *When Law and the Internet First Met*, 3 GREEN BAG 2D 171 (2000).

86 *See* Matthew Mirapaul, *A Reality Show for Your Desktop, But There's a Catch*, N.Y. TIMES, Sept. 18, 2001, at E2.

> "How secure can one feel in a decentralized network? Is it possible for someone to look at what's on your hard drive when you log into a peer-to-peer network? The answers to these questions lie in which peer-to-peer environment one joins. Some have built in firewall-like mechanisms to warn of hackers trying to access your computers, while others leave your computer wide open. . . .
>
> Most consumer applications request that you leave your PC on and accessible all the time. In such 'open' systems, you are permanently leaving a back door open to your PC with all of the attendant issues of privacy, virus attacks and other security concerns."[87]

Although it is technically possible to employ some measures, such as firewalls, to protect one's computer from unwanted invasion, they are usually considered to be counterproductive to a file-sharing environment.[88] Moreover, one study found that a majority of peer-to-peer users of Kazaa (a popular peer-to-peer service) "were unable to tell what files they were sharing, and sometimes incorrectly assumed they were not sharing any files when in fact they were sharing *all* files on their hard drive."[89] Such lack of knowledge raises the risk that other peers are capable of accessing extremely personal information stored on one's hard drive, particularly one's credit card, email correspondence, and financial or social security information.[90]

Indeed, from both an architectural as well as a philosophical perspective, cyberspace networks, particularly of the peer-to-peer variety, bear much similarity to the Panopticon. The Panopticon refers to the design of a prison that facilitates constant surveillance by placing guards in a central tower, thereby creating a sense of "conscious and permanent visibility that assures the automatic functioning of power."[91] The

---

87 SIIA, *supra* note 76, at 12.

88 *Id.*

89 Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of P2P File-Sharing*, at 1, *available at* http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf (last visited Dec. 05, 2004).

90 *Id.*

91 OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 9 (1993).

panoptic design, first mentioned by Jeremy Bentham and then further developed by the French philosopher Michel Foucault, applied to many different types of disciplinary surveillance, including rehabilitation and education.[92] Foucault's commentary is consciously tied to Bentham's own description, which consists of a central tower, bordered by windows that are made capable of gazing into various cells; each of those cells is also made capable of looking into each others' spaces.[93] Each cell, therefore, creates an illusion of solitariness, but ensures that the person senses that he or she is being watched at the same time.[94]

The primary effect of this combination of space and enclosure is for individuals to internalize the overseeing gaze of authority figures, and eventually to discipline their behavior to comport with expectations of these figures, irrespective of whether or not they were actually present and watching at the time. By creating the illusion of constant surveillance, individuals begin to internalize the feeling of being observed. "[I]t is at once too much and too little," Foucault wrote, "that the prisoner should be constantly observed by an inspector." Rather, "the inmate must never know whether he is being looked at any one moment; but he must be sure that he may always be so."[95]

Any individual can operate the Panopticon, and no motive is required; anyone was eligible, wrote Foucault, including "the curiosity of the indiscreet, the malice of a child, the thirst for knowledge of a philosopher who wishes to visit this museum of human nature, or the perversity of those who take pleasure in spying or punishing."[96] Indeed, the more anonymous and temporary observation can be, the greater the anxiety of the person who is being watched.[97] As Professor Daniel Solove notes, "by constantly living under the reality that one could be observed at any time, people assimilate the effects of surveillance into themselves. They obey not because they are

---

92 MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200 (Alan Sheridan trans., 1977); *see also* JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovic ed., 1995).

93 FOUCAULT, *supra* note 92, at 200.

94 *Id.*

95 *Id.*

96 *Id.* at 202.

97 *Id.*

monitored but because of their fear that they could be watched. This fear alone is sufficient to achieve control."[98] Surveillance is prophylactic: it prevents legal transgressions by transforming an external gaze into an internal one.[99]

While the panoptic metaphor has been crucial to understanding disciplinary processes in real space, I would argue that it is especially useful when applied to the effects of surveillance on the Web. In a peer-to-peer environment, the traditional distinction between private and public space readily collapses, leaving open a minefield of possibilities for invasion and observance. The identities and activities we adopt in cyberspace can become transparently visible, compromising privacy and identity. Many of our activities in cyberspace—communications, files, stored pictures, online activities—can be monitored, revealed, and recorded at the same time. As a result, the file sharing revolution renders certain files stored on individual computers potentially accessible,[100] from the most personal to the most public information, enabling "invasion without physical invasion."[101] Moreover, in a peer-to-peer system, there is no hierarchy: every computer has the same authority to access data as every other computer, whether owned by a state or private entity. In a world where individuals store more and more personal information on computers, peer-to-peer searches can become especially intrusive, particularly since many individuals may not realize what they are sharing online.[102] Consequently, the possibilities for information gathering are enormous, irrespective of who authorizes or initiates the investigation.[103]

---

98 Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1415 (2001).

99 Martin Jay, *In the Empire of the Gaze: Foucault and the Denigration of Vision in Twentieth-century French Thought*, *in* FOUCAULT: A CRITICAL READER 192 (David Couzens Hoy ed., 1986).

100 Indeed, while some peer-to-peer programs allow a person to segregate shared files from private ones, the dependability of these barriers varies according to the program. SIIA, *supra* note 76, at 12 (discussing the characteristics of various file sharing technologies).

101 Lessig, *supra* note 67, at 59.

102 Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1096 (1996).

103 Aside from Kazaa's widely publicized use of spyware, one recent study reports that forty-five percent of the executable files traded on Kazaa, one of the most popular file sharing services, contain malicious code-

2. THE DIGITAL PERSONA AS PROPERTY

As I have argued, the permeable boundaries between private and public space clearly alter the relationship between intellectual property and informational privacy. Here, Arendt's distinction between the private sphere—as invisible, hidden, and full of depth—and the comparatively more shallow public sphere, offers us little solace. Many individuals attach privacy expectations to their activities, identities, and expressions in public space, particularly where the sharing of information is concerned, even if the law fails to validate them.

Here, intellectual property principles play an inherently contradictory role: on one hand, they serve as a theoretical foundation for viewing the collection of consumer information as property that can (and should) be treated like any other commodity; on the other hand, the very same principles also theoretically justify granting consumers greater control over their personal information.[104] This tension between intellectual property as a protective foundation for consumers, on one hand—and data harvesters, on the other—creates an added, and underlying, conflict regarding the propertization of personal information. On one hand, as Rochelle Dreyfuss has pointed out, intellectual property protections exist so that companies can assert private control over personal information used publicly, such as the copyright protection afforded to databases.[105] Yet, today, intellectual property is now being considered as a framework for individuals to assert rights over private activities conducted publicly—such as surfing the net, purchasing by computer, or through appearances in public places surveilled by

---

like viruses and Trojan horses. Some code was designed to infect other files marked for sharing; others installed programs that enabled the sending of spam through the computer; and still others stole personal information and passwords saved on the computer. *See* Kim Zetter, *Kazaa Delivers More Than Tunes*, WIRED NEWS, Jan. 9, 2004, *at* http://www.wired.com/news/business/0,1367,61852,00.html/wn_ascii.

104 *See* Samuelson, *supra* note 53; *see also* Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2003); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO L. J. 2381 (1996); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies* 54 HASTINGS L. J. 877 (2003).

105 See Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection In Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8 (1999), *at* http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_8/.

video cameras.[106] As Dreyfuss points out, these activities take place in public or semipublic spaces, even though privacy advocates continue to analyze these activities under the rubric of privacy principles.[107]

The nature of cyberspace also ushers in a contradictory complication: we act as though we have perfect anonymity in cyberspace, when in fact, much of the information we produce is not only owned by others, but also subject to a great degree of surveillance. Despite clear risks of panopticism, as Daniel Solove has observed, the Internet "gives many individuals a false sense of privacy. The secrecy and anonymity of the Internet is often a mirage."[108] Put another way, the Internet offers an almost limitless possibility of identities, expressions, and activities; on the other, it promises a vast array of monitoring mechanisms to ensure that the work of record-keeping quietly continues.

The more strongly people perceive their informational privacy and anonymity, the more likely they are to feel free to fully create and express different identities and views in cyberspace. Perceptions of anonymity in cyberspace have enabled a level of participation in public discourse unlike anything before, allowing individuals with limited financial resources to "publish" information and opinions on matters of public concern.[109] As Professor Sherry Turkle has written, "[w]hen we step through the screen into virtual communities, we reconstruct our identities on the other side of the looking glass."[110] Even outside of structured forums, a user can adopt a multiplicity of gender, sexual, racial, or other categorical identities, invent accompanying personal histories, and engage in an assortment of acts that she would probably not perform in real life.[111] In other words, virtual space allows individuals to construct identities they choose for themselves, rather than the

---

106 *Id.*

107 *Id.*

108 Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1092 (2002).

109 *See* Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 861 (2000).

110 Turkle argues that the Internet has enabled us to think about identity in terms of multiple selves, rather than in terms of a singular, unitary self. SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET 177 (1995).

111 *Id.* at 212.

ones they are born with.[112] This ability to adopt transitory and multiple identities is at the heart of cyberspace's limitless possibility.[113]

Obviously, the creation of such identities draws heavily on perceptions of informational privacy. Initially, informational privacy evolved under the notion that personal papers "fully and transparently identified the people whose lives they represented."[114] Yet today, the perception of informational privacy extends, at least in cyberspace, to something quite different: it covers the very act of creating personalities and accessing information, in addition to the possibility of anonymously publishing information. Suppose person Y chooses to open an email account under an assumed name, and with that identity to surf the Web, make purchases, sign on to listservs, and engage in online conversation. Her online identity, conversations, and activities are all "public" in the sense that they can be subject to varying degrees of transparency in cyberspace. However, her true identity, or her personal information—preferences, shopping habits, web searches—are all "private" in the sense that she might prefer them to be secluded from public knowledge. Her perception of anonymity permeates her expressions and activities in cyberspace, in countless ways—from the words she chooses and the identities she uses, to her choices in accessing information.[115]

In a related observation, Julie Cohen has argued for the protection of "intellectual privacy," a principle that embraces the privacy-related aspects of consumer acquisition and use of materials as well as protection from disclosure.[116] Central to this principle are three underlying themes: autonomy,

---

112 *Id.* at 226, 240.

113 LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 33 (1999) (Whereas real space requires that you reveal "your sex, your age, how you look, what language you speak, whether you can see, whether you can hear, [and] how intelligent you are," cyberspace requires only that you reveal your computer address.).

114 Philip E. Agre, *The Architecture of Identity*, INFORMATION, COMMUNICATION & SOCIETY, at 1, 3 (1999).

115 *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395 (1996).

116 Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 580 (2003).

informational privacy, and spatial privacy.[117] Intellectual privacy, in Cohen's formulation, applies to protect the consumption of intellectual property products within presumptively private spaces, as well as the nexus between intellectual exploration and private physical space.[118] As Cohen points out:

> Just as spatial privacy allows for physical nudity, so it also allows for metaphorical nudity; behind closed doors, one may shed the situational personae that one adopts with co-workers, neighbors, fellow commuters, or social acquaintances, and become at once more transparent and more complex than any of those personae allows. Spatial privacy affords the freedom to explore areas of intellectual interest that one might not feel as free to explore in public. It also affords the freedom to dictate the circumstances – the when, where, how, and how often – of one's own intellectual consumption, unobserved and unobstructed by others.[119]

In response to these interests, privacy advocates, along with the Federal Trade Commission (FTC), have espoused concrete norms to protect personal data.[120] As a result, interactions between commercial Web sites and their visitors are framed in terms of visible, declaratory assurances of informational privacy.[121] Many individuals have felt a growing sense of entitlement to their informational privacy, despite the technology that exists for massive information-gathering on the Internet.[122] Moreover, in addition to the FTC regulations,

---

117 *Id.*

118 *Id.* at 576.

119 *Id.* at 579.

120 Steven A. Hetcher, *Commentaries on Eric Posner's Law and Social Norms: Cyberian Signals,* 36 U. RICH. L. REV. 327, at 337-38 (2002), citing 15 U.S.C. §§ 45(a)(1), 41-58 (observing that the Federal Trade Commission has spearheaded a number of efforts to protect consumer privacy on the Web pursuant to its authority under the Federal Trade Commission Act, which mandates that the agency respond to "unfair" and "deceptive" trade practices). For a discussion of the FTC's role in protecting privacy, *see* Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV 1609 (1999); Jeff Sovern, 69 FORDHAM L. REV. 1305 (2001).

121 Hetcher, *supra* note 120, at 331.

122 For example, some Web sites are capable of collecting "clickstream data," which tracks a user's computer as it navigates through the Web, monitoring the time, order and duration the computer spent on each

Congress has enacted The Electronic Communications Privacy Act of 1986, which restricts the interception of oral, wire, and electronic communications while in transit; and the Computer Fraud and Abuse Act, as well as other provisions.[123]

Yet, despite the laudable principles behind the entitlement to informational privacy, the reality of protection is quite different. Instead of ensuring consumer protection, the technological means for consumer monitoring have grown even more advanced—and more subtle—with the passage of time.[124] Today, techniques of data collection are especially pernicious because they are subtle, ongoing, largely unregulated, and inextricably linked to a person's online activities.[125] Various entities collect an enormous amount of personal information from users with scant attention to the moral and legal privacy implications raised by its collection.[126] Web sites use "tracking software" that logs information about users, which is then used

---

Web page as well as any files downloaded or accessed.

123 *See, e.g.*, the Privacy Protection Act of 1980, the Computer Matching and Privacy Protection Act of 1988 (regulating government record-keeping); and the Fair Credit Reporting Act (protecting the disclosure of credit information).

124 *Id.* Although many Net users operate under an illusion of anonymity, the reality is often that one's online activities can very easily be monitored. Richard T. DeGeorge, *Law and Ethics in the Information Age*, 20 BUSINESS AND PROFESSIONAL ETHICS JOURNAL 5, 12-18 (2001) (concluding, "[t]he voluntary approach to privacy protection does not work, and often raises false beliefs and expectations.")

125 *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1195-99 (1998) (discussing how the private sector seeks to exploit data commercially for database marketing); Jonathan Krim, *Web Firms Choose Profit over Privacy; Policies Can Hide Sale of Customer Data*, WASH. POST, July 1, 2003, at A1 (noting that many Web sites promise to protect consumer information from sale to a third party, but instead often rent the information to others). For other studies on the surreptitious collection of information in cyberspace, *see* generally Roger Clarke, *Information Technology and Dataveillance*, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html (1988); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

126 One study conducted by the FTC found that ninety-two percent of the 674 Web sites it visited collected personal information from their visitors, but eighty-six percent of those did not disclose their reasons for collecting the information or share what they did with the data after collection. Michelle Z. Hall, Note, *Internet Privacy or Information Piracy: Spinning Lies on the World Wide Web*, 18 N.Y.L. SCH. J. HUM. RTS. 609, 610 (2002) (citing FTC, *FTC Releases Report on Consumers' Online Privacy*, *at* http://www.ftc.gov/opa/1998/06/privacy2.htm (June 4, 1998)).

for a variety of purposes.[127] ISPs are capable of tracking software downloaded by individuals.[128] These records are a form of identification: Web server logs show that an individual using a particular ISP visited a Web site on a certain date and time, and the ISP usually keeps records of the identity of the IP address holders.[129] Others use "Web bugs," which are small, invisible graphics placed on Web sites or email messages to monitor the activities of individual users.[130] On email messages, Web bugs allow the creator of the message to know when the message was read, to detect the IP address of an anonymous user, and to determine if and when the message is forwarded to others.[131] These examples suggest that companies are routinely harvesting consumer information, ironically even as the FTC requires them to profess a public commitment to protecting consumer privacy.

The most significant illustration of this development stems from the growing expansion of property rights over consumer information to the harvesters themselves, rather than the individual.[132] Without a corresponding architectural structure to supplement the human desire for seclusion, it becomes extremely difficult to discern a clear dividing line between public and private information.

This situation is best demonstrated by reference to web browsing information, which reflects a similar hierarchical divergence between expectations of privacy and property. As

---

127 In a tracking software system, every time a user requests certain information from a content provider, that request is stored on an "access log" that stores the user's Internet address, computer type, requested page, date, and time, most of which are transmitted back to the provider in order to track the Web site requested, the information found, and levels of activity on the site, along with other types of information. *See* Hall, *supra* note 126, at 616.

128 Marc Waldman ET AL.., *Trust*, *in* PEER-TO-PEER 242, 244 (Andy Oram ed., 2001).

129 *Id.* at 250-51.

130 John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?*, 39 ALTA. L. REV. 346, 355-56 (2001) (describing the various ways third parties employ "Web bugs" online).

131 Lynn Chuang Kramer, *Private Eyes Are Watching You: Consumer Online Privacy Protection – Lessons from Home and Abroad*, 37 TEX. INT'L L.J. 387, 394-95 (2002); *see also* ELEC. PRIVACY INFO. CTR., PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 60 (2002) (additional privacy concerns).

132 Bergelson, *supra* note 104, at 383.

Professor Solove has pointed out, individuals are not the lone creators of their web-browsing information, partly because so much of that information is created by the interaction between the user and various web sites.[133] Moreover, much of the information that is used is likely to be considered public information—names, addresses, telephone numbers, or e-mail addresses.[134] Yet, at the same time, however, it is undeniable that a consumer might consider a significant amount of a person's online activities—surfing particular sites, for example—to be private and sensitive information.[135]

Nevertheless, in perhaps the most ironic result of the informational privacy debate, intellectual property rights in such information are granted to the gatherer of the information, instead of to the subject herself.[136] Indeed, an individual, at least doctrinally speaking, has little power to control, own, or prevent disclosure of personal information held by third parties to other, institutional information-seekers.[137] For example, in *United States v. Miller*, the Supreme Court held that a person had no legitimate "expectation of privacy" in his bank records after they were turned over to a third party.[138] Given the absence of a clearly defined, legislative enforcement mechanism to protect informational privacy, constitutional or otherwise, in cyberspace, a system of self-regulation has sprung up to ostensibly honor a governing principle: a Web site should leave a person's consumer information alone, except to the extent that the person consents to the use and collection of his or her personal data.[139] Yet, despite this praiseworthy proposition, once an item of information has been recorded in an online

---

133 Solove, *supra* note 23, at 1112.

134 Jessica Thill, *The Cookie Monster: From Sesame Street to Your Hard Drive*, 52 S. CAR. L. REV. at 924, 938 (2001). *See* Electronic Privacy Information Center, *Privacy and Consumer Profiling*, *at* http://www.epic.org/privacy/profiling; James P. Nehf, *Recognizing the Societal Value in Information Privacy,* 78 WASH. L. REV. 1, 23-24 (2003); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1424-25 (2001), and JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2001).

135 *Id.*

136 *See* Bergelson, *supra* note 104, at 383 ("Under the current law, individuals neither own their personal information, nor have a recognized privacy interest in it.").

137 Mell, *supra* note 17, at 20

138 United States v. Miller, 425 U.S. 435 (1976).

139 *See* Hetcher, *supra* note 120, at 335.

computer system, no consistent rules govern the ownership of such information not already protected by copyright or other intellectual property doctrines.[140]

The most apt symbol of this development involves legal claims over database property, which are considered a robust form of commodifiable property, even though they raise strong privacy implications. For example, in *In re Toysmart.com*, a bankruptcy court permitted the sale of personal consumer information to a third party, despite the fact that its original privacy policy expressly promised that "personal information….is never shared with a third party," and that "all information obtained by toysmart.com is used only to personalize your experience online."[141] Despite these guarantees, a bankruptcy court permitted the sale of Toysmart.com's database to a third party entity, pursuant to the third-party's assurances to the FTC that it would maintain the same privacy standards of Toysmart.com itself.[142] In response, a dissenting commissioner curtly observed, "[i]f we really believe that consumers attach great value to their personal information and that consumers would be able to limit access to such information through private agreements, we should compel businesses to honor the promises that they make to consumers . . .In my view, such a sale should not be permitted because 'never' really means never."[143]

Clearly, the commodification of personal information, particularly in the Internet context, has powerful implications, altering the incentives for protection for consumer privacy. Here, the construct of information as property—particularly as database property—actively subordinates the protection of privacy to property principles.[144] This observation seems relatively straightforward in the context of a sale of database of personal information (like Toysmart.com), but it is equally

---

140 *See* Mell, *supra* note 17, at 22.

141 *See In re* Toysmart.com, LLC, No. 00-13995-CJK (Bankr. D.Mass. July 20, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmarttbankruptcy.1.htm.

142 *Id.*

143 Dissenting Statement of Commissioner Swindle, *In re* Toysmart.com, LLC, No. X000075, *available at* http://www.ftc.gov/os/2000/07/toysmartswindlestatement.htm.

144 For a wonderful discussion of the relationship between privacy and property in the data context, see Paul M. Schwartz, Property, Privacy and Personal Data, 117 HARV. L. REV. 2055 (2004).

applicable to other contexts as well. Cookies, for example, are pieces of code that provide a Web site with information about a user and that can be used to identify her computer to create personalized marketing information.[145] In one of the first privacy cases regarding web browsing information, *In re DoubleClick*, the plaintiffs contended that DoubleClick's cookies illegally collected information that Web users considered to be personal and private information,—including a user's name, email address, home and business address, telephone number, searches performed, and Web sites visited. This information was then aggregated and compiled to build demographic profiles of the users, eventually resulting in 100 million profiles.[146] Just before the case was filed, DoubleClick purchased Abacus Direct Corp., a direct marketing service company that maintained a database of names, addresses, telephone numbers, retail purchasing habits, and other personal information of approximately 90 percent of U.S. households.[147] Certain members of the public feared, perhaps justifiably, that a merger between the two companies might result in their matching information about the on and off-line behavior of individual households.[148] Later, a number of plaintiffs filed suit in federal court, making claims under federal and state law, including allegations that DoubleClick had violated the Electronic Communications Privacy Act (ECPA), the Federal Wiretap Act,

---

145 Seth R. Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, *in* FIRST ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH TECH AND CHANGING REGULATORY ENVIRONMENT (PLI Patents, Copyrights, Trademarks, and Literary Property Course, Handbook Series No. G0-00G0, 2000), *available at* WL 607 PLI/PAT *141, at *143 (2000).

146 *Id.* at *144. The first time a user accesses a Web site that is part of the DoubleClick network, composed of over 11,000 sites, a cookie with a globally unique identifier (GUID) is placed on her computer. Every time she accesses any of the Web sites connected to the network, the information is automatically transmitted back to DoubleClick, thus allowing the company to build a portfolio of information about an individual consumer. Seth R. Lesser, Privacy Law in the Internet Era: New Developments and Directions, 607 PLI/Pat 141 at 144 (2000); *See also In re DoubleClick Privacy Litigation*, No. 00 CIV 0641 NRB, 2001 WL 303744 (S.D.N.Y. Mar. 28, 2001)..

147 *See Doubleclick,* 2001 WL 303744, at *505.

148 Indeed, shortly after it acquired Abacus, DoubleClick removed its assurance from its Privacy Policy that information gathered from users online would not be associated with their personally identifiable information. Shortly thereafter, the FTC launched an investigation into whether DoubleClick's collection of consumer information constituted an unfair and deceptive trade practice. *Id.*

various state laws governing privacy, and common law invasions of privacy and trespass to property.[149]

In a significant opinion, the district court rejected each of these claims and dismissed the complaint, marking the first time a court dealt substantively with company-sponsored information harvesting, and invasions of consumer privacy by computer monitoring. In doing so, the court drew several conclusions that extended property rights in the information to harvesters, rather than to the individuals themselves. The court first distinguished DoubleClick's property rights to the cookies in questions from the privacy rights of the parties, subjugating the latter to the former. In stark contrast to the principles set forth by both Locke and Warren and Brandeis, the court's opinion suggested that an individual's personal identifying information is the property of the company that harvests it, not of the consumer. Rather than construing the information as a property held by the consumer, the court placed a primary value on the company's property rights to the information.[150] In a powerful assertion of DoubleClick's rights over the cookies placed on the individual hard drives, the court observed:

> "Even if we were to assume that cookies and their identification numbers were 'electronic communication[s] . . . in electronic storage,' DoubleClick's access is still authorized. . . . In every practical sense, the cookies' identification numbers are internal DoubleClick communications—both 'of' and 'intended for' DoubleClick. DoubleClick creates the cookies, assigns them identification numbers, and places them on plaintiffs' hard drives."[151]

In other words, the opinion suggested that the cookies were the ultimate property of DoubleClick, irrespective of the consumer's proprietary interests in the information, and should take precedence over the privacy rights of the individual consumers

---

149 *Id.* at *500, *507.

150 As a basic matter, the court held that the cookies placed on the individual hard drives were not in "electronic storage" under the ECPA, because they remained on the plaintiff's computers virtually indefinitely, and the ECPA was intended only to protect communications held in interim storage by electronic communication service providers. *Id.* at 511-13.

151 *Id.* at 513.

themselves. The court explained that users generally—unwittingly—contractually authorize Web sites to gather information because the Web sites they visit may allow banner advertisements to gather information.[152] Consequently, the court reasoned that the visit itself suggested consumer consent to such monitoring.[153]

Thus, given the property rights accorded to DoubleClick, the court held that DoubleClick could not be held liable for any invasions of privacy that the cookies themselves cause. Because the cookies do not actually store information, but instead merely identify browsers associated with particular information, the court observed that nothing could legally preclude third parties from obtaining this information by agreement.[154] In a striking observation, the court observed that "[t]he cookies and their identification numbers are vital to DoubleClick and meaningless to anyone else."[155] It also found that the cookies are akin to "purely internal administrative data" meant only for DoubleClick, not for the consumer.[156] Here, the court explained that virtually "all" plaintiffs are "unaware" that the cookies exist, that they have identification numbers, and that the numbers are critical to DoubleClick's operations.[157] The court analogized that a cookie was akin to a barcode placed on a business reply card.[158] Barcodes and identification numbers, like cookies, are meaningless to consumers, but valuable to companies.[159]

Moreover, the court rejected the plaintiff's claims under the Federal Wiretap Act, which provides for criminal punishment and a private right of action against any person who intentionally intercepts an electronic communication for the purpose of committing a tortious act in violation of federal or

---

152 *Id. See* Alexander H. Burke, *Information Harvesting on the Net*, 14 LOY. CONSUMER L. REV. 125, 134 (2002); *see also* Chance v. Avenue A., Inc., 165 F. Supp.2d 1153, 1161 (W.D. Wash. 2001).

153 *Id. See also Chance,* 165 F. Supp2d at 1161. For an opposing view, see *Pharmatrak*, 329 F.3d at 13.

154 *Doubleclick, Inc.*, 154 F. Supp. 2d at 513-514.

155 *Id.*

156 *Id.*

157 *Id.*

158 *Id. But see Pharmatrak*, 329 F.3d at 9 (disagreeing with this view).

159 *Doubleclick, Inc.,* at 515.

state law.[160] Here, the court implicitly suggested that the presence of profit motives or ordinary business practices could reasonably immunize trespass of a person's confidential information. The court opined that even if it found that DoubleClick committed every act alleged in the Complaint, the mere commission of a tortious act does not prove a tortious purpose. Citing congressional commentary, it pointed out "[t]here are, of course, certain situations in which consensual electronic surveillances may be used for legitimate purposes . . . without intending in any way to harm the nonconsenting party."[161] Because DoubleClick's motives were determined to be commercial in nature, not illegal or tortious, there was no evidence to raise the question of whether DoubleClick acted with a tortious purpose, and the court dismissed the claim.[162]

In reaching these conclusions, however, the court actually reversed a number of perceptions among the U.S. public regarding the entitlement to informational privacy. For example, the court's opinion wrongly suggests that such tracking information—and the act of tracking the information itself—are activities that are somehow "meaningless" to the actual consumer. This observation is belied by the court's own opinion. Indeed, after rejecting the plaintiffs' claims, the court appeared to recognize that DoubleClick's actions *did* violate normative expectations of informational privacy. The court, for example, concluded its decision by declaring that the consumer privacy concerns raised in the litigation were "not unknown to Congress," and predicted that congressional action on privacy protection was a likely possibility. "Congress is aware of the conduct plaintiffs' challenge and is sensitive to the privacy

---

160 *Id*.

161 *Id.*

162 The court observed, "DoubleClick's purpose has plainly not been to perpetuate torts on millions of users, but to make money by providing a valued service to commercial Web sites." *Id.* at 519. In analyzing the plaintiffs' third claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the court also found that the aggrieved plaintiffs did not plead a cognizable cause of action because they had failed to allege facts that could support the finding that the alleged injuries—invasion of privacy, trespass to personal property, and misappropriation of confidential data—met the $5,000 threshold requirement. Because the plaintiffs could have, at no cost to themselves, prevented DoubleClick from collecting personal information by selecting options on their browsers or by using an "opt-out" cookie from DoubleClick's Web site, the Court found that any remedial economic losses were insignificant, "if, indeed, they exist at all." *Id.* at 520.

concerns it raises," the court concluded, plainly recognizing that the injury visited on the plaintiffs was problematic, even if not cognizable by preexisting legislation.[163]

In many ways, the Court's treatment symbolizes the growing divide between expectation and reality that characterizes the state of informational privacy in cyberspace. On one hand, the court clearly recognized the rhetorical force behind entitlements of informational privacy and its accompanying expectations in cyberspace, but on the other hand, it placed a greater value on the property rights of the monitoring company itself. In this context, as well, principles of informational privacy, fail to protect against the surreptitious collection of data; rather, property rights become reified through its subordination.

II. THE CONVERGENCE BETWEEN CONSUMER AND PIRACY SURVEILLANCE

The developments that I have outlined above—the increasing prominence of an electronic persona, and the increasing subtleties behind monitoring the electronic persona—may seem distinguishable, but they become even more intimately related in the peer-to-peer context, particularly where copyright enforcement is concerned. Indeed, the confused and somewhat fearful way both public and private entities have responded to peer-to-peer file sharing demonstrates an interesting convergence of interests between anti-piracy advocates and harvesters of personal information. The end result is a regime of surveillance that quietly mimics regimes of consumer monitoring: here, intellectual property owners have sought to find ways to protect their works from unauthorized use, thereby creating a new mode of monitoring that crosses the boundaries between commercial self-interest and prurient intrusion on informational privacy. And, just as undesirably, such regimes have led both public and private entities to respond even more forcefully than necessary, seeking to erode not only the peer-to-peer networks that have sprouted throughout the Net, but the protection of informational privacy and identity.

---

163 *Doubleclick, Inc., at* 520.

In the previous section, I argued that perceptions of informational privacy and anonymity in cyberspace have inevitably led individuals to perceive a mantle of anonymity that they might not enjoy in real life.[164] Add to this another element: peer-to-peer file-sharing programs that permit the exchange of copyrighted content from each other's hard drives.[165] Obviously, the seduction—and danger—of the peer-to-peer world is that it enables the seemingly anonymous and widespread distribution of content, such as film, music, software, and text. Unsurprisingly, the potential for unauthorized transmission of copyrighted works has led some to characterize the Internet, for better or worse, as a "pirate utopia."[166] Yet despite the clear risk of panoptic surveillance discussed in the previous section, peer-to-peer networks are permeated with a high perception of cooperation and trust between users, which raises the question of why, in the face of such risks of detection, individuals continue to cooperate so readily in sharing their files with others.[167]

For some time, file sharers believed that no one was watching as millions continued to upload and download copyrighted files with impunity. According to Professor Lior Strahilevitz, an additional explanation for such cooperative behavior stemmed from "charismatic code," which involves "technologies that magnify cooperative behavior and mask uncooperative behavior in peer-to-peer networks."[168] Since peer-to-peer applications are designed to encourage cooperation by as many users as possible, they harnessed actual members of the community to enforce norms of file sharing and to encourage

---

164 A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Case, And Distributed Databases*, 15 J.L. COM. 395, 462-464 (1996).

165 *See* Hari Balakrishnan, et. al., *Looking Up Data in P2P Systems*, 46 COMMUNICATIONS OF THE ACM 43 (2003).

166 *See* Hakim Bey, *The Temporary Autonomous Zone*, *in* CRYPTO ANARCHY, CYBERSTATES, AND PIRATE UTOPIAS 401 (Peter Ludlow ed., 2001) (comparing online communities to our perception of pirate communities).

167 *See* Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505, 508 (2003); *see also* Michael Feldman et. al., *Free Riding and White Washing in Peer to Peer Systems,* PROCEEDINGS OF THE ACM SIGCOMM WORKSHOP ON PRACTICE AND THEORY OF INCENTIVES IN NETWORKED SYSTEMS 228 (2004), *at* http://doi.acm.org/10.1145/1016527.1016539.

168 Strahilevitz, *supra* note 167, at 510.

reciprocity.[169] Another explanation for widespread complicity in copyright infringement is provided by Professor Tim Wu, who argues that peer-to-peer networks exploit an important ambiguity regarding ethics of home copying.[170] Unlike norms against stealing in real space, which are generally well-established, peer-to-peer networks are designed to "look and feel more like non-commercial home copying [of copyrighted content]," thereby blurring the distinction between "stealing" and "copying."[171]

Part of the reason for the growth of such strategies ultimately stems from the nature of copyright law itself. Copyright law has traditionally relied on private entities—owners, private detectives, creators—for its execution. Although the No Electronic Theft Law Act ("NET Act"),[172] for example, provides for criminal prosecutions for infringement (even where no monetary profit or commercial gain can be derived from the infringing activity), most copyright actions tend to involve private, rather than public, modes of enforcement. A decision to enter into a lawsuit over infringement is completely discretionary to the copyright owner,[173] as is a copyright owner's ability to silence the speech of others through actions for infringement. Moreover, copyright law is infused with gatekeeper concepts, in that third parties often play key roles to

---

169 *Id.* at 534. In one example, a Gnutella screen falsely represented to users: "The other half of Gnutella is giving back. Almost everyone on GnutellaNet shares their stuff." *Id.* at 550.

170 *See* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 685 (2003).

171 *Id.*

172 No Electronic Theft (NET) Act, Pub. L. No. 105-147 (1997) (codified in the sections of 17 & 18 U.S.C.). Under these provisions, individuals can also be held civilly liable for actual damages of lost profits. *Id.* Online infringement of copyrighted music is punishable by up to three years in prison and $250,000 in fines, or six years for repeat offenders. *See* Karen J. Bernstein, *The No Electronic Theft Act: The Music Industry's New Instrument in the Fight Against Internet Piracy*, 7 UCLA ENT. L. REV. 325 (2000) (discussing the NET Act and sentencing guidelines under it); Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 250-52 (1999) (discussing changes in the criminal law after the passage of the NET Act); Heather Jacobson & Rebecca Green, *Computer Crimes*, 39 AM. CRIM. L. REV. 273, 288-92 (2002) (discussing the NET Act and other acts regarding the illegality of online piracy).

173 This observation extends to the patent context as well. *See* John R. Thomas, *Liberty and Property in the Patent Law*, 39 HOUS. L. REV. 569, 596 (2002).

prevent infringement.[174] Following this model, copyright law has traditionally imposed liability on parties who were capable of copying and distributing works, like book publishers, record manufacturers, film studios, and others capable of producing works on a massive scale.[175]

Yet, partly due to the outcome of various cases in the peer-to-peer context, particularly *Grokster*, liability has been shifted towards individual users, rather than software intermediaries.[176] As a result, in the wake of *Napster* and the DMCA, peer-to-peer file sharing has become the new proxy for criminality and infringement.[177] Just as the law's failure to protect individual privacy has facilitated the creation of consumer surveillance, it has also enabled intellectual property owners to develop similarly panoptic strategies to address the problem of piracy. Intellectual property owners have responded to peer-to-peer file sharing in a way that exposes a clear synergy between consumer monitoring and copyright enforcement. They have done so by attempting to expand the law to control the dynamics of Web architecture, informational privacy, and anonymity, and by enabling intellectual property owners to detect and defend their products against unauthorized uses.

Today, the seemingly intractable problem of digital piracy has led to the creation of massive offensives—criminal, civil, and international—spearheaded by private intellectual property owners. Private companies routinely join forces with law enforcement officials to investigate and prosecute individuals for trafficking in pirated materials.[178] The music industry has also

---

174 *See* Reinier Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 53-54 (1986).

175 *See* Wu, *supra* note 170, at 710.

176 *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1164-1166 (9th Cir. 2004).

177 *See* Aaron M. Bailey, *A Nation of Felons: Napster, the NET Act, and the Criminal Prosecution of File-Sharing*, 50 AM. U. L. REV. 473 (2000) (offering a treatment of the criminal implications of illegal file sharing).

178 *See* RIAA, *RIAA Releases Mid-year Anti-Piracy Statistics*, *at* http://www.riaa.com/news/newsletter/press2001/100901.asp (last visited Oct. 17, 2003) (reporting that the RIAA works closely with federal, state, and local officials, and that it aided in 1,762 arrests and indictments in the first six months of 2001). In 1999, for example, Jeffrey Levy, a student at the University of Oregon, pled guilty to criminal copyright infringement for his use of school computers to post software and music on the Web for others to download. *See* Ashbel S. Green, *Net Piracy Gets First Conviction: UO*

launched a calculated attempt to shift the political and economic costs of copyright enforcement onto third parties, particularly ISPs.[179] A constant drumbeat of threatened suits, both direct and contributory, has resulted in a host of measures taken by ISPs out of fear of liability for copyright infringement.[180] The recording industry's armies of anti-piracy investigators routinely crawl through the Internet, including university networks, searching for and logging presumed unauthorized uses of copyrighted material.[181]

As part of this attack on consumer downloading, the RIAA relies on using the term "piracy" to denote an alarmingly expansive array of activities. The use of the concept of piracy to refer to the unauthorized duplication of original commercial products,[182] or counterfeiting,[183] dates back to the nineteenth

---

Student, PORTLAND OREGONIAN, Aug. 21, 1999, *available at* 1999 WL 5367412. In announcing the prosecution's case, Assistant Attorney General James K. Robinson declared:

> Mr. Levy's case should serve as a notice that the Justice Department has made prosecution of Internet piracy one of its priorities . . . . Those who engage in this activity, whether or not for profit, should take heed that we will bring federal resources to bear to prosecute these cases. This is theft, pure and simple.

Id.

Today, the Department of Justice has listed intellectual property crimes as one of its key priorities. See Katie Dean, Ashcroft Announces Assault on Piracy, wired.com, October 14, 2004.

179 *See infra* Part III. The RIAA, a trade association whose membership produces ninety percent of all sound recordings in the United States, fights "a well-nigh constant battle against Internet piracy, monitoring the Internet daily, and routinely shutting down pirate Websites by sending cease-and-desist letters and bringing lawsuits." Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., 180 F.3d 1072, 1074 (9th Cir. 1999); RIAA, *What the RIAA Is Doing About Piracy*, *at* http://www.riaa.com/issues/piracy/riaa.asp (last visited Oct. 17, 2003) (describing the RIAA's strategy of using subpoenas that require ISPs to identify the operators of sites that host infringing files).

180 *See* text accompanying notes 258-369.

181 As part of this program, anti-piracy forces have also implicitly equated Internet piracy with other types of undesirable criminality. One method focuses primarily on consumer education; the RIAA actively propagates the notion that downloading MP3s, or copying other copyrighted works, is simply another form of theft. *See* RIAA, *Penalties of Piracy*, *at* http://www.riaa.com/ issues/piracy/penalties.asp (last visited Oct. 17, 2003) (defining different copyrights and outlining possible penalties for copyright infringement).

182 Anderson v. Nidorf, 26 F.3d 100, 101 n.1 (9th Cir. 1994)

century.[184] Today, however, the term also suggests the growing power of content owners to discursively define much more expansive controls over access to content itself.[185] Suddenly, for the RIAA's purposes, it seems that downloading music for personal purposes is "piracy," equated via sheer rhetoric to organized, usually criminal, counterfeiting of intellectual property. So, too, is sharing music, lending someone a tape, or perhaps even recording a sample of music on an answering machine. All of these acts, seemingly innocuous and innocent just a few years ago, today arguably fall under the rubric of "piracy," a metaphor suggesting that these acts are somehow

---

(quoting from Piracy and Counterfeiting Amendments Act of 1982, 18 U.S.C. § 2311 (1982)); *see also Diamond Multimedia Sys.*, 180 F.3d at 1072 (discussing piracy as the unauthorized copying of copyrighted materials).

183 As Judge Posner observed, "[p]iracy and the infringement of copyrights, titles (presumably of books, songs, products, services, and so forth), and slogans (advertising and other) are simply different forms of theft (broadly conceived) of information." Curtis-Universal, Inc. v. Sheboygan Emergency Med. Servs., Inc., 43 F.3d 1119, 1124 (7th Cir. 1994).

184 *See* Evans v. Eaton, 16 U.S. (3 Wheat.) 454 (1818) (describing an alleged use of a flour manufacturing machine as "piracy").

185 Indeed, the term "piracy" is now ubiquitous throughout media commentary on intellectual property law, a largely unhelpful but rhetorically powerful term that is often bandied about by lawyers and activists to denote a vast array of seemingly "illegal" activities. *See* Jessica Litman, *War Stories*, 20 CARDOZO ARTS & ENT. L.J. 337, 342-50 (2002). Litman states:

> Piracy used to be about folks who made and sold large numbers of counterfeit copies. Today, the term 'piracy' seems to describe any unlicensed activity. . . . Content owners argue that the reason consumers are now pirates is that technology now makes it possible for small-scale unauthorized users to commit grand theft. From the so-called pirates' point of view, though, they are doing the same sort of things unlicensed users have always done–making copies of things for their own consumptive use, sharing their copies with their friends, or taking the works apart to see how they operate. What has changed is not the behavior but the epithet. Content owners are understandably concerned that in a digital environment, conduct that used to be harmless might have the same effect as the commercial sale of large numbers of counterfeit copies. They have managed to persuade a substantial segment of the public that if behavior theoretically could have the same effect as piracy, it must *be* piracy, and must therefore reflect the same moral turpitude we attach to piracy, even if is the same behavior that we all called legitimate before.

Id. at 349-50.

contemporaneously equivalent to crossing the high seas, invading a ship, stealing its contents, and threatening life.[186]

This strategy has been effective.[187] The RIAA has threatened ISPs and universities with contributory infringement suits if they do not act immediately to reveal the identity of subscribers, terminate the subscribers' Internet connections, and issue generalized threats of criminal prosecution to the student body.[188] In April 2003, the RIAA took another step,

---

186 The RIAA's Web site, for example, declares that piracy is "old as the Barbary coast, new as the Internet." Its announcement observes:

> No black flags with skulls and crossbones, no cutlasses, cannons, or daggers identify today's pirates. You can't see them coming; there's no warning shot across your bow. . . . *Today's pirates operate not on the high seas but on the Internet, in illegal CD factories, distribution centers, and on the street.* The pirate's credo is still the same–why pay for it when it's so easy to steal? The credo is as wrong as it ever was. Stealing is still illegal, unethical, and all too frequent in today's digital age. That is why RIAA continues to fight music piracy." RIAA, *Anti-Piracy*, *at* http://www.riaa.com/issues/piracy/default.asp (last visited Oct. 17, 2003). The RIAA defines music piracy in four specific categories: (1) pirate recordings, or the unauthorized duplication of only the legitimate recordings, minus the trade packaging normally associated with the music product; (2) counterfeit recordings, or unauthorized recordings of the prerecorded sound as well as the unauthorized duplication of original artwork, label, trademark, and packaging; (3) underground or "bootleg" recordings, or unauthorized recordings of live concerts or those broadcast on radio or television; and (4) online piracy, involving the unauthorized uploading of a copyrighted sound recording to make it publicly available, downloading the sound recording from the Internet site (even if it is not resold), or certain uses of "streaming" technology from the Internet.

Id.

187 In the first half of 2001, for example, the RIAA announced that its efforts "led to a record number of arrests, raids, illegal product seizures, guilty pleas and convictions." *See* RIAA, *RIAA Releases 2001 Physical Anti-Piracy Figures*, *at* http://www.riaa.com/news/newsletter/040502.asp (last visited Oct. 17, 2003) (discussing copyright enforcement methods utilized in 2001).

188 In 2003, the RIAA sent letters to every university and college in the United States, as well as the top one thousand corporations, reminding them of their obligations as ISPs. *See* RIAA, *Actions Taken by U.S. Music Community to Step Up Public Education Efforts in Just the Past Twelve Months*, *at* http://www.riaa.com/news/newsletter/062503_d.asp (June 25, 2003).

filing suits against four college students accused of using internal college networks to facilitate file trading,[189] and announcing its plan to sue others. Since then, over six thousand people have been sued for copyright infringement, including a twelve-year-old girl.[190] As a result, ISPs have also taken up the mantle of copyright enforcement: employers and universities have banned the use of file sharing software, fired employees for engaging in acts of copyright infringement at work, and threatened to prosecute and expel students for their file sharing activities.[191] Some colleges refuse to permit individuals to send MP3 files at all, irrespective of whether the files fall under fair use or are taken from the public domain.[192] A multitude of ISPs act immediately after receiving notice from intellectual property owners, taking down Web sites and terminating Internet access for their subscribers with little concern for whether or not the alleged infringement is actually taking place.[193]

---

189 *See* Reuters, *RIAA Sues College File Traders*, WIRED NEWS, Apr. 3, 2003, *at* http://www.wired.com/news/technology/0,1282,58340,00.html.

190 Katie Dean, *Movie Studios Sue File Traders*, WIRED NEWS, Nov. 16, 2004, *at* http://www.wired.com/news/digiwood/0,1412,65730,00.html. Kristen Philipkoski, *Battle Not over for File Sharers*, WIRED NEWS, Dec. 23, 2003, *at* http://www.wired.com/news/digiwood/0,1412,61714,00.html.

191 Consider the recent letter issued to students at Pennsylvania State University, which warned:

> The software, record, and movie industries are stepping up their enforcement of copyright laws. They are using computer technology to detect those who run servers or simply download something they have no right to possess. The likelihood of being caught is growing every day and prosecutions will become more frequent. . . . Messing up your future is a steep price to pay for music or a video.

Rodney Erickson, Provost, *An Important Message on a Key Issue from the Provost* (Mar. 31, 2003) (on file with author).

In September 2002, the administrators of the University of Southern California warned students that using peer-to-peer file sharing networks could force the university to deny network access to students, warning that "the entertainment industry has been 'obtaining snapshots' of Internet IP addresses and a list of files being traded by people across the country." *See* Brad King, *USC to Students: No Sharing Files*, WIRED NEWS, Sept. 13, 2002, *at* http://www.wired.com/news/mp3/0,1285,55159,00.html.

192 *See* E-mail from Rebecca Tushnet, Fordham University, to Sonia K. Katyal, Associate Professor, Fordham University School of Law (Apr. 1, 2003) (on file with author) (noting that sending MP3s to university email accounts is not permitted).

193 *See, e.g.*, Electronic Frontier Foundation, *Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands*, *available at*

In the following section, I offer a new reading of the implications of the various cases involving peer-to-peer transmissions, arguing that the DMCA's treatment of contributory liability—as well as other anti-piracy initiatives—perpetuates a conflict between privacy, speech, and intellectual property that feeds into the creation of private regimes of piracy surveillance.

A. ORIGINS OF PIRACY SURVEILLANCE

Just as the law's failure to enact robust protections for informational privacy facilitates the creation of consumer surveillance, it has also played a mediating role in enabling intellectual property owners to develop similar strategies to address the problem of piracy. In this section, I offer a new reading of *Napster*, arguing that the DMCA's treatment of contributory liability—as well as other anti-piracy initiatives—perpetuates a conflict between the protection of informational privacy and intellectual property.[194] As this section will argue, the *Napster* court's adoption of a knowledge standard for contributory liability has unwittingly transformed Internet Service Providers into potential copyright enforcers, a factor that has hastened the development of piracy surveillance on the Internet.

1. THE DIGITAL MILLENNIUM COPYRIGHT ACT AND PEER-TO-PEER JURISPRUDENCE

Until *Napster* was announced, anti-piracy laws, though pervasive and expanding in power, largely escaped the public eye. Yet on February 12, 2001, the Ninth Circuit dealt a substantial blow to the file sharing community when it affirmed

---

http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php (last visited Jan. 21, 2004) (offering examples of ISPs forced to take down specific, non-infringing information); *Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Permanent Subcomm. on Investigations, Comm. on Governmental Affairs*, 108th Cong. 1 (2003) [hereinafter *Privacy & Piracy, Hearing Before the Senate Permanent Subcomm. on Investigations*] (statement of Lorraine Sullivan) (observing that Time Warner, Sullivan's cable provider, was "forced" to release her personal information to the RIAA). *See also infra* Part III.

194 A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

in part a preliminary injunction against Napster, Inc., a corporation that developed software to facilitate the transmission of MP3 files.[195] Napster's search and "hotlist" functions allowed users to search for a particular song or to keep a list of previously accessed users handy so that they could be notified if others from their hotlist were logged into the system. Most significantly, Napster software maintained a rough index of files available to facilitate transfer of MP3 music, a factor that suggested an element of centralization to its peer-to-peer format.[196]

On this proposition, the RIAA claimed that Napster users were engaged in the "wholesale reproduction and distribution of copyrighted works, all constituting direct infringement."[197] In addition to Napster, the suit named a number of anonymous Jane Doe defendants consumers who had been using Napster—and various universities, including Yale University, the University of Southern California, and Indiana University, alleging that they were complicit in the infringement.[198] On appeal, the Ninth Circuit observed that Napster's users violated two of the copyright holders' exclusive rights: the rights of reproduction and distribution.[199]

At the time, almost no scholars looked beyond the relationship between law and technology to focus on the effect of

---

195 *Id.* at 1011. For discussions of Napster and its various implications, see Michael W. Carroll, *Disruptive Technology and Common Lawmaking: A Brief Analysis of* A&M Records, Inc. v. Napster, Inc., 9 VILL. SPORTS & ENT. L.J. 5 (2002) (discussing the implications of the *Napster* decision); Stephanie Greene, *Reconciling* Napster *with the* Sony *Decision and Recent Amendments to Copyright Law*, 39 AM. BUS. L.J. 57 (2001) (discussing the effects of the *Napster* decision on copyright law); Raymond Ku, *Creative Destruction of Copyright*, 69 U. CHI. L. REV. 263 (2002); Glynn Lunney, *The Death of Copyright*, 87 VA. L. REV. 813 (2001), Neil Netanel, *Impose a Non-Commercial Use Levy*, 17 HARV. J. L. & TECH. 1 (2003); Peter Yu, *P2P and the Future of Private Copying*, 76 U. COLO. L. REV. __ (forthcoming 2005);.

196 *Napster*, 239 F.3d at 1012.

197 *Id.* at 1013. In April 2000, when Metallica filed suit against Napster in Los Angeles District Court for copyright infringement and racketeering, it delivered to Napster 60,000 pages of documents identifying the usernames of people who made Metallica songs available online and demanded that Napster block them from using the service. Fisher & Yang, *supra* note 69, at Case Study 1: Napster. Napster complied and blocked 317,377 users from using its service the following month. *Id.*

198 *Napster*, 239 F.3d at 1013.

199 *Id.* at 1013-15.

Napster and the DMCA on informational privacy and the protection of personal identity, an omission that looms large four years later. Yet *Napster*'s neat standard of contributory liability created a power-sharing agreement of sorts, in which intellectual property owners shouldered the responsibility to police the Internet for evidence of unauthorized uses, and ISPs faced the responsibility of disabling access to these infringing works after receiving proper notice under the DMCA.[200] In turn, the law has privatized the protection of copyright, creating incentives for content owners to engage in self-help surveillance of consumer activities through peer-to-peer frameworks.

Following the DMCA, the *Napster* court established a set of directives for ISPs to follow in addressing the infringing activities of their users.[201] Under these provisions, an ISP is required either to identify the subscriber and/or to take down the posting as long as minimal assertions of a "good faith" belief in infringement are met.[202] The governing law has held that "one who, with knowledge of the infringing activity, induces,

---

200 *See WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2180 Before the House Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 89 (1997) [hereinafter *WIPO, Hearing Before the House Subcomm. on Courts and Intellectual Property*] (statement of Roy Neel, President, United States Telephone Association). As Neel explained:

> We believe that the task of ferreting out copyright infringement on the Internet should fall to the copyright owner. Today, copyright owners have access to a large array of Internet search engines and 'spiders' to sniff out material they know belongs to them (unlike the ISPs, who cannot be certain who may have recently purchased which copyrighted material). Once the copyright owners discover infringement, they can bring it to the attention of the ISPs. It is at this point that the ISPs can sensibly act.

Id.

201 *See Napster*, 239 F.3d at 1027-28; *see also* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1881-82 (2000). The DMCA also relieves ISPs of monetary liability for temporary storage, passive transmission, or retransmission of materials, provided that the ISP meets certain structural and technological requirements. The actual words of the DMCA exempt an ISP from contributory liability for copyright infringement unless the ISP has notice of the infringing material and has failed expeditiously to remove it. 17 U.S.C. § 512(c)(1)(A)-(C) (2000).

202 *See* 17 U.S.C. § 512(c)(3); Yen, *supra* note 201, at 1881.

causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer."[203] Thus, if an ISP "learns of specific infringing material available on [its] system and fails to purge such material from the system, [it] knows of and contributes to direct infringement."[204] Moreover, if the ISP engages in any "personal conduct that encourages or assists the infringement," it is also liable for contributory infringement.[205] The actual words of the DMCA, however, exempt an ISP from contributory liability for copyright infringement *unless* the ISP has proper notice of the infringing material and has failed expeditiously to remove it.[206] This means that unless the ISP has notice that one of its sites contains pirated MP3 files, it is under no obligation to search out such infringing material on its servers. Liability is also limited where an online provider is "unwittingly linking or referring users to sites containing infringing materials."[207]

These DMCA standards were largely instituted to strike a middle ground between two opposing standards: one that required actual knowledge of copyright infringement (an approach favored by ISPs), and another that instituted strict liability (favored by copyright owners).[208] As a result, ISPs face liability in situations where the provider had actual knowledge of the third-party infringement, or where constructive knowledge could be inferred from "facts or circumstances from which infringing activity is apparent."[209] Taken together, these

---

203 Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (footnote omitted).

204 *Napster*, 239 F.3d at 1021.

205 *Id.* at 1019. In applying these tests, the court concluded that Napster "knowingly encourage[d] and assist[ed] the infringement of plaintiffs' copyrights," because Napster had both actual and constructive knowledge that its users exchanged copyrighted music. *Id.* at 1020; *see also* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995) (defining and discussing contributory infringement).

206 Digital Millennium Copyright Act (DMCA) 17 U.S.C. § 512(c) (2000).

207 *Id.* (quoting the DMCA, 17 U.S.C. § 512(d) (2000)).

208 *See NII Copyright Protection Act of 1995: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong. 35 (1995).

209 *See WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearings on H.R. 2280 Before the House Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary*, 105th Cong., 82 (1997).

measures, at first glance, might suggest that the DMCA was relatively responsive to the concerns of ISPs in avoiding liability for the infringing activities of their subscribers. Yet, if one looks closer, it is clear something is missing from this picture: an asserted commitment to consumer privacy. Although the DMCA, as well as the *Napster* opinion, were admirable attempts to set forth a framework for contributory liability for ISPs, building on the substantial body of literature and law on third-party liability, they failed to establish or affirmatively suggest the need for any privacy protections for individual subscribers. Further, the DMCA neither offered any guidelines for detecting piracy, nor did it even require substantive judicial oversight or confirmation of a legitimate copyright dispute. As a result, standards that require evidence of actual or constructive knowledge raise the difficult and vexing question of whether, and how much, ISPs are indirectly encouraged to monitor their consumers in order to escape liability. These areas directly impact consumer privacy and autonomy in countless and invisible ways; and yet are often overlooked by courts and commentators.

These problems become particularly acute when we turn to the peer-to-peer world, which was "not even a glimmer in anyone's eye when the DMCA was enacted."[210] The DMCA has a section entitled "Protection of Privacy," which provides that an ISP is not required to monitor its service or to affirmatively seek facts indicating infringing activity, except to the extent that standard technical measures require.[211] But these "standard technical measures" are notoriously difficult to define in the wake of changing norms of technology and surveillance. The more consumer surveillance technologies alter the fabric of cyberspace, and expand to unmask and record the activities and identities of Internet subscribers, the more difficult it becomes to define and construct standard technical measures, as well as to appropriately protect expectations of privacy in response. Moreover, the vast array of ways in which ISPs and intellectual property owners have embarked on an endless journey—irrespective of this provision—through the Internet to detect the identities of those engaging in allegedly unauthorized uses of

---

210 *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 38 (D.D.C. 2003) (quoting Brief of Amici Curiae Alliance for Public Technology, et al., at 6), *rev'd*, Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs. Inc., 351 F.3d 1229 (D.C. Cir. 2003).

211 17 U.S.C.A. § 512(m) (1999).

their material clearly raises due process and speech concerns, a factor that I focus on in Part III.

Consider, for example, the difficult relationship that ISPs have with their subscribers after *Napster*. Here, ISPs play a key role in enforcing copyright law for two reasons. First, they serve as the conduit by which the intellectual property owner identifies the subscriber, and second, under the DMCA, they are forced either to take down the infringing material or to terminate Internet access to the subscriber. Thus, they are often the only barriers between ordinary citizens and the surveillance measures used by content owners to identify them.[212] As a result, ISPs are often caught between two conflicting motivations: the need to protect others' intellectual property and the need to protect their consumers' privacy, autonomy and freedom of expression.

Why has this occurred? Part of the answer involves the *Napster* opinion itself, which requires evidence of actual knowledge of specific acts of infringement, but then fails to explain what constitutes acceptable methods of searching for such information.[213] Absent specific information which

---

212 *See WIPO Hearing Before the House Subcomm. on Courts and Intellectual Property*, *supra* note 200, at 77 (statement of Robert W. Holleyman II, President, Business Software Alliance). Holleyman stated:

> "Often in conducting internet anti-piracy cases, we can locate the source of the material as a particular site on a service provider's system, but because the Internet is essentially an environment replete with 'aliases,' we cannot determine the identity of the person. This makes it quite hard to proceed with prosecution, and it would be a valuable addition to the approach taken by the bill for it to also provide incentives for service providers to share information, under appropriate circumstances, about the infringer's identity."

Id.

213 *Napster*, 239 F.3d at 1021 ("[I]f a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement."). Absent specific information that identifies infringing activity, a court cannot hold a computer system operator liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material. *Id.* Despite this balance of interests between copyright owners and ISPs, some privacy advocates previously expressed concerns that the processes used to identify the direct infringer gave "too much latitude to those who might pursue fishing expeditions" for evidence of infringement. *WIPO Hearing Before the House Subcomm. on*

identifies infringing activity, the *Napster* court concluded that a computer system operator cannot be held liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted files.[214] Instead, the Ninth Circuit chose to require specific knowledge of infringing material, thereby effecting a crucial, and overlooked, transition into piracy surveillance.[215] By placing the burden on copyright owners to identify potential infringers, *Napster* and the DMCA expanded the reach of private regimes of copyright enforcement.

Moreover, under the DMCA's "safe harbor" provisions, codified at 17 U.S.C. § 512, certain service providers may avoid contributory liability if they fulfill certain highly specialized conditions. These safe harbors apply to ISPs that may be: (a) transmitting, routing, or providing connections for infringing material; (b) caching, or temporarily and intermittently storing infringing material; (c) hosting a user who may store infringing material on a network that is controlled or operated by or for the ISP, as long as the ISP acts expeditiously to remove or deny access to the material, among other requirements; and (d) linking or referring users to an online location that contains infringing material by using information location tools like a directory, index, or hypertext link, among others.[216] Sections (b), (c) and (d), however, require ISPs to comply with the notice-and-takedown process, which requires the provider to "expeditiously remove or disable access to" infringing material

---

Courts and Intellectual Property, *supra* note 200.

214 *Napster*, 239 F.3d at 1020. Indeed, to the *Napster* court's credit, it did attempt to carve out a small area for permissible peer-to-peer transmission by recognizing the possibility for substantial non-infringing uses of Napster. The court declined to impute liability to Napster on the basis of its peer-to-peer file sharing technology alone. Being governed by *Sony Corporation of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), the *Napster* court observed, "We are compelled to make a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system." *Napster*, 239 F.3d at 1020.

215 The court decided that Napster's service could continue, as long as the music industry provided notice to Napster of the unauthorized copyrighted works and files available on the system. After the decision was remanded to the district court, the music industry began the difficult process of filtering authorized from unauthorized titles, a project that was bitterly opposed by Napster executives, who continued to ask the Ninth Circuit for relief from the intrusive measures used to search for files on the system. *See* Associated Press, *Judge Keeps Heat on Napster*, WIRED NEWS, July 12, 2001, *at* http://www.wired.com/news/ mp3/0,1285,45184,00.html.

216 *See* 17 U.S.C. § 512(a)-(d) (2000).

upon receipt of a "notification of claimed infringement" from a copyright owner that complies with certain requirements.[217] Once proper notice is given, the burden of compliance then shifts to the service provider. If the provider fails to comply with the notice-and-takedown request, then it may lose its immunity under the DMCA.[218]

As a result, the DMCA has led to the creation of a new kind of surveillance that enables content owners to search the Internet for unauthorized distributions of their products and creations—indeed, an entire industry has sprung up, seemingly overnight, that searches through individuals' hard drives, Web sites, and chat rooms to find evidence of infringement. The notice-and-takedown provisions have two other aspects that are especially important: first, they are typically limited to situations where the ISP is "hosting" an online site at its own servers; for this reason, the ISP receives a limited scope of immunity as long as it removes or disables access to the site. Second, and equally significant, the DMCA provision also provides for a "counter-notification" procedure that enables the Web site owner to dispute accusations of infringement. As a result of these guidelines, intellectual property owners have undertaken a program of monitoring for piracy, and ISPs have developed a response system that acts almost immediately to "take down" allegedly infringing material in order to avoid allegations of contributory liability.[219]

---

217 *See* Recording Industry Ass'n of America, Inc. v. Verizon Internet Services., Inc., 351 F.3d 1229, 1234 (D.C. Cir. 2003).

218 *See* Richard Raysman & Peter Brown, *Notice and Takedown Under the Digital Millennium Copyright Act*, N.Y.L.J., Feb. 11, 2002, *available at* http://www.brownraysman.com/pubs/articles/pdf/020211.pdf; and 17 U.S.C. § 512(g)(2)(B)-(g)(3) (2000). Finally, the statute also provides for limited damages and attorney's fees if material is improperly removed as the result of a misrepresentation. *See id.* § 512(f).

219 Elizabeth G. Thornburg, *Going Private: Technology, Due Process, and Internet Dispute Resolution*, 34 U.C. DAVIS L. REV. 151 (2000). Thornburg states:

> The notice and take-down provisions of the DMCA are . . . privately-operated. They depend on turning the ISP into the copyright holder's enforcer. Thus a private copyright holder complains to a private ISP, which in turn privately implements the remedy of disabling access to the challenged portions of a Web site. Unless the Web site owner files a lawsuit, the entire process takes place out of the public eye. It is commenced by a private party in a private setting and

Today, just a few years after the passage of the DMCA and the release of *Napster*, the war over digital copyright protection has continued to escalate. As courts continue to interpret the reach of *Sony*, they have indirectly altered the relationship between copyright and privacy. For example, in *Grokster*, the Ninth Circuit, affirming the decision of the district court, held that the defendants were not liable for either contributory or vicarious infringement, due to the number of current and future noninfringing uses of the software; and because of the lack of centralization, supervision, and control over its end users.[220] Because the software lacked the centralized search index and mandatory registration characteristics of Napster, the defendants were unable to patrol, control, or manage the activities of their end users. The decision said little about the specific issue of consumer privacy, but suggested a clear delineation between the particular software design, which ostensibly lacked the ability to block access to individual users, and the responsibility to safeguard, monitor, and control the actions of their users.[221] Since none of the communication between defendants and users created a point of access for filtering or searching for infringing files (the infringing material was exchanged by peers directly, instead of through a centralized server), the defendants clearly lacked the ability to police their users.[222] Given the defendants' inability to police, the court seemed to suggest no need or ability to regulate their activities, suggesting that the defendants' had little responsibility, unlike Napster, to monitor the uses of its subscribers. In short, the lack of centralization and control enabled users to engage in activities without significant

---

> enforced by another private party. There is no court, no hearing, and no decision on the issue of copyright infringement.

Id. at 189.

For a discussion of similar issues in the European context, see Sjoera Nas, *The Multatuli Project ISP Notice & Take Down*, Oct. 1, 2004, *at* http://www.bof.nl/docs/researchpaperSANE.pdf.

220 Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154 (9th Cir. 2004).

221 *See* Grokster, 380 F.3d at 1165 ("[G]iven the lack of a registration and log-in process, even Grokster has no ability to actually terminate access to filesharing functions, absent a mandatory software upgrade to all users that the particular user refuses, or IP address-blocking attempts.").

222 *Id.*

supervision from the defendants, and thereby allowed the defendants to escape liability.[223]

In contrast, the Seventh Circuit, just briefly, touched more directly upon the issue of privacy and privacy-enabling technologies, suggesting a greater degree of responsibility to a peer-to-peer defendant to monitor subscriber activity. Unlike *Napster* and *Grokster*, which enabled a relatively transparent exchange of files, *Aimster* actually encrypted files before circulating them. Thus, the presence of encryption became terribly relevant to the outcome: while the Seventh Circuit observed that encryption had valuable, non-infringing uses in fostering privacy, it also created the potential for social costs by facilitating unlawful transactions. Consequently, the court concluded that "a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used."[224] Following *Sony*, the court observed that, "[b]y eliminating the encryption feature and monitoring the use being made of its system, Aimster could, like Sony, have limited the amount of infringement."[225] Given Aimster's failure to do so, the court concluded that "its ostrich-like refusal to discover the extent to which its system was being used to infringe copyright is merely another piece of evidence that it was a contributory infringer."[226] In the end, Aimster suggests some degree of supervision of encrypted files is required in order to escape liability, irrespective of the original software design (or even the purpose of encryption itself).

When we compare the standards set forth in *Napster*, *Aimster*, and *Grokster*, we should see a relatively clear mandate: the greater the centralization, the greater the need for supervision; the greater the presence of encryption, the greater the need for supervision. In other words, the presence of privacy-enhancing technologies, like encryption, demands, and actually requires more surveillance in order to escape liability. In other words, *Aimster* suggests a stark irony: the use of

---

223 Clearly, in the end, this factor, while favoring a finding of non-liability for the defendants, set the stage for the RIAA's eventual decision to sue end users instead.

224 *In re* Aimster Copyright Litigation, 334 F.3d 643, 650-51 (7th Cir. 2003).

225 *Id.* at 654.

226 *Id.* at 655.

privacy-enhancing technologies requires one to undertake privacy-eroding practices like surveillance in order to avoid liability in the peer to peer context.

2. THE LEGACY OF *VERIZON*

In late July of 2002, the Recording Industry Association of America (RIAA) contacted Verizon seeking the identity of a user of "a computer connected to the Verizon network that is a hub for significant music piracy."[227] Verizon, citing consumer privacy concerns, refused to provide the information, and the RIAA filed suit under the Digital Millennium Copyright Act (DMCA), in a test case that involved the reach of the DMCA's special subpoena provision, known as Section 512(h).[228] In the past, these subpoenas (which disclosed the subscriber's name, address, and contact information) almost always involved individuals who stored the infringing material on the ISP's own servers, thereby making it possible for the ISP to "take down" the infringing material.

However, in this case the allegedly "infringing" information was stored on the user's *own computer hard drive*, not on Verizon's servers.[229] Consequently, Verizon refused to comply with the subpoena, explaining, "[n]o files of the Customer are hosted, stored, or cached by [Verizon]."[230] According to Verizon, the DMCA did not authorize a subpoena

---

227 Brief for RIAA at 1, *In re* Verizon Internet Services, Inc., 240 F.Supp.2d 24, No. 02-MS-00323 (D.D.C. 2003), *available at* http://www.riaa.com/news/filings/pdf/verizon/motiontoenforce.pdf, (on file with the Yale Journal of Law and Technology).

228 17 U.S.C. § 512 (2000). As Verizon's Vice-President Sarah Deutsch explained, "If the RIAA's interpretation [of the Digital Millennium Copyright Act] is accepted, there is no way we can continue to ensure our customers' privacy rights as we understand them today." Chris Marlowe, *RIAA, Verizon Tiff Revolving Around Customer Privacy*, HOLLYWOOD REP., Aug. 22, 2002, *available at* 2002 WL 24791730.

229 *See* Brief for RIAA, *supra* note 227, at 7. On July 24, 2002, the RIAA delivered a letter along with the subpoena alleging that a computer on Verizon's Internet service was "distributing to the public for download unauthorized copies of hundreds of copyrighted sound recordings owned by RIAA member companies." The letter, consistent with the notice requirements of the DMCA, specified the subscriber's IP address, along with a list of the recordings it made available for downloading. Apparently, the individual in question made these files available by Kazaa, a peer-to-peer file sharing mechanism. *See* Brief for Verizon at 6, *In re Verizon*, *supra* note 227.

230 Brief for RIAA at 8, *In re Verizon, supra* note 227.

when the offending material is stored on a person's home computer, as opposed to the Verizon network, since the applicable provision is addressed to "material that resides on a system or network controlled or operated by or for [a] service provider."[231] Because the individual's files resided on the home computer, and not the network, Verizon contended that it was "not involved with its subscriber's activities, except at most, as a passive conduit within the meaning of subsection 512(a)."[232] It claimed that the subpoena was limited only to "[i]nformation residing on systems or networks at direction of users."[233] Again, since the material was stored on a person's home computer, and not Verizon's servers, Verizon contended that the DMCA did not require it to release the subscriber's identity to the RIAA.

According to Verizon, the RIAA was seeking to expand Section 512(h) notification to cover "*all* Internet users" who stored material on their home servers, not just ISPs who stored infringing material on their networks.[234] Verizon stated that the RIAA proposed "a dazzlingly broad subpoena power that would allow any person, without filing a complaint, to invoke the coercive power of a federal court to force disclosure of the identity of any user of the Internet, based on a mere assertion in a form . . . that the user is engaged in infringing activity."[235]

In response, the RIAA threatened to subject Verizon to a suit for contributory infringement, explaining that the safe harbor provisions of the DMCA only protect an ISP from liability for its own acts of copyright infringement, and not from refraining to respond to a valid subpoena seeking the identity of

---

231 *See* 17 U.S.C. § 512(c)(3)(A) (2000); Brief for Verizon at 3, *In re Verizon, supra* note 227; *Verizon*, 240 F. Supp. 2d at 29. For this reason alone, Verizon argued that neither § 512(c)(3)(A) or §512(h) was applicable. Brief for Verizon, *In re Verizon, supra* note 227.

232 Brief for Verizon at 3, 7, *In re Verizon, supra* note 227.

233 *Id.*

234 *Id.* at 3.

235 *Id.* Verizon argued:

Even if only users to the Kazaa peer-to-peer file-sharing software are considered, RIAA's proposed construction of subsection 512(h) would allow RIAA to obtain subpoenas requiring service providers to identify any or all of the more than 100 million users who have downloaded Kazaa software, one million of whom are Verizon subscribers. *Id.* at 3-4.

Alternatively, Verizon proposed a solution: The RIAA should initiate a "John Doe" lawsuit against the individual, and then issue a discovery-based subpoena under the Federal Rules of Civil Procedure to force Verizon to identify the infringer. *Id.* at 5.

one of its subscribers.[236] Verizon claimed that the DMCA provisions clearly demonstrated that Congress contemplated the issue of material residing on its system. Verizon explained that if the material were stored on the person's individual computer, and not Verizon's network, it would have been impossible to disable access to it. Indeed, the only way Verizon could conceivably comply with the DMCA's provisions would be to cancel the user's subscription account, an overbroad sanction that would terminate the user's access to applications that had nothing to do with the alleged infringement.[237] Had Congress intended such a result, it responded, it would have drafted a clearer statute towards that intention.[238] "If all that is required is an assertion of suspected infringement and a 'freestanding' notice of infringement," Verizon predicted, "any copyright owner could issue such a subpoena."[239]

Given the fact that almost everyone can be a copyright owner in cyberspace, Verizon contended that the RIAA's construction would result in a world where anyone who wants to assert copyright infringements may do so and obtain the identity of another person through the DMCA's subpoena power.[240] The result would potentially expose the identity of anyone in cyberspace.[241] As one letter from a coalition of ISPs warned:

> "We are concerned that the RIAA's legal strategy – using a subpoena process in the Digital Millennium Copyright Act to obtain personal information about subscribers of basic Internet service – may have legal and technical consequences that exceed the stated purpose of this effort. Little is known or understood about this initiative, how individuals are being targeted, what is being done with the information, what is being done to facilitate compliance with subpoena requests and pay for the

---

236 Brief for RIAA at 14, *In re Verizon, supra* note 227.
237 Brief for Verizon at 5, *In re Verizon, supra* note 227.
238 *Id.* at 16.
239 *Id.* at 21.
240 *Id.* at 21-22.
241 *Id.* at 23.

> resulting costs, how long the information will be kept, and how it is being protected."[242]

In the end, the district court's decision accomplished just what Verizon feared most. It found that the subpoena power in the DMCA applied to *all* ISPs within the scope of the DMCA.[243] The court rejected any distinction between material stored on Verizon's servers and those stored on home computers. It concluded that the subpoena provisions applied both to those ISPs that just offered connections to the Internet, *as well as* those who stored information on their servers at their users' direction.[244] To justify its position, the court cited another provision of the DMCA that clearly defined "service providers" to include both types of ISPs—those that merely offered the transmission, routing, and provision of connections and as well as those that stored information on their servers.[245] The court stated that one had to evaluate the applicability of the subpoena in line with the statute as a whole, not by a piecemeal, constrictive interpretation.[246]

As a result of the initial ruling, copyright owners were able to obtain a subscriber's identifying information based on an asserted good-faith belief of copyright infringement, even when the offending material was not stored by the ISP. The district court's interpretation of the DMCA did not require any notice to

---

242 *See* Letter from Kevin S. McGuiness, Executive Director, NetCoalition.Com, to Mr. Cary Sherman, President, RIAA (Aug. 11, 2003) (on file with author).

243 *In re Verizon*, Inc., 240 F. Supp. at 26.

244 *Id.* at 32-33.

245 *See id.* at 31 (discussing the textual definition of "service provider").

246 The court explained:

> [The DMCA subpoena provision] is written without limitation or restriction as to its application. It is entitled "Subpoena to identify infringer" – not "Subpoena to identify infringer storing copyrighted material on a service provider's network." . . . If Congress intended to restrict or limit the subsection (h) subpoena authority based on where the infringing material resides, one would expect to see that limitation spelled out in subsection (h). And if Congress intended to limit subsection (h) subpoenas strictly to service providers under subsection (c), it certainly could have made such a limitation explicit.

Id. at 33.

be given to the subscriber in the event of a subpoena. Nor did the DMCA subpoena provision, in and of itself, offer any mechanism for the subscriber to assert any substantive rights on his or her behalf. Likewise, there were no provisions for damages should the subpoena result in the improper revelation of a person's identity; and finally, and perhaps most important, little judicial oversight existed to ensure that only meritorious disclosures of the subscriber's identity took place.[247]

In the end, the *Verizon* case went to the D.C. Circuit on appeal and was reversed, but only after nearly four hundred individuals had already been sued by the RIAA, their identities publicly exposed to the media.[248] The appeals court resoundingly rejected the district court's construction, concluding that both the terms of Section 512(h) and the overall structure of Section 512 direct that a subpoena may only be issued to an ISP that is actually storing the infringing material on its servers.[249] Given that Verizon was not storing the information on its own servers, the RIAA could not identify the relevant "material to be removed or access to which is to be disabled" under the terms of the DMCA.[250] The court explained:

---

247 *See* Brief for Appellant at 30-31, Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) (Nos. 03-7015, 03-7053) (consolidated appeals). Since the district court's interpretation provided for little judicial oversight (indeed, the district court's oversight over a subpoena is largely ministerial, rather than substantive), a number of unfortunate disclosures could happen. One example was offered by Parry Aftab, Executive Director of WiredSafety.org, an organization that works towards greater online security. He suggested that as a result of the DMCA subpoena provision, stalkers, sexual predators, and perpetrators of online fraud will be able to pierce the anonymity of individuals by finding their IP addresses, asserting a belief of copyright infringement, and obtaining a DMCA subpoena for their name and address. Aftab offers the sobering example of a violent child rapist who used the Internet to find a map and layout of a boys' school dormitory, predicting that the DMCA subpoena provision radically raises the risk of in-person confrontations between predators and potential victims. Declaration of Parry Aftab at 2, Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, No. 03-MS-0440 (D.D.C. 2003).

248 *See* Kristen Philipkoski, *Battle Not over for File Sharers*, WIRED NEWS, Dec. 23, 2003, *at* http://www.wired.com/news/digiwood/0,1412,61714,00.html.

249 Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1231 (D.C. Cir. 2003).

250 *Id.* at 1234-35 (quoting DMCA, 17 U.S.C. § 512(c)(3)(A)(iii) (2000)).

> "No matter what information the copyright owner may provide, the ISP can neither 'remove' nor 'disable access to' the infringing material because that material is not stored on the ISP's servers. Verizon can not remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscribers' computers."[251]

The court explained that the language of the DMCA also clearly distinguished between actually terminating a subscriber's account and removing or disabling access by *others to the infringing material* resident on the subscriber's computer.[252] Moreover, the court found that the notice-and-takedown section squarely applied to situations where the ISP hosted, cached, or stored infringing material; it did not apply to situations where the ISP is simply routing infringing material to or from a personal computer (as in the peer-to-peer context).[253]

Thankfully, as a result of the *Verizon* ruling on appeal, the RIAA and others are now required to file a lawsuit against the individual pursuant to Rule 27 of the Federal Rules of Civil Procedure, and then to institute normal discovery-based procedures in order to determine the identity of a purported infringer.[254] Because a copyright owner is now required to file a lawsuit against the purported infringer, a judge will have substantive discretion over whether to grant the subpoena.[255]

---

251 *Id.* at 1235.

252 *Id.* Given that these two different remedies were clearly specified by the terms of the DMCA, the court found that Congress must have intended to distinguish the two. *Id.*; *see* DMCA, 17 U.S.C. § 512(j)(1)(A)(i) (2000) (authorizing injunction restraining ISP "from providing access to infringing material"); *id.* § 512(j)(1)(A)(ii) (authorizing injunction restraining ISP "from providing access to a subscriber or account holder . . . who is engaging in infringing activity . . . by terminating the accounts of the subscriber or account holder").

253 *See Verizon*, 351 F.3d at 1237.

254 In contrast to Section 512(h) of the DMCA, which does not expressly require the filing of a complaint, Rule 27 requires the filing of a petition that demonstrates that "the petitioner expects to be a party to an action cognizable in a court of the United States but is presently unable to bring it or cause it to be brought." FED. R. CIV. P. 27(a)(1); *see infra* Part IV.

255 *See* Philipkoski, *supra* note 190. It bears noting that a Canadian court, when faced with the identical question, reached an even more protective conclusion. In the case of BMG Canada v. Doe, No. T-292-04

Yet, despite the outcome of *Verizon*, and the Supreme Court's eventual refusal to grant certiorari, the relationship between copyright and privacy continues to be a muddled, and largely contentious, collision of principles. For example, as *Verizon* shows, the DMCA and *Napster* each failed to articulate a clearly defined standard for proper *notice* of a user's infringement, an omission that has led to substantial confusion regarding the required substance of an accusation.[256] Is an ISP required to wait for a court order to terminate access to an individual when notified by a copyright owner that she has traded files on Napster or Kazaa, assuming that she is engaging in direct infringement, to avoid liability as a contributory infringer? Or, should an ISP immediately terminate a user's subscription if it receives notice of infringement? If so, what constitutes proper notice?[257] In a very recent case, *MPAA v.*

(Can. Mar. 31, 2004), in which a variety of Canadian record labels sought disclosure of the identities of 29 subscribers who allegedly made copyrighted files available to others, the Court applied a rather rigorous test, which required it to explore whether privacy concerns trumped the public interest in disclosure. In the end, the court concluded that downloading a song for personal use fell within the private copying exception in Canada's Copyright Act, and that, significantly, uploading copyrighted files did not constitute infringement because merely placing a file in a shared directory did not actually authorize infringement. Part of this conclusion is attributable to the court's conclusion in Muzak Corp. v. Composers, Authors, and Publishers Assn. of Canada, 2 S.C.R. 182 (1953) (observing that one does not 'authorize' infringement by authorizing the mere use of equipment that could be used to infringe). In the end, the court observed that it did not find "any real difference between a library that places a personal copy on a shared directory linked to a P2P service," and absolved liability entirely.

256 The *Verizon* court observed:

> Nothing in the Act itself says how we should determine whether a notification "includes substantially" all the required information . . . . Clearly, however, the defect in the RIAA's notification is not a mere technical error; nor could it be thought "insubstantial" even under a more forgiving standard. The RIAA's notification identifies absolutely no material Verizon could remove or access to which it could disable, which indicates to us that § 512(c)(3)(A) concerns means of infringement other than P2P file sharing.

Id. at 1236.

257 Moreover, although the DMCA does provide some guidance for proper notice requirements, they are actually much more difficult to ascertain than they seem. For example, in order to provide "effective notice," the DMCA requires a written communication that includes a number of elements, such as: identification of the copyrighted work or works claimed to have been infringed (or a list of such works at the site); information "reasonably sufficient" to permit the service provider to locate the material,

Rossi, the Ninth Circuit held that the governing standard under the DMCA required a subjective, not objective, determination of infringement.[258] In that case, which involved a notice-and-takedown situation, the MPAA failed to perform the necessary

---

as well as the complaining party; and, most significantly, a "statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law." 17 U.S.C. § 512(c)(3)(A)(iv)-(v) (2000). The *Napster* court failed to further clarify these provisions, referring only to the need for copyright owners to refer to "specific infringing files." A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001). Since *Napster*, three cases have noted substantial confusion regarding this point. *See* ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001); Arista Records, Inc. v. Mp3Board, Inc., No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002); Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

258 See MPAA v. Rossi, 2004 WL 2725717 at 1 (9th Cir. Dec. 1, 2004). In that case, a person advertised, on a website called internetmovies.com, the following contents: "Join to download full length movies online now! new movies every month!"; and "NOW DOWNLOADABLE." All of the links were non-operable, and no movies could actually be downloaded from the site. *Id.* at *3. Under the DMCA, when a copyright owner suspects his copyright is being infringed, he or she must follow the notice and takedown provisions set forth in § 512(c)(3) of the DMCA, which provide (in part):

> (A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:
>
> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
>
> (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
>
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
>
> (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted. (v) A statement that the complaining party *has a good faith belief* that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

17 U.S.C. § 512(c) (emphasis added).

diligence to confirm that its allegations of infringement were false.[259] In that case, the Ninth Circuit patently refused to enact a standard that required a "reasonable investigation into the allegedly offending website,"[260] and instead ruled that Congress intended that the DMCA "protect potential violators from subjectively improper actions by copyright owners."[261] In other words, a copyright owner's subjective belief that infringement was occurring was enough to trigger the notice-and-takedown process. No further investigation or confirmation is required; a good-faith allegation is sufficient under *Rossi*'s lenient standard.

In the end, ISPs face a classic difficulty in this context: whether they should side with their customers, requiring a court-ordered injunction to terminate a person's subscription under the rubric of protecting privacy; or whether they should remain ever-vigilant against piracy and terminate an account holder's subscription based on mere subjective, good-faith notice from the copyright owner. Largely due to this conflict, some ISPs might refrain from engaging in active content detection of their users' accounts, choosing instead to wait until they receive notice of infringement from law enforcement officials. Others, of course, might prudently relent at the first accusation of infringement, handing over their subscribers' identities and terminating their access at the first possible opportunity.[262] And still others, as I shall describe below, might institute proactive technical measures to monitor their subscribers' activities and prevent them from undertaking activities that might raise the risk of copyright infringement (whether or not it actually takes place). The more privatized the enforcement, the more disparate (and uncertain) the outcome.

---

259 *Id.* at * 2-3.

260 *Id.* at *2.

261 *Id.* at *3.

262 For a helpful explication from an ISP point of view, see Sjoera Nas, *The Daily Practices of an ISP in Dealing with Complaints About Illegal Content, Presentation in Brussels*, Nov. 12, 2002, *available at* http://www.xs4all.nl/overxs4all/auteursrecht/lezing.html (transcript of presentation by Sjoera Nas, Public Affairs Officer of XS4ALL Internet Rightswatch Conference, stating that "[p]roviders are systematically torn in splits between freedom of expression and requests to take down offensive, damaging or illegal content").

B. SPECTERS OF PIRACY SURVEILLANCE

In August 2001, the Ninth Circuit, in a debate of unprecedented visibility, refused to install certain software that would enable monitoring of their computers to detect the downloading of music, streaming video, and pornography.[263] The software was a filtering device ostensibly designed to prevent overloading the network system—but the judges believed that the alleged purpose behind its installation was broader. They feared that third parties would use such "content-detection" monitoring policies to identify individuals who engaged in file sharing or other potentially nefarious activities at work. A firestorm of controversy ensued. The judges ultimately defied the administrative order, disabled the software, and issued a host of statements publicly criticizing the administrative decision.[264] As Judge Alex Kozinski put it:

> "At the heart of the policy is a warning – very much like that given to federal prisoners – that every employee must surrender privacy as a condition of using common office equipment. Like prisoners, judicial employees must acknowledge that, by using this equipment, their 'consent to monitoring and recording is implied with or without cause.' . . .
>
> The proposed policy tells our 30,000 dedicated employees that we trust them so little that we must monitor all their communications just to make sure they are not wasting their work day cruising the Internet."[265]

Even though the larger policymaking body of the federal court system, the Judicial Conference, disagreed with the Ninth Circuit, and chose to continue using the monitoring software, its decision angered some federal workers, highlighting the tradeoffs that many universities and employers have made in

---

263 *See* Neil A. Lewis, *Rebels in Black Robes Recoil at Surveillance of Computers*, N.Y. TIMES, Aug. 8, 2001, at A1.

264 *Id.*

265 Alex Kozinski, *Privacy on Trial*, WALL ST. J., Sept. 4, 2001, at A22.

order to prevent being saddled with a lawsuit for contributory liability.[266]

As this example demonstrates, the problem of piracy has led some private entities to respond even more forcefully than necessary, seeking to destroy not only the peer-to-peer networks that have sprouted across the Internet, but the very boundaries of privacy, anonymity, and autonomy in cyberspace.[267] Even despite the outcome of *Verizon*, fear of suits for contributory infringement has led to regimes of institutional monitoring from ISPs, colleges, and private entities.[268] Some schools have utilized monitoring regimes that bar students from sharing certain types of files; others undertake less invasive bandwidth monitoring practices; and still others continue to closely monitor students' and employees' activity out of fear of suits for contributory liability.[269]

---

266 *See Judges Bar Use of Court Computers for Pornography, Large Personal Files*, 70 U.S. L. WK. 2183 (2001) (reporting that that the administrative court banned Gnutella, Napster, Glacier, and Quake from court computers claiming that it had found no legitimate court use).

267 Even though the original Napster filed for bankruptcy after a long standstill, it is now regarded as a legitimate service – notwithstanding the host of replacements, each more decentralized than the previous one, which have risen up to take its place. Kazaa, for example, at one point, claimed sixty million users around the world and twenty-two million in the United States, enabling far more illegal downloading than Napster ever did. Thankfully, however, many colleges are turning to license-based services to avoid some of the legal costs from unauthorized p2p use. Todd Woody, *The Race to Kill Kazaa*, WIRED, Feb. 2003, *available at* http://www.wired.com/wired/archive/11.02/kazaa_pr.html ("In the first six months of 2002, CD sales fell 11 percent – on top of a 3 percent decline the year before.") Charles C. Mann, *The Year the Music Dies*, WIRED, *available at* http://www.wired.com/wired/archive/11.02/dirge.html (Feb. 2003). At the same time, sales of blank CDs jumped forty percent last year. *Id.*

268 A related problem also involves protection of student records. Under the Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g(b)(2) (2000), educational institutions cannot disclose personally identifiable information about a student from an "education record" except where a subpoena has been lawfully issued, and as long as the educational institution notifies the student in advance of complying with the subpoena. *See* Mass. Inst. of Tech. v. Recording Indus. Ass'n of Am., Misc. Act. No. 1:03-MC-10209-JLT (D. Mass. Aug. 7, 2003).

269 *See supra* note 4 and accompanying text; Nick Reed, *Computers Seized in File-Sharing Raid*, THE LANTERN OF OHIO ST. U., May 27, 2003, *available at* http://www.thelantern.com/news/2003/05/07; and Scott Carlson, *Tending the Net: Computer-Discipline Offices Offer a Human Touch When Investigating Student Complaints*, CHRON. OF HIGHER EDUC., June 7, 2002

The result is a protracted, and largely invisible, web of surveillance that tracks many of the same instrumentalities involved in current privacy litigation.[270] This article defines piracy surveillance to encompass particular types of monitoring that: (1) are performed by private, non-government entities; (2) encompass extrajudicial determinations of copyright infringement; and (3) are extralegal in nature; that is, surveillance that takes place entirely outside of ongoing litigation.

As this section will illustrate, the advent of piracy surveillance alters the definition and application of intellectual property rights. As Part I suggested, property concepts have traditionally served to shield—and to protect—the privacy interests of individual owners as well as third parties. In contrast, piracy surveillance radically transforms—and extends—the reach of intellectual property rights by enabling copyright owners to detect, deter, and prevent acts of potential infringement by third parties. The RIAA defends its efforts, maintaining that it:

> "is acting no differently than anyone in this country whose property rights have been violated and who is faced with a decision whether to press a legal claim: we are making a judgment as to whether pursuing a particular lawsuit is appropriate given the circumstances."[271]

Yet there is a crucial difference between this analogy between property rights in real space and intellectual property rights in cyberspace: freedom of expression and anonymity. As I have argued, many individuals harbor expectations of privacy in

---

(discussing the institution of NEThics Campus police).

270 For example, some forms of piracy surveillance use "smart agents" or "bots," which have been the subject of litigation in other contexts. *See infra* Part II-A; eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1060-61 (N.D. Cal. 2000); Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1354 n.4 (Cal. 2003); Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. DAYTON L. REV. 179, 187 (2001); Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 570-71 (2001); Laura Quilter, Note, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421, 423-24 (2002).

271 *Privacy & Piracy, Hearing Before the Senate Permanent Subcomm. on Investigations*, *supra* note 193, at 8 (testimony of Mitch Bainwol, Chairman and CEO, RIAA).

cyberspace, believing that their personal identifying information is only shared with third parties with their consent or pursuant to a valid subpoena. Piracy surveillance eviscerates this expectation by creating an institutional monitor to detect acquisition and use of copyrighted materials. Because these methods of surveillance often involve extrajudicial determinations of infringement, they necessarily involve speech-based judgments, often enabling a copyright owner to determine for himself or herself whether or not individuals are engaging in fair use. The malleable standard for subjective "good faith" infringement allows creative activities that might fall within a "grey" area of fair use—sampling, space shifting, other transformative works, etc.—to become, effectively, automatically subject to the permission of the copyright owner for their circulation and publication.[272]

Moreover, under the DMCA, there are no regulations governing the detection of alleged acts of infringement through file sharing, or through any other medium. The RIAA—or any other copyright owner—is not required to explain, justify, or even share its detection methods with the public. Nor does the DMCA require any performance of "due diligence" to ensure that infringement is occurring; the Act provides little substantive definition of "good faith infringement." Thus, piracy surveillance methods, for all their asserted efficacy, also herald the growing encroachment of a panoptic architecture over constitutionally protected values such as speech, privacy, and due process. Finally, proponents of piracy surveillance also subscribe to a logic of vigilantism: as they are designed and implemented by private, non-state entities, they invite equally intrusive counter-surveillance responses from ordinary citizens.

1. MONITORING

Like many techniques involving consumer surveillance, copyright owners in cyberspace rely heavily on the use of "smart agents." Here, they are used to identify acts of perceived infringement, and, in light of the outcome of *Verizon*, copyright

---

272 Here, the user may be able to restore the material through the "put back" procedure set forth in 512(g)(2), but this requires the service provider to wait a certain number of days after receiving a counter-notification, and still penalizes speech that may fall within these "grey areas."

owners can now quickly identify and contact a perceived infringer. In cyberspace, the RIAA maintains a team of Internet specialists and an automated twenty-four-hour Web crawler, a "bot" that continually crawls through the Internet to identify allegedly infringing activities.[273] A "bot" is a shortened term of "robot" and essentially refers to a program that is capable of crawling from one server to another, compiling lists of Web addresses that possess certain characteristics (in this case, those that offer unauthorized titles of copyrighted material).[274] One Web crawler, run by Copyright.net, crawls through a person's hard drive looking for uploaded copies of particular songs in peer-to-peer networks like Gnutella, Aimster, and Napster.[275] It singles out individual hard drives containing an uploaded copyrighted song, matches the computer's Internet address to its ISP, and serves notice to the ISP, requesting that the ISP terminate the person's online connection until she removes the offensive copy.[276] The RIAA's software robot, dubbed Copyright Agent, has served more than one million copyright violation notices to ISPs on behalf of seven hundred and fifty song writers and performers.[277]

Many of the RIAA's tactics remain shrouded in secrecy, prompting one Congressman to hold hearings on the scope and method of the recording industry's tactics.[278] In one recent case,

---

273 *See* RIAA, *What the RIAA Is Doing About Piracy*, *at* http://www.riaa.com/issues/piracy/riaa.asp (last visited Dec. 05, 2004).

274 *See What's a Bot*, *at* http://www.botspot.com/common/whats_bot.html (last visited Dec. 05, 2004) (describing "bots" as a form of artificial intelligence that digs through data).

275 *See* Dawn C. Chmielewski, *Software Foils Bootleg Tunes*, SAN JOSE MERCURY NEWS, Feb. 28, 2001, at 1C (describing a new technology that detects bootlegged songs on personal hard drives). As one report stated, "[the] Ranger [bot] is scouring the globe—Web sites, chat rooms, newsgroups and peer-to-peer file-sharing sites—spanning 60 countries, searching in English, Chinese and Korean. . . . Ranger is 24-7. Ranger is relentless." Frank Ahrens, *"Ranger" vs. the Movie Pirates: Software Is Studios' Latest Weapon in a Growing Battle*, WASH. POST, June 19, 2002, at H1.

276 Ahrens, *supra* note 275, at H1.

277 *Id. See also* Robert G. Gibbons & Lisa M. Ferri, *The Legal War Against Cyberspace Piracy*, N.Y. L.J., Aug. 5, 1999, at 1 (observing that the American Society of Composers, Authors and Publishers uses automated software to locate sites containing the music of any of its members). Another program, known as MediaForce, uses similar tactics internationally as well. *See* Iain Ferguson, *MediaForce Still Trying to Block Aust Piracy*, *at* http://www.zdnet.com.au/news/security/0,2000061744,20271820,00.htm (Feb. 5, 2003).

278 *See* Associated Press, *RIAA Tactics Under Scrutiny*, WIRED

in which a Brooklyn woman was accused of offering more than nine hundred songs on Kazaa, the RIAA used a library of digital fingerprints, called "hashes," as well as metadata tags, which are often relied upon by forensic investigators in computer hacking cases, to rebut her claim that the songs shared on her computer were from compact discs that she had legally purchased. Using these tools, the RIAA traced several song files on the woman's computer to files she had downloaded through the Napster service.[279] The fingerprints were used to dispute her claims of legitimate space shifting, and to show that the source for file sharing did not involve a legitimate purchase of CDs.[280]

NEWS, Sept. 16, 2003, *at* http://www.wired.com/news/digiwood/0,1412,60460,00.html. Senator Norm Coleman held a series of hearings on September 30, 2003, entitled *Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technologies on the Entertainment Industry*. At the hearing, a music representative explained:

> To gather evidence against individual infringers, RIAA typically uses software that searches the public directories available to any user of a peer-to-peer network. These directories list all the files that other users of the network are currently offering to distribute. By logging onto these open networks and searching for recordings owned by RIAA's members just like any other user, the software finds users who are offering to distribute copyrighted music files. When the software finds such a user, it downloads a sample of the infringing files, along with the date and time it accessed the files, and locates the user's Internet Protocol ("IP") address. Additional information that is publicly available allows RIAA to then identify the infringer's Internet Service Provider.

Privacy & Piracy, Hearing Before the Senate Permanent Subcomm. on Investigations, *supra* note 193, at 8 (testimony of Mitch Bainwol, Chairman and CEO, RIAA).

279 *See* Ted Bridis, *RIAA Discloses Some Methods of Tracking*, AP ONLINE, Aug. 28, 2003, *available at* 2003 WL 62378104.

280 *See id.* According to the RIAA, some of the files offered for download by one particular defendant (who operated under the pseudonym "nycfashiongirl") contained media information that also suggested that they were "ripped" by someone other than the defendant. *See* Opposition of Recording Industry Association of America to Motion of Intervenor to Stay Motion and Enforce Subpoena at 11-13, *In re* Verizon Internet Servs., Inc., 217 F.R.D. 239 (D.D.C. 2003) (Misc. Act. No. 03-MC-804-HHK/JMF), *available at* http://www.eff.org/IP/P2P/Jane_Doe_v_RIAA/RIAA-opp.pdf. For other files, the RIAA matched hashes from the defendant's sound files to those contained in a database of music downloaded from Napster in 2000. *Id.* at 13.

Even before a judicial case is filed, these strategies of private enforcement utilize a cleverly decentralized system, wherein the copyright owner is burdened with the cost of detecting infringement, and the ISP is burdened with the need to balance threats of contributory infringement with the importance of protecting the consumer from illegitimate threats and undue disclosure. Under the DMCA's expedited subpoena provisions, the RIAA sends out notices to ISPs to force them to identify the site operator, or end-user.[281] Once it identifies the site operator, the RIAA may send that person a warning email, may send messages to the ISP, or may even initiate litigation.[282] At some schools, automated Web crawlers detect where downloading takes place.[283] When it is located, the RIAA sends letters asking the school to take action against the alleged infringer.[284] To reinstate her account, the infringer must remove the offending title and replace it with an encrypted copy of the song that allows the rights holder to restrict how it will be used.[285] Some schools engage in copyright infringement detection even without assistance from the RIAA: the University of Florida uses Icarus, which scans the network for file-sharing activity. If caught once, students are warned and

---

281 *See* RIAA, *What the RIAA Is Doing About Piracy*, *supra* note 273.

282 *Id.*

283 At universities, the RIAA has instituted a "Soundbyting campaign," which it claims to have resulted in a fifty-five percent drop in the number of music sites on university servers offering illegal downloads. According to the Electronic Frontier Foundation, the University of Wyoming used a program that "fingerprinted" all network traffic in order to detect unauthorized copying. The program also copied everything sent over the network in order to detect the exchange of sound files—emails, grade reports, documents, and the like, including the collection of unauthorized information. *See* Elec. Frontier Found., *Universities Should Resist Network Monitoring Demands*, *at* http://www.eff.org/IP/P2P/university-monitoring.pdf (last visited Dec. 04, 2004).

284 Liza Porteus, *Beware of the Music Downloading Spies*, U-WIRE, Oct. 26, 2000, *at* http://www.uwire.com. Monitoring goes beyond just looking at the name of a file. *Id.* Other companies have devised ways to identify music files based on their actual sound. Jon Healey, *New Technologies Target Swapping of Bootlegged Files*, L.A. TIMES, Feb. 20, 2001, at C1. Still other companies, such as Cyveillance, Ewatch, and Cybercheck, assist customers in protecting their brands by using customized software to track trademark infringement, copyright infringement, counterfeiting, and the bootlegging of music and movies. *See* Gibbons & Ferri, *supra* note 273. These companies may also search for any association of brand names with pornography, and search for any damaging rumors in chat rooms. *Id.*

285 *See* Gibbons & Ferri, *supra* note 277.

kicked off for 30 minutes, the second time, they are kicked off for 5 days; the program also eliminates file sharing, prevents online gaming, and sending files over instant messenger. [286] Once it sees heavy bandwidth usage and the data stream looks like music or a file being shared, it stops the student's connection.

Here, monitoring techniques carry an almost perfect explication of the panoptic metaphor regarding behavioral control. In one example, Carnegie Mellon decided to check the public folders of 250 student computers connected to the university network, and found hundreds of MP3's for distribution from 71 machines; students lost their in-room connections for the rest of the semester.[287] Panoptic architecture offers a rather inexpensive means of producing discipline—no chains or locks are needed; all that is required is that the people perceive the risk of surveillance.[288] The risk that the copyright owner is always watching, always searching, always monitoring, facilitates compliance.[289] From the copyright owner's perspective, peer-to-peer surveillance allows for near-perfect automated detection, and creates a risk of disclosure that deters would-be infringers from sharing files. Under this technology, it matters little whether or not the RIAA is actually investigating or monitoring file transfer: The goal of such strategies is to create a perceptible *risk* of detection. This risk of detection and disclosure, in turn, is precisely what facilitates compliance. Consider, for example, the reports suggesting file sharing dropped by nearly half since the filing of the initial *Verizon* lawsuit.[290] By utilizing technologies that facilitate constant monitoring of file-sharing activity, the music

---

286 Matt Buchanan, *Don't Fear MediaDefender*, WASH. SQUARE NEWS, Oct. 9, 2003 *at* http://www.nyunews.com/opinion/columnists/5884.html.

287 Kelly McCollum, *How Forcefully Should Universities Enforce Copyright Law on Audio Files?*, CHRON. OF HIGHER EDUC., Nov. 19, 1999.

288 FOUCAULT, *supra* note 92, at 202.

289 GANDY, *supra* note 91, at 10.

290 *See* Jefferson Graham, *Lawsuits Help Cut Song-Swapping in USA by Half*, USA TODAY, Jan. 5, 2004, at 1B (reporting on a study finding that unauthorized online song swapping has been cut in half since record companies started suing swappers in the fall of 2003); Associated Press, *Lawsuits Slow Music Downloads*, WIRED NEWS, Jan 5, 2004, *at* http://www.wired.com/ news/technology/0,1282,61790,00.html.

industry has managed to deter infringement and instill fears of identity disclosure among file sharers.[291]

Before the *Verizon* case was filed, peer-to-peer norms continued to support the sharing of files, ostensibly because file sharers perceived that they faced little risk of prosecution or disclosure of their identities. Yet peer-to-peer technology has enabled intellectual property owners to model their efforts after methods of consumer surveillance.[292] After *Verizon*, peer-to-peer networks are no longer anonymous, amorphous communities characterized by unique social norms and noncompliance with copyright laws.[293] Rather, the use of smart agents, coupled with the risk of identity disclosure, has pierced the protection of anonymity that many file sharers expect.

Techniques of piracy surveillance can be used, either directly or indirectly through an intermediary, to detect infringement or to penalize perceived infringers. Most significantly, each of these techniques is private in character, in the sense that each of these methods is administered and utilized by a non-government entity, and is governed by few restrictions. Since surveillance activities are usually extrajudicial in character—that is, no judicial determination of infringement has been made—little recourse exists to defend oneself against an accusation.

There are significant drawbacks to such surveillance. Even though the RIAA claims to engage in due diligence to confirm evidence of infringement, the technology can easily

---

291 Graham, *supra* note 293. Aside from demonstrating panoptic strategies of surveillance, these techniques also rely on strategies of discretionary nonenforcement. Recently, the RIAA announced that it had decided to pursue investigations against individuals who offer "substantial" amounts of music online to others over peer-to-peer services. *See Privacy & Piracy, Hearing Before the Senate Permanent Subcomm. on Investigations*, *supra* note 193, at 7-8 (testimony of Mitch Bainwol, Chairman and CEO, RIAA). Yet it did not to elaborate on what it meant by "substantial," presumably hoping to deter everyone from sharing files—from the person who offers thousands of song titles to the college student offering only a few songs. *See id.*

292 *See generally Privacy & Piracy, Hearing Before the Senate Permanent Subcomm. on Investigations*, *supra* note 193 (testimony of Mitch Bainwol, Chairman and CEO, RIAA).

293 For excellent reading on this topic, see Strahilevitz, *supra* note 167; Wu, *supra* note 170.

mistake legitimate files for copyrighted works.[294] This can impose a great burden on an author's freedom of speech that extends to anyone targeted by monitoring technologies. For example, Warner Brothers, owner of the copyright to *Harry Potter and the Sorcerer's Stone*, sent a notice to ISP UUNet asking it to disable a user's Internet access because of a single (allegedly infringing) file titled *harry potter book report.rtf*.[295] More recently, the Business Software Alliance incorrectly targeted a company that used software called *OpenOffice*, notifying the company that it was making unauthorized copies of Microsoft Office available, simply because its "bot" detected the use of the word "office" in the program.[296]

In another, more public incident, the RIAA sent out more than two dozen letters that incorrectly targeted institutions suspected of posting copyrighted music on their servers.[297] In one example, the RIAA's Web crawlers had zeroed in on an MP3 copy of a song by a group of astronomers posted by an astrophysics professor named Peter Usher, which the RIAA confused with popular artist Usher Raymond.[298] In another example, the RIAA apologized to a national broadband provider for sending a cease-and-desist letter that alleged illegal activity

---

294 *See generally Privacy & Piracy, Hearing Before the Senate Permanent Subcomm. on Investigations*, *supra* note 193, at 8 (testimony of Mitch Bainwol, Chairman and CEO, RIAA) (observing that an RIAA employee "manually reviews and verifies the information"); *see also Piracy of Intellectual Property on Peer-to-Peer Networks: Hearing Before the House Subcomm. on Courts, the Internet, and Intellectual Property of the Comm. on the Judiciary*, 107th Cong. 23-33 (2002) [hereinafter *Piracy of Intellectual Property, Hearing Before the House Subcomm. on Courts*] (statement of Gigi B. Sohn, President, Public Knowledge).

295 *Piracy of Intellectual Property, Hearing Before the House Subcomm. on Courts*, *supra* note 294, at 24 (statement of Gigi B. Sohn, President, Public Knowledge).

296 *See* Declan McCullagh, *BSA (Microsoft) Screws Up, Targets OpenOffice Distribution*, POLITECH, *at* http://www.politechbot.com/p-04511.html (Feb. 28, 2003).

297 Gil Kaufman, *RIAA Admits Piracy Goof*, ROLLING STONE.COM, *at* http://www.rollingstone.com/news/newsarticle.asp?nid=18053 (May 14, 2003).

298 *Id.* The song was sung by an astronomy group called The Chromatics, about a gamma ray satellite designed by Penn State; the RIAA sent the take-down notice to the university, which then threatened to take down the entire site within 48 hours. Unfortunately, the incident took place during the final examination period. *See Complaint from Recording Industry Almost Closes Down a Penn State Astronomy Server*, CHRON. OF HIGHER EDUC., May 23, 2003.

on a subscriber's File Transfer Protocol site.[299] The contents of the letter read that the site illegally "offers approximately 0 sound files for download."[300] In another instance, Wal-Mart sent a Section 512(h) notice to a comparison-shopping Web site that allowed consumers to post prices of items sold in its stores, claiming incorrectly that its prices were copyrighted when they were in fact uncopyrightable facts.[301] Other "bots" have generated DMCA notices for films or court documents that are part of the public domain.[302]

These problems have been exacerbated, rather than mitigated, by the recent filing of lawsuits against individuals engaged in copyright infringement. In one situation, the RIAA obtained the identity of an individual, and proceeded to file a copyright infringement action against a 66-year-old grandmother who had never downloaded any songs and did not even own a computer equipped with file-sharing software.[303] In another case, the RIAA used a DMCA subpoena to sue an individual whose IP address allegedly did not match the one the RIAA investigated for downloading songs.[304]

Moreover, many individuals poorly assess the risk of online surveillance and continue to engage in online activities without realizing the risk of exposure.[305] Many people have no

---

299 Declan McCullagh, *RIAA Apologizes for Erroneous Letters*, CNET NEWS.COM, May 13, 2003, *at* http://news.com.com/2100-1025-1001319.html.

300 *Id.* The letter continued, "Many of these files contain recordings owned by our member companies, including songs by such artists as Creed." *Id.*

301 *See* Brief of Amici Curiae Alliance for Public Technology, et al., in Support of Appellant Verizon Internet Services and Urging Reversal at 12, Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) (Nos. 03-7015, 03-7053) (consolidated appeals); Declan McCullagh, *Wal-Mart Backs Away from DMCA Claim*, CNET NEWS, *at* http://news.com.com/2100-1023-976296.html (Dec. 5, 2002).

302 *See* McCullagh, *supra* note 299. In one instance, the Internet Archive was sent a DMCA notice by a copyright owner who mistook films in the public domain for a copyrighted movie; *see also Universal Studios Stumbles on Internet Archive's Public Domain Films*, *at* http://www.chillingeffects.org/ notice.cgi?NoticeID=595 (last visited Dec. 6, 2004) (containing an erroneous DMCA notification of unauthorized use of Universal Motion Pictures).

303 *Id.*

304 Joseph Menn, *Group Contends Record Labels Have Wrong Guy*, L.A. TIMES, Oct. 14, 2003, at C2.

305 *See* Good & Krekelberg, *supra* note 89.

idea what they are sharing online, and with whom. In such circumstances, the law rarely steps in to validate consumer expectations of privacy or to educate citizens regarding the limits of their rights in cyberspace. To illustrate this point, consider this case. On July 2, 1999, a customer-support specialist for Road Runner, a high speed ISP, received a call from an anonymous male who told the specialist that he was at a friend's house, scanning other computers, and had viewed child pornography on a computer that he believed Road Runner serviced.[306] The computer's owner had activated its printer and file sharing mechanism, which allowed others to view the images stored on its hard drive.[307] The caller gave the specialist the computer's IP address, the directory, and the file names in which the images were located.[308] Shortly afterward, the specialist located the computer with the corresponding IP address and viewed two images of a sexual nature involving children.[309]

After escalation in the management structure and consultation with its corporate attorney, Road Runner then contacted the FBI and recommended that it obtain a court order to procure the subscriber's information.[310] The United States Attorney's Office agreed and located the subscriber's home address, telephone number, email address, and general account information.[311] A special agent then called the home and spoke with one of the email subscribers, Michael Kennedy, who stated that he always left his computer on and connected to the Internet.[312] When asked if he could share any "concerns" with Road Runner's service, Kennedy responded that he "thought the company should warn customers about the possibility of someone else trying to enter their computers through the Internet."[313] After the FBI obtained a search warrant and officials went to search the house, Kennedy admitted that he had downloaded onto his hard drive pictures of young boys

---

306 United States v. Kennedy, 81 F. Supp. 2d 1103, 1106 (D. Kan. 2000).

307 *Id.* at 1107 n.7.

308 *Id.* at 1106.

309 *Id.*

310 *Id.* at 1107.

311 *Id.*

312 *Id.*

313 *Id.* at 1108.

engaging in sexual acts.[314] He claimed not to know the identity of the person from whom he had downloaded the images, and that he did not think that anyone would discover he had downloaded the pictures.[315] Shortly after a grand jury returned an indictment for his arrest, Kennedy turned himself in.[316]

Notably, the court resoundingly rejected every argument Kennedy raised in support of his expectation of privacy, suggesting that individuals who engage in file-sharing activities essentially have no right to privacy under the Fourth Amendment's right to protection against unreasonable searches and seizures. The court rejected Kennedy's assertions that Road Runner trampled on his Fourth Amendment rights when it divulged his subscriber information to the government because he had failed to demonstrate an "objectively reasonable legitimate expectation of privacy in his subscriber information," since he had activated his computer's file sharing mechanism.[317]

The *Kennedy* court analyzed the privacy issues Kennedy raised by turning to the test articulated in *Katz v. United States*, in which the Court established that a "search" takes place only when a government violates an individual's reasonable expectation of privacy.[318] "[W]hat a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection," the *Kennedy* court repeated, quoting from *Katz*.[319] In other words, because Kennedy had voluntarily "turned over" information to third parties, like the ISP, the court concluded that he had no legitimate expectation of privacy in any of his online activities:

---

314 *Id.*

315 *Id.*

316 *Id.*

317 *Id.* at 1110.

318 *Id.* Under *Katz v. United States*, 389 U.S. 347, 351-52 (1967), the test for a constitutionally "unreasonable search" is two-fold: first, it requires that a person exhibit a subjective expectation of privacy; and second, that the expectation of privacy be one that society also recognizes as reasonable. In analyzing the second question, the Court later opined that "'[the] test of legitimacy is not whether the individual chooses to conceal assertedly "private" activity,' but instead 'whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment.'" California v. Ciraolo, 476 U.S. 207, 212 (1986) (quoting Oliver v. United States, 466 U.S 170, 181-83 (1984)).

319 *Kennedy*, 81 F. Supp. 2d at 1110 (quoting *Katz*, 389 U.S. at 351).

> "When defendant entered into an agreement with Road Runner for Internet service, he knowingly revealed all information connected to the IP address 24.94.200.54. He cannot now claim to have a Fourth Amendment privacy interest in his subscriber information."[320]

The court's recitation of *Katz* highlights some of the most severe difficulties with protecting informational privacy in the information age. *Kennedy* demonstrates the discontinuity of expectations of privacy and anonymity; a person might share information under a subjective expectation of anonymity (supported, perhaps by the ISP's assurances of consumer privacy), even though a court might reach the opposite conclusion.[321]

In sum, under *Katz*, it appears unclear whether a person can legally possess a reasonable expectation of anonymity and engage in file sharing at the same time, even though, practically speaking, many individuals do so quite readily. The court suggested that Kennedy's use and activation of a file sharing mechanism essentially meant that files contained within his hard drive could be considered public—not only his numerical subscription information, but the actual content of his files as well.[322] Currently, the DMCA, as it is written, contains no protection for anonymous speakers in the face of accusations of infringement.[323] And, as the mistaken examples in the previous section demonstrate, the risk of exposure is not limited to clear-cut cases alone, but to anyone who may be caught within the panoptic Web of copyright enforcement. In sum, the *Kennedy* case, and others like it, highlights a troubling contradiction regarding perceptions of informational privacy online: individuals poorly assess the reality of transparency, leading them to expect anonymity, even when engaging in illicit

---

320 *Id.*

321 In some of the cases relied upon in the Fourth Amendment context, a person's identity is already known or ascertained through other means, and usually protected by additional regulations to support privacy. *See* Smith v. Maryland, 442 U.S. 735, 738, 741 n.5 (1979) (noting that the pen register did not disclosure the content of Smith's communications).

322 *Kennedy*, 81 F. Supp. 2d at 1110; *see also* United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at **4 (4th Cir. Aug. 3, 2000) (holding that there is no legitimate expectation of privacy in information which is voluntarily conveyed to a third party).

323 For elaboration of this point, see *infra* Part III.

activities that are open to private surveillance. As one author observes, a person's expectations of privacy in such circumstances may be wildly varied, suggesting that many do not understand the extent to which the technology itself collects information or monitors the online activities of an ISP's subscribers.[324] As we will see, *Kennedy*'s gutting of Fourth Amendment protections carries special weight when we turn to the question of criminal copyright infringement for peer-to-peer distribution of music and other copyrighted media. When private citizens act in a law-enforcement capacity, as the ISP or the anonymous caller did in *Kennedy*, they can further limit the scope of an individual's protections under the Fourth Amendment.[325]

2. MANAGEMENT

Digital rights management ("DRM") is another kind of piracy surveillance that harnesses similar trajectories of monitoring and record collection in the consumer surveillance context.[326] Unlike the technology explored in the previous section, some DRM techniques require an affirmative act by the consumer to inform the company of her identity prior to using a copyrighted product.[327] Thus, in this sense, some types of DRM

---

324 *See* Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 102 (2000).

325 The test for determining whether or not a person is acting as an agent of the government is whether the private party "in light of all the circumstances of the case, must be regarded as having acted as an 'instrument' or agent of the state [when the search or seizure occurred]." Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971). In the *Kennedy* case, for example, the defendant argued that the initial warrantless searching of his computer files violated his Fourth Amendment rights because government actors did them. United States v. Kennedy, 81 F. Supp. 2d at 1111-12 (D. Kan. 2000). The court soundly rejected this argument on the grounds that the government neither knew of, nor acquiesced in the intrusive conduct, and that Kennedy had made no showing that the government involvement was significant enough to change the conduct into government searches. *Id.*

326 For an excellent summary on the legal and policy issues on DRM, see *Symposium: The Law & Technology of Digital Rights Management*, 18 BERKELEY TECH. L.J. 487-771 (2003).

327 For a helpful, historical piece justifying digital controls, see Jane C. Ginsburg, *From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law*, 50 J. COPYRIGHT SOC'Y U.S.A. 113 (2003) (arguing that the right to control access to a work is

cannot function without some encroachment on a user's privacy: copyrighted products that contain DRM cannot operate without verification of the user's identity.[328] Other techniques can restrict a computer from "altering, sharing, copying, printing [or] saving" protected files.[329]

Some DRM strategies are designed to set and automatically enforce limits on user behavior' for example, some music delivery formats that prevent copying (even for space-shifting purposes) while others restrict the type of devices used for playback.[330] Today, DRM also encompasses encrypted media files, watermarks that identify their users, counters that keep track of each playback or viewing, and copycodes that control the duplication of files, thereby allowing a copyright owner to track whether or not a file is uploaded or digitally shared with others.[331] Content-scrambling system algorithms can also add a

---

an integral right of copyright law).

328 *See* Jeff Howe, *Licensed to Bill*, WIRED, Oct. 2001, at 140, 147, *available at* http://www.wired.com/wired/archive/9.10/drm.html?pg=1 (describing the technology behind DRM and its potential for revenue). In another case, Blizzard Entertainment, a games developer, admitted that in an attempt to deter software pirates, it collected the names and email addresses of gamers without their knowledge. *See Gamemaker Under Fire for Invasion of Player Privacy*, COMPUTERGRAM INT'L, *available at* http://www.findarticles.com/cf_0/m0CGN/ n3404/20578101/p1/article.jhtml (May 6, 2003).

329 *See* EPIC, *Digital Rights Management and Privacy*, *at* http://www.epic.org/privacy/drm (last visited Dec. 6, 2004). For more on DRM technologies, see Julie Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462 (1998); Pamela Samuelson, *DRM {and, or, vs.} the Law*, 46 COMM. ACM 4, at 41-45 (April 2003), *available at* http:// www.sims.berkeley.edu/~pam/ papers/acm_v46_p41.pdf. There is also a fair amount of literature on trusted computing as well, which implements security features in computer hardware. See Eben Moglen, *Free Software Matters: Untrustworthy Computing,* Aug. 11, 2002, *available at* http://emoglen.law.columbia.edu/ publications/lu-22.html; Richard Stallman, *Can You Trust Your Computer?* GNU Project, *at* http://www.gnu.org/philosophy/can-you-trust.html; Seth Schoen, *Trusted Computing: Promise and Risk*, *at* http://www.eff.org/infrastructure/ trusted_computing/2003/001_tc.php; Ryan Roemer, *Trusted Computing, Digital Rights Management and the Fight for Copyright Control on Your Computer*, 2003 UCLA J of L & TECH. 8 (2003); Lessig, Code at 127; Chad Woodford, Note, *Trusted Computing or Big Brother?* 75 U. COLO. L. REV. 253 (2004); Megan Gray, *The Legal Fallout from Digital Rights Management Technology*, 20 COMPUTER & INTERNET LAW 20 (2003).

330 *See* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 580 (2003).

331 Howe, *supra* note 328, at 142. The code, however, that

further, geographic restriction that ensures that DVDs only play in designated regions.[332] Still other technologies can report back on the activities of individual users, which can be used for a variety of purposes, including marketing.[333] Other programs can be designed to disable access to a work after detecting an unauthorized use, ensuring that constant monitoring takes place to ensure compliance with the terms and conditions of a license.[334]

It makes sense, both economically and practically, to ask a copyright owner to internalize the costs of enforcement through such management systems. Yet these systems often involve the ability to preclude fair use, one of the key limitations on a copyright holder's exclusive scope of rights.[335] As two commentators observe, "[u]nless DRM systems include a 'judge on a chip,' they will remain incapable of determining whether a

---

enables the anti-piracy software is widely believed to be installed in home and office hard drives, thereby opening the door to more anti-piracy measures. *See Privacy Advocates Slam Industry Plan for Hard Drives*, WALL ST. J. EUR., Jan. 18, 2001, *available at* 2001 WL 2840879. In 2001, television makers endorsed a new copy-protection scheme that installs certain technology in television sets to block the making of digital copies of television shows. *See* Jube Shiver, Jr., *Company Town TV Makers Take a Side on Anti-Piracy Technologies Media*, L.A. TIMES, May 16, 2001, at C5 (describing how television makers are backing a new copy-protection scheme). The technology, known as FireWire, uses a combination of user-authentication and encryption to determine whether digital content should be transmitted from one device and can limit the number of copies generated. *Id.*

332 *Cohen*, *supra* note 330, at 581.

333 *Id.*

334 *Id.* The Uniform Commercial Code validated self-help provisions in its Uniform Computer Information Transactions Act (UCITA), formerly known as U.C.C. 2B. The provisions, which covered contracts in "computer information," provided that upon material breach of a contract, the licensor can prevent a licensee from using the product and repossess the property; another provision permitted the use of other self-help remedies as long as they could be accomplished without a breach of the peace. Uniform Computer Information Transactions Act (UCITA), §§ 701, 815(b) (last revisions or amendments completed 2002), *available at* http://www.law.upenn.edu/bll/ulc/ucita/2002final.htm (last visited Dec. 6, 2004). *See also* Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L. J. 1089 (1998); Craig Dolly, *The Electronic Self-Help Provisions of UCITA: A Virtual Repo Man?*, 33 J. MARSHALL L. REV. 663 (2000); David Friedman, *In Defense of Private Orderings: Comments on Julie Cohen's "Copyright and the Jurisprudence of Self-Help,"* 13 BERKELEY TECH. L.J. 1151, 1154 (1998).

335 *See* Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998).

user is copying part of a work for purposes of piracy or parody."[336] Moreover, since many of these strategies also fail to protect consumer privacy, they also display a striking convergence of piracy and consumer surveillance. Consider the use of anti-piracy technologies that prevent users from converting, or "ripping," software tracks into an MP3 format from a CD. Such technology, called Digital Content Cloaking Technology, requires users who desire digital copies to provide personal information in order to track the customer's listening habits. In one suit over the use of such technology, labels attached to the product failed to disclose that the company tracked, stored, and disseminated personal identifying information of the consumer.[337]

Digital Rights Management, therefore, replicates a convergence between consumer and piracy surveillance that can be built into a variety of technologies, from copyrighted products to computer hardware. Like many other types of "trusted computing" efforts, it offers an extrajudicial mediator to decide the boundaries of acceptable use of copyrighted products, potentially eviscerating the vitality of fair use in the process.[338] Moreover, with DRM's brand of piracy surveillance, the law either fails to step in, or when it does, risks enabling a degree of self-help that is both invasive and replicates the panoptic structures I identified earlier. In theorizing this point, particularly the panoptic overlap between piracy and consumer surveillance, consider the following example. SONICblue makes ReplayTV digital video recorders ("DVRs") which enable

---

336 C.J. Alice Chen & Aaron Burstein, *Foreword* to Symposium: *The Law & Technology of Digital Rights Management*, 18 BERKELEY TECH. L.J. 487, 491 (2003).

337 *See* Benny Evangelista, *Suit Challenges CD Copyright Scheme*, S.F. CHRON., Sept. 11, 2001, at C3 (reporting on a lawsuit claiming that consumer rights were violated by new anti-piracy technology). In the end, the copyright owner agreed to ensure that its digital downloads were anonymous, to purge all of its customers' identifying information, and to place a warning label on further CDs that the CD in question would not work in DVD or CD-Rom players from then on. *See Consumers Win One Against Copy Protection*, Feb. 22, 2002, *at* http://www.polarity1.com/pcrr16.html; Tom Spring, *Face The Music: Suits Pending over Copy Controls*, Apr. 11, 2003, *at* http://www.pcworld.com/news/article/0,aid,93904,00.asp; *Sunncomm and Music City Records Agree to Resolve Consumer Music "CD-Cloqueing" Law Suit by Providing Better Notice and Enhancing Consumer Privacy*, Feb. 22, 2003, *available at* http://www.techfirm.comsunnsett.pdf (press release).

338 *See* Julie Cohen and Dan Burk, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J. L. TECH. 41 (2001).

television viewers to make digital copies of copyrighted television programs, to skip commercials, and to send copies of televised programs to other ReplayTV users.[339] The plaintiffs in a recent action, mostly motion picture studios, filed suit arguing that the activities of DVR owners constituted direct copyright infringement, and that the makers of the DVRs were contributorily liable as well.[340]

To buttress their claims, the plaintiffs demanded all documents and information that SONICblue possessed on its customers, particularly the television shows they recorded, and other data showing their viewing habits.[341] Even though SONICblue did not possess this information, the plaintiffs demanded that it reengineer its product to collect the data.[342] SONICblue refused, contending that it feared the information gathered could be used to file a host of suits against private individuals for acts of direct infringement.[343] The magistrate judge overseeing the case agreed with the plaintiffs and ordered SONICblue to install surveillance software to detect possible infringement and to record the viewing habits of individuals.[344] Not surprisingly, the magistrate judge's order unleashed a firestorm of controversy. "To require companies to spy on their customers in order to report suspicious activity to the movie studios is a complete invasion of privacy, particularly to those individual customers who don't even have the option of opting out," observed one representative of a free speech watch

---

339 Brief of Amici Curiae Civil Liberties and Consumer Groups in Support of Defendants' Objections to Magistrate Judge's Discovery Order at 1, Paramount Pictures Corp. v. ReplayTV, Inc., No. CV 01-9358FMC(EX), (C.D. Cal. Apr. 29, 2002, *available at* http://www.epic.org/privacy/replaytv/amici_brief_eick_order.pdf.

340 *Id.*

341 *Id.* Ironically, SONICblue had previously decided *not* to monitor its subscribers' usage due to cost and privacy considerations (especially given the public outcry over reports that one of their competitors, TiVo, used such monitoring practices). *See Id.* at 3.

342 *Id.* at 1.

343 Jane Black, *Faceless Snoopers Have the Upper Hand*, BUSINESSWEEK ONLINE, June 5, 2002, *at* http://www.businessweek.com/technology/content/jun2002/tc2002065_2710.htm.

344 Paramount Pictures Corp. v. ReplayTV, Inc., No. CV 01-9358FMC (EX), 2002 WL 1315811 (C.D. Cal. Apr. 29, 2002); *see Court Reverses Order for ReplayTV to Collect and Turn over Customer Usage Information*, ADLAW BY Request, June 10, 2002, *at* http://www.adlawbyrequest.com/inthecourts/ ReplayTV061002.shtml (on file with author).

group.[345] The order was swiftly reversed by a district court judge, who concluded that such requests "impermissibly require[] defendants to create new data which does not now exist."[346]

Although the surveillance issue was not directly addressed, the outcome of the dispute illuminates the tradeoff between privacy and increased piracy enforcement identified with respect to DRM technologies. In the wake of such conflicts, the law gains a predatory potential to traverse boundaries between private and public, creating a panoptic governance over individual acquisition and use of copyrighted material. In this climate, copyright holders may be able to force ISPs to reveal private information, including logs of the programs downloaded by individuals, any record of consumer activity, and Web sites visited.[347] And it may not matter whether the individual actually committed acts of copyright infringement – the accusation itself may be sufficient to warrant exposure of one's personal identity, as the DMCA provisions illustrate.

Such lawsuits raise the important question of how courts, legislators, and intellectual property owners can balance these interests of privacy and prevention of piracy.[348] Congress itself,

---

345 *Court Reverses Order for ReplayTV to Collect and Turn over Customer Usage Information*, *supra* note 344.

346 Order on Parties' Motions for Review of Magistrate Judge's Discovery Order of Apr. 26, 2002, at 3, Paramount Pictures Corp. v. ReplayTV, Inc., No. CV 01-9358FMC(EX), 2004 WL 57219 (C.D. Cal. Jan. 9, 2004).

347 *See* Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace,* 28 CONN. L. REV. 981 (1996):

> The activity of profiling, per se, is not new. It is a well-established practice through which businesses of all types seek to learn as much as possible about customers who show interest in their products or services. For transactions that occur in 'real' (as opposed to digital) space, however, the ability to profile one's customer base is limited to some extent by customers' willingness to self-report—for example, by filling out product registration cards. In contrast, profiling in the digital age holds out, for the first time, the tantalizing promise of 'perfect' information, because digital communications can be structured to create detailed records of consumer purchases and reading activities.

Id. at 988.

348 It bears noting that not all DRM technologies invade

in the pre-Internet age, already expressed a strong concern about the moral and administrative difficulties behind private enforcement of copyright in the home. In the 1970s, home-use recording from radio and television broadcasts was discussed in committee hearings, floor debates, and reports from the Office of Copyrights, and each evinced similar concerns regarding invasion of the spatial privacy of the home and the enforcement issues it would create.[349] For example, during one colloquy, Barbara A. Ringer, a representative from the Office of Copyrights, recognized the potential problem of unauthorized video recordings finding their way into the market. At that time, she stated that although this was a problem that Congress might face in the future, it could not be met by carrying copyright enforcement into the home. Her testimony observed: "I do not see anybody going into anyone's home and preventing this sort of thing, or forcing legislation that would engineer a piece of equipment not to allow home taping."[350]

---

individual expectations of privacy, however. *See*, *e.g.*, Stefan Bechtold, *Value-Centered Design of Digital Rights Management*, *at* indicare.berelecon.de/tiki-print-article.php?articleID=39 (outlining some DRM technologies that respect privacy and fair use); Fred von Lohmann, *Reconciling DRM and Fair Use: Preserving Future Fair Uses? at* http://www.cfp2002.org/fairuse/lohmann.pdf.

349 For example, in June 1971, Subcommittee No. 3 of the House Committee on the Judiciary met in hearings on the sound recording amendment. Representative Beister of Pennsylvania engaged in the following revealing dialogue with Ms. Barbara Ringer, then Assistant Register of Copyrights:

> MR. BEISTER. I can tell you I must have a small pirate in my own home. My son has a cassette tape recorder, and as a particular record becomes a hit, he will retrieve it onto his little set. Now, he may retrieve in addition something else onto his recording, but nonetheless, he does retrieve the basic sound. And this legislation, of course, would not point to his activities, would it?
>
> MISS RINGER. I think the answer is clearly, "No, it would not." I have spoken at a couple of seminars on video cassettes lately, and this question is usually asked: "What about the home recorders?" The answer I have given and will give again is that this is something you cannot control. You simply cannot control it.

Prohibiting Piracy of Sound Recordings: Hearings on S. 646 and H.R. 6927 Before Subcomm. No. 3 of the House Comm. on the Judiciary, 92d Cong. 22 (1971) (statement of Barbara A. Ringer, Assistant Register of Copyrights).

350 *Id.*

The Office of Copyrights continued to hold this view throughout the years of legislative revision.[351] As the original *Sony* court observed, this position developed in part from a concern about invasion of the individual's privacy in the home:

> "As Ms. Ringer testified, home recording simply cannot be controlled. Nobody is going into anyone's home to prevent it. . . . Of course, not all activity is made legal by virtue of occurring in a private home. Congress can constitutionally legislate against some activity which may occur in the home, but doing so necessarily requires caution. Here, legislative history shows that, in balance, Congress did not find that protection of copyright holders' rights over reproduction of their works was worth the privacy and enforcement problems which restraint of home-use recording would create."[352]

Looking back, it is resoundingly clear that the advent of technology has changed this original determination, particularly where the DMCA is concerned. Today, DRM technologies and other forms of piracy surveillance routinely govern and restrain one's at-home activities and usage of cultural products. DRM allows for the privatization of copyright enforcement; it eliminates judicial oversight and precludes an adversarial forum for the consumer's protection.[353] These systems operate automatically and panoptically, without the benefit of a complaint, response, third-party determination, or even a modicum of judicial involvement.[354] In other words, copyright enforcement has encroached, and integrated itself, into the home.

3. INTERFERENCE

A final method, significantly more unilaterally aggressive than the others, involves the use of smart agents that interdict transmissions. Here, companies use similar "bot" technology to

---

351 *See* Universal City Studios, Inc. v. Sony Corp. of Am., 480 F. Supp. 429, 446 (C.D. Cal. 1979), rev'd, 464 U.S. 417 (1984).

352 *Id.*

353 *See* Matt Jackson, *Using Technology to Circumvent the Law: The DMCA's Push to Privatize Copyright*, 23 HASTINGS COMM. & ENT. L.J. 607, 609 (2001).

354 *See* Thornburg, *supra* note 219, at 189.

search for a file and then, once found, drown the connection with so many requests that it prevents anyone from accessing any of the person's files, legitimate or not.[355] Other technologies simply interrupt a download as it occurs.[356] According to one company that produces interdiction software:

> "MediaDefender's computers hook up to the person using the P2P protocol being targeted and download the pirated file at a throttled down speed. MediaDefender's computers just try to sit on the other computers' uploading connections as long as possible, using as little bandwidth as possible to prevent others from downloading the pirated content. . . .
>
> The goal is not to absorb all of that user's bandwidth but block connections to potential downloaders. If the P2P program allows ten connections and MediaDefender fills nine, we are blocking 90% of illegal uploading."[357]

Note how the speaker assumes that all ten connections involve infringing files. Still other software creates *spoofing*, which involves the creation of phony media files and dumping them, en masse, onto peer-to-peer networks.[358] Spoofed files are often corrupt or damaged, and produce static, popping, cracking noises, or complete silence.[359] Another strategy involves

---

355 *See Piracy of Intellectual Property, Hearing Before the House Subcomm. on Courts*, *supra* note 293, 23-33 (statement of Gigi B. Sohn, President, Public Knowledge) (discussing interdiction); *see also* Matt Bai, *Hating Hilary*, WIRED, Feb. 2003, at 95, 97 (discussing several anti-piracy techniques), *available at* http://www.wired.com/wired/archive/11.02/hating.html?pg=1.

356 Healey, *supra* note 284. For example, once IpArchive's technology spots an unauthorized transfer, it can stop the transfer and send a notice directing the user to an authorized source for the file. *Id.* Importantly, the company will not identify the sender or the recipient, for privacy reasons. *Id.* In contrast, another program, Vidius, does identify the Internet addresses of the senders and recipients, and can often access names and contacting information if the ISP complies with the request. *Id.*

357 *Piracy of Intellectual Property, Hearing Before the House Subcomm. on Courts*, *supra* note 293, at 42. (statement of Randy Saaf, CEO, MediaDefender).

358 *See* Bai, *supra* note 355, at 97.

359 *See* Stephanie C. Ardito, *The Peer-to-Peer Piracy Prevention Act*, INFO. TODAY, Sept. 2002, at 18 (describing the countermeasures that

redirection, which draws upon the use of a decoy song file that activates a Web browser that takes the person to a legitimate site to purchase music.[360] A program called "freeze" locks up a computer system for a variable period of duration—also displaying a warning about downloading music.[361] Another program, called "silence," scans a computer hard drive for pirated music and then attempts to delete the files. [362]

Interdiction and spoofing are currently widely used throughout the peer-to-peer file sharing community, and have vastly increased in use during the last several months. They were also the primary subjects of a bill, introduced in the summer of 2002 by Congressman Howard Berman, which would award copyright holders an exemption from various laws proscribing computer break-ins when seeking perceived pirates.[363] (Some forms of interdiction, for example, bear strong resemblance to a traditional "denial of service attack," a crime which is illegal under state and federal anti-hacking statutes, including the Computer Fraud and Abuse Act).[364] Representative Berman argued that the vast increase in piracy, coupled with the continuing decentralization of peer-to-peer networks, made such efforts necessary, pointing out that the law has long allowed property owners to use self-help to protect their property and citing examples of DRM to support his position.[365]

---

copyright holders have employed to combat the growth of P2P networks). Moreover, because most users who upload MP3 files usually make all of their files immediately available to others, spoofed files can quickly spread beyond the RIAA's own servers, and infect the entire network. *See* Strahilevitz, *supra* note 167, at 584-85.

360 *See id.*

361 Andrew Ross Sorkin, *Zapping the Music Pirates*, THE INTERNATIONAL HERALD TRIBUNE, May 6, 2003, at 1.

362 *Id.*

363 *See* Peer-to-Peer Piracy Protection Act of 2002, H.R. 5211, 107th Cong.; *see also* James S. Humphrey, *Debating the Proposed Peer-to-Peer Piracy Prevention Act: Should Copyright Owners Be Permitted to Disrupt Illegal File Trading over Peer-to-Peer Networks?*, 4 N.C. J.L. & TECH. 375, 375 (2003); *see also* Alex Salkever, *Taking the Piracy Fight Too Far*, BUS. WK. ONLINE, *at* http://www.businessweek.com/technology/content/jul2002/tc2002079_7636.htm (July 9, 2002).

364 *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000).

365 *See* Salkever, *supra* note 363; *see also* Press Release, Howard L. Berman, Berman Introduces Legislation to Foil Peer to Peer Piracy (July 25, 2002), *available at* http://www.house.gov/apps/list/press/ca28_berman/piracy_prevention_act.html (citing software companies that make their software inoperable if their terms of use are violated, and cable operators that use electronic countermeasures to thwart the theft of their signals).

One possible advantage to these "interference" methods of surveillance is that they do not carry the same risks of identity disclosure as the other two methods, because they are focused on preventing infringement from occurring (rather than penalizing or monitoring the infringer). A peer-to-peer connection is simply disabled, rather than identities recorded and exposed. But it is easy to imagine the likelihood of copyright owners creating other programs that do carry these risks.[366] One potential avenue, for example, involves the spreading of "snitch" files that would actively collect information, such as the identity of the infringer, a list of files available for uploading, and the IP addresses of recipients of infringing uploads.[367] It could also be programmed to replicate itself as others accessed certain files, and could be passed on to other infringers.[368] This incriminating information could conceivably be used to generate cease and desist letters or criminal referrals.[369]

As these strategies suggest, the creation of safe harbors for such "corporate vigilantism" involves some risk that copyright owners might easily overstep their boundaries by extrajudicially determining that infringement has occurred, and damaging a computer or Internet connection as a result. Piracy surveillance techniques are developed and purchased by industries that seek to realize significant profits by inventing ways to deter and detect infringement. Under these regimes, the consumer becomes a helpless entity, unable to negotiate or even contact the copyright owner when a person's online activities are detected.

In the absence of public rules governing such behavior, and with the parties' abilities to engage in discussions with one another lacking, both offenders and non-offenders will become governed and monitored by the same regime. Fair use defenses

---

366 *See Privacy & Piracy, Hearing Before the Senate Permanent Subcomm. on Investigations*, *supra* note 193, at 1-3 (statement of Derek S. Broes, Executive Vice President of Worldwide Operations, Brilliant Digital Entertainment, Inc. and Altnet, Inc., criticizing programs that have "hacked applications and broken ranks with accepted rights of privacy on the Internet to spy on user behavior, analyze their files and generally divert intended actions of technology solutions selected and being used by end users").

367 *See* Joseph D. Schleimer, *Electronic Countermeasures to Copyright Infringement on the Internet: Law & Technology*, J. INTERNET L., Nov. 2001, at 1-3.

368 *Id.*

369 *Id.* at 3-4.

can be circumvented by private control. Moreover, because so much piracy surveillance takes place outside of the boundaries of government regulation, the "private" regime of piracy surveillance will likely be rewarded with another, equally protective individual self-help regime by individuals: encryption. Encryption creates a kind of "robust anonymity" that can sever the link between certain types of personal information and the person to whom it relates.[370]

Obviously, encryption is a type of privacy-enhancing technology that aids both law abiding and law evading citizens. But, as applied to the piracy surveillance scenario, particularly in the wake of *Aimster*, encryption will have distributional consequences on the nature of legitimate speech in cyberspace. Risk-averse individuals who are fearful of detection from copyright enforcers (either because they are actually pirating materials or are treading on a "grey area" of fair use) will be encouraged to encrypt their messages or files to escape detection.[371] As such, files that normally would be broadcast in cyberspace will be kept from the viewing eye of the public. In some circumstances, where the files represent perfect replications of copyrighted songs, the use of encryption might be desirable, because encryption prevents use by the general public, thereby reducing the number of infringing transactions. On the other hand, where the file represents something that arguably falls within a "grey area" of fair use (like the song in question in *Campbell v. Acuff-Rose Music*),[372] risk-averse creators might opt for encryption to avoid detection in cyberspace. This narrows the scope of the audience reached for

---

370 As Jerry Kang explains, encryption uses a cryptographic algorithm and a key to encode a message into ciphertext. The intended recipient uses a key to decode the message back into its original form. If the cryptographic algorithm is strong, and the key properly selected and kept secret, it is infeasible for an unauthorized party to intercept the ciphertext and decrypt it back into plaintext. *See* Kang, *supra* note 125, at 1242. Encryption will, increasingly, play a powerful role in the facilitation of darknets, which are thought to represent a newer, and more private, community for file sharing. *See, e.g.*, Heather Green, The Underground Internet, BUSINESSWEEK, Sept. 15, 2003, at 80.

371 *See, e.g.*, Robert Kay, *Next-Generation File Sharing With Social Networks*, *at* http:///www.openp2p.com/lpt/a/4671 (last visited Dec. 5, 2004)

372 *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 574-75 (1994) (deciding whether 2 Live Crew's parody of "Oh, Pretty Woman" constituted fair use).

a work, reducing the demand for certain works and eventually deleteriously affecting the incentive to create.

Moreover, as Professor Jerry Kang points out, the legality of some encryption methods is often uncertain.[373] As peer-to-peer jurisprudence suggests, information exchanges might get more privatized through encryption, but the more privatized these exchanges become, the more courts appear willing to require added degrees of surveillance and control. Consider the outcome of *Aimster*, which clearly suggested the need for software redesign to preclude encryption, and to encourage consumer monitoring. The presence of encryption, in that case, served to highlight the software developers' own "willful blindness," thereby opening up the doors to contributory liability. Finally, encryption methods also have the undesirable effect of encouraging a potentially wasteful "arms race" between entities that may attempt to develop technologies to overcome encryption and those that seek to develop ways to protect it. The constant use of resources for the protection and fencing of information appears to be one of the few ways in which individuals might be able to protect themselves from unwanted surveillance. Finally, while these surveillance activities fall within the twilight boundary between the protection of privacy and property, they also implicate a radically different view of copyright law than has been previously thought possible, altering the costs and benefits of copyright enforcement.

III. TOWARDS A REGIME OF PANOPTIC PUBLICATION

Part II outlined a number of ways in which intellectual property owners have privately sought to enforce copyright restrictions on cultural products and to detect unauthorized uses of their products. This result has significant effects on privacy, freedom of speech, and copyright itself—particularly where expression falls within "grey areas" of the fair use doctrine. As the protection and control of intellectual property expands, the protection of informational privacy shrinks. As a result, speech suffers. Consumers are forced to internalize the costs of their loss of anonymity and will curb their expression by restricting their conduct to that which is unquestionably insulated from liability. This phenomenon, in turn, can reduce the number of

373 *See* Kang, *supra* note 125, at 1242.

works created and disseminated, but can also quite drastically affect the way individuals experience and use cultural products.

How does piracy surveillance affect the incentives for creativity? Imagine that every activity you did on the Internet that involved the fair use of someone's copyrighted work – reviewing a photograph, creating a collage of copyrighted expressions, quoting certain texts, commenting on existing texts – was immediately subject to the permission of the copyright owner. Or, worse yet, imagine the copyright owner was capable of recording your activities and curtailing them if it deemed them to constitute "infringement." Where would your rights lie, particularly with respect to your freedom of expression or right to defend your activities from scrutiny? One risk-averse response might be to curb your behavior to prevent embarrassing or unwanted intervention from copyright owners. You might, then, erase detailed references to cultural products in your writing, avoid using language that resembles copyrighted speech, maybe even avoid certain forms of commentary, parody, fan fiction, collage, or sampling entirely. The eventual result would be a gradual chilling of creative behavior; the constant, silent, assertion of surveillance for infringement might eventually deter you from speaking at all.

This section argues that the nature of copyright has become fundamentally altered by the use of piracy surveillance in a regime of "panoptic publication." Under this regime, anyone who publishes information in cyberspace – whether a commentary on a particular book, or a work that draws upon existing work – can be subjected to an extrajudicial determination of infringement. In this way, copyright's bundle of rights becomes extended in two major ways. First, a copyright owner, through the guise of piracy surveillance, is endowed with a near-perfect ability to control and monitor others' use of a work, potentially circumventing fair use or other expressive defenses; and second, a copyright owner, under the DMCA, becomes endowed with the ability to unmask the identity of any author on the Internet, as long as a sufficient accusation of infringement is made under the DMCA.[374]

---

374 This risk has softened somewhat in the wake of *Verizon*, but the actual words of the DMCA, still unclear, could give rise to a contrary interpretation by another court. *See* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs. Inc., 351 F.3d 1229, 1233 (D.C. Cir. 2003) (noting

As I have suggested, piracy surveillance methods involve some relative tradeoff between an individual's interests in using, expressing, or disseminating intellectual property (and in protecting her identity from disclosure), and the interests of a third-party copyright enforcer. Just as an individual might place a high value on protecting her privacy or autonomy from invasion, a third-party enforcer may place a high value on protecting her property from unwanted use or infringement. The question, then, is how judges and legislators should balance these interests appropriately.

In this section, I will analyze both the arguments for and against such surveillance, and argue that any proposed, private benefits to individual copyright owners have not considered the substantial social costs for such surveillance regimes on non-offending individuals. Obviously, one benefit of piracy surveillance is somewhat clear: a reduction in the harm caused by copyright infringement. But this benefit must also be weighed against the various costs involved, which include the potential of piracy surveillance to: block access to certain types of legitimate information, prevent fair use of cultural products, expose anonymous speakers, mistake legitimate files for illegitimate ones, and cast a wide net of groundless accusation. As this section will argue, proponents of such systems often fail to recognize these substantial costs for non-offenders, such as risk-aversion, the possibility of mistake, and over-deterrence of speech and fair use.

Let me begin by clarifying that I am not arguing that the types of piracy the RIAA seeks to deter are – or should be – immune from liability. Rather, my concern in this Article is to protect *other* types of expression – fair uses, anonymous speech – that can become wrongly caught within the panoptic web of surveillance. Consider, for example, the world of fan fiction, remixes, or even alternative commentary tracks for DVDs. All of these are areas of creativity, each of which can be subject to varying degrees of fair use defenses, and which can be monitored and potentially silenced under the current DMCA regime.[375] The very purpose of copyright is to ensure that a balance exists

---

that under the DMCA, "a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity," not to an ISP that is merely serving as a conduit for data transmitted between two Internet users).

375 I am grateful to Fred Von Lohmann for these suggested examples.

between control over private ownership and expression in order to create incentives for more speech creation. Yet piracy surveillance eviscerates this balance between control and expression, leading to an inescapable logic of vigilantism. Instead of protecting the creation of cultural products, piracy surveillance has transformed copyright into a regime where copyright owners are legally empowered with a variety of means to panoptically identify, classify, and threaten potential pirates; and, in doing so, are made capable of controlling the public's access to cultural products to an unprecedented degree, thereby reducing the incentives for further speech and creation.

A. PRIVACY AND AUTONOMY

The underlying logic behind piracy surveillance is inextricably tied to real space principles, suggesting that intellectual property is equivalent, in both form and content, to other types of properties in real space. Thus, proponents of piracy surveillance point out that comparable measures of legalized self-help (like the right of repossession or defense of property) are traditionally available to property owners in real space; thus, the same should be available to intellectual property owners in cyberspace.[376] This is true: A property owner is permitted, under the law, to take certain actions to recover stolen possessions, and is granted some immunity from trespassing on others' land for that purpose. Yet there is a crucial difference between such strategies in real space as opposed to cyberspace: Self-help methods in real space are traditionally premised on maintaining, not destroying, preexisting boundaries between private and public space. For this reason, self-help strategies in real space reify, rather than erode, the architecturally-created balance between spatial protections for privacy and protection of property discussed in Part I of this Article. Indeed, both the common law and the U.C.C. have extended self-help allowances to property owners with a few important caveats: both bodies of law limit the right to enter private property in order to repossess items to those

376 *See* Email from Alec French, Minority Counsel, House Judiciary Subcommittee on Courts, the Internet, and Intellectual Property, on behalf of Rep. Berman, to Declan McCullagh, Chief Political Correspondent for CNET News.com (Sept. 4, 2002) (explaining the copyright protection provided by the Peer-to-Peer Piracy Prevention Act), *available at* http://www.politechbot.com/p-03949.html.

circumstances where some degree of consent or acquiescence has been shown, and usually in circumstances where an existing contract has been breached.[377]

Thus, given that the law traditionally creates exceptions to the law of trespass to permit self-help repossession of chattels kept on private property, courts usually justify these limitations only if the actors can accomplish them without a breach of the peace, and with the consent of the private property owner.[378] Other cases require some notification before taking unilateral action.[379] Moreover, case law from real space suggests that even trespassers enjoy some expectations of privacy from unreasonable searches and seizures.[380] Above all, any force must be reasonable under the circumstances, and a person is liable for any harm done in the exercise of these privileges.[381] No case has ever held that an entry into one's home, without the consent of the owner, is justifiable self-help.[382]

The use of piracy surveillance scenarios in cyberspace shatters this traditional balance between the protection of property and the protection of privacy. After all, intellectual

---

377 *See* Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1101-02 (1998); *see also* Pamela Samuelson, *Embedding Technical Self-Help in Licensed Software*, COMM. OF THE ACM, Oct. 1997, at 13.

378 Samuelson, *supra* note 377, at 15; *see generally* Douglas Ivor Brandon et al., *Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845 (1984) (exploring the permitted use of self-help in various legal areas).

379 *See, e.g.*, Jon K. Wactor, *Self Help: A Viable Remedy for Nuisance? A Guide for the Common Man's Lawyer*, 24 ARIZ. L. REV. 83, 92 (1982) (collecting case law on this point).

380 *See* People v. Schafer, 946 P.2d 938, 944-45 (Colo. 1997) (recognizing trespasser's rights to privacy in sealed tent); *see also* Luke M. Milligan, Comment, *The Fourth Amendment Rights of Trespassers: Searching for the Legitimacy of the Government-Notification Doctrine*, 50 EMORY L.J. 1357, 1360 (2001) (discussing trespasser privacy expectations and protection provided by state and federal courts).

381 Brandon, *supra* note 378, at 861; *see also* RESTATEMENT (SECOND) OF TORTS § 198 (1965) (discussing "Entry to Reclaim Goods on Land Without Wrong of Actor").

382 *See* James R. McCall, *The Past as Prologue: A History of the Right to Repossess*, 47 S. CAL. L. REV. 58 (1973). Repossessors are usually barred from forcibly entering a person's home, for example. *See also* Butler v. Ford Motor Credit Co., 829 F.2d 568, 570 (5th Cir. 1987); Dearman v. Williams, 109 So. 2d 316, 321 (Miss. 1959); Kirkwood v. Hickman, 78 So. 2d 351, 356 (Miss. 1955).

property is not real property, and a number of particularized rules govern the use of intellectual property. A host of statutory exceptions (including fair use) limit an owner's exclusive control over intellectual property.[383] Moreover, self-help analogies from real space often fail to consider the costs of such invasion on a non-offending individual. Instead of serving as a passive constraint to protect from invasions of real property (like a lock or fence), some piracy surveillance techniques (like the use of smart agents for monitoring) are instituted without probable cause or notice to the user and carry the potential to eviscerate one's anonymity.[384] In sum, 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.

Here is where the panoptic metaphor is so prescient. Constant monitoring alters online behavior in inescapable ways – one's speech, surfing habits, use of cultural products, and even identity itself. In this sense, piracy surveillance has deleterious implications for autonomy. Consider Lawrence Lessig's commentary on this point:

---

383 *See* 17 U.S.C. § 107 (2000). For example, "although one enraged musician testified to Congress that copyright infringement was 'theft,'" the literal equivalent of someone "walk[ing] into a record store, grab[bing] what they wanted and walk[ing] out," that is not precisely the case, as even the Supreme Court has recognized. Bailey, *supra* note 141, at 488; *see also* Dowling v. United States, 473 U.S. 207, 217 (1985) ("[I]nterference with copyright does not easily equate with theft, conversion, or fraud.").

384 Consider a real space example. In one piracy surveillance strategy, researchers created equipment that detects the faint radio signals emitted regularly by computers. A special code installed in the software would allow monitors to identify the software the computer is currently using by broadcasting certain signals. Using the technology, anti-piracy groups could detect the number of signals emanating from a company's office to determine infringement. *New British Anti-Piracy Solution Based on Intelligence Techniques*, TELECOMWORLDWIRE, Mar. 2, 1998, *available at* 1998 WL 5141163. Now, compare this with recent Supreme Court jurisprudence, which only just recently observed that the use of sense-enhancing technology to gather information about the interior of a home constituted a "search" within the meaning of the Fourth Amendment, pointing out that the very core of Fourth Amendment jurisprudence involved the right of a man to retreat into his own home, free from governmental intrusion. *See* Kyllo v. United States, 533 U.S. 27, 31-34 (2001). Indeed, *Kyllo* holds that the use of devices that are not used in general public to explore details of a home is presumptively unreasonable without a warrant. *Id.* at 40.

> If you walked into a store, and the guard at the store recorded your name; if cameras tracked your every step, noting what items you looked at and what items you ignored; if an employee followed you around, calculating the time you spent in any given aisle; if before you could purchase an item you selected, the cashier demanded that you reveal who you were – if any and all of these things happened in real space, you would notice. You would notice and could then make a choice about whether you wanted to shop in such a store. . . .

In cyberspace, you would not. You would not notice such monitoring because such tracking in cyberspace is not similarly visible."[385]

For this reason, as Julie Cohen points out, technologies that force changes in user behavior decrease the zone of autonomy that *all* users enjoy with respect to the enjoyment of intellectual goods:[386] Both by directly constraining private behaviors related to intellectual consumption and by enabling creation of detailed and permanent records of such consumption, these technologies have the potential to change dramatically the way people experience intellectual goods.[387]

Proponents of piracy surveillance contend, following *Kennedy*, that a person does not enjoy any reasonable expectation of privacy in material that he or she might leave open for public view, display, or use, especially music files that can be uploaded to others. The *Verizon* trial court echoed this point, observing, where an ISP subscriber "opens his computer to permit others, through peer-to-peer file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."[388] But this point fails to consider the other policy concerns that turn on the importance of protecting non-offending individuals from unwanted surveillance in

---

385 Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 504-05 (1999).

386 Cohen, *supra* note 330, at 580.

387 *Id.*

388 *In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 267 (D.D.C. 2003).

cyberspace. As the Ninth Circuit just noted in *Theofel v. Farey-Jones*:

> The subpoena power is a substantial delegation of authority to private parties, and those who invoke it have a grave responsibility to ensure that it is not abused. Informing the person served of his right to object is a good start, see Fed. R. Civ. P. 45(a)(1)(D), but it is no substitute for the exercise of independent judgment about the subpoena's reasonableness. Fighting a subpoena in court is not cheap, and many may be cowed into compliance with even overbroad subpoenas, especially if they are not represented by counsel or have no personal interest at stake.[389]

Unlike analogies in real space, piracy surveillance does not entail formal notice, consent, or negotiation between the parties. Nor does it protect constitutional assurances of anonymity. Individuals who are caught within the panoptic Web of piracy surveillance have little protection: Any of their uses of cultural products, or expression, is subjected to the governing, extrajudicial gaze of a copyright owner. Under the DMCA subpoena provision, for example, it does not matter whether the person has actually infringed on a copyright or not – all that matters is that the owner has a subjective "good faith belief" that the infringement has occurred.[390] The same can also be said of DRM technologies, which entirely circumvent judicial oversight in favor of automatic copyright enforcement.

Moreover, piracy surveillance implicates two particular rights, both connected to autonomy: first, the right to speak anonymously; and second, the right to receive information. To

---

389 341 F.3d 978, 984 (9th Cir. 2003).

390 DMCA, 17 U.S.C. § 512(c)(3)(A)(v) (2003). *But see* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs. Inc., 351 F.3d 1229, 1231 (D.C. Cir. 2003) (holding that the RIAA's attempts to obtain the identity of Verizon subscribers accused of unauthorized sharing of copyrighted files is not authorized under the DMCA's subpoena provision); Katie Dean, *RIAA Strikes Again at Traders*, WIRED NEWS, Jan. 21, 2004, *at* http://www.wired.com/news/digiwood/0,1412,61989,00.html (describing the RIAA's filing of 532 "John Doe" suits against individuals it has accused of illegal file-sharing, in response to the D.C. Circuit's ruling that the DMCA does not authorize the RIAA's attempts to subpoena ISPs to obtain the personal information about the ISPs' subscribers).

its credit, the *Verizon* court duly acknowledges that some lower courts have held that the First Amendment recognizes a right to anonymity, both in real space and on the Internet.[391] But the court limited the scope of this right by pointing out that courts have usually embraced a right to anonymity in situations involving "core First Amendment expression."[392] By drawing this unduly stark line between First Amendment rights of expression and copyright infringement, the court mistakenly presumed that the individual in question – indeed, every individual potentially subject to a DMCA notice – was already guilty of infringement, and thus was not entitled to any First Amendment protections.[393]

Extrajudicial determinations of copyright liability are particularly precarious, especially where disclosure of anonymity is at risk.[394] In *McIntyre v. Ohio Elections Commission*, the Supreme Court found that an Ohio law violated the First Amendment because it prohibited the distribution of anonymous campaign literature.[395] In that case, the Court held that when a statute places burdens on "core political speech," it will apply a heightened degree of scrutiny to the statute, and uphold it if it is "narrowly tailored" to advance an "overriding state interest."[396] This recommended balancing test is essential to preserving the important discursive values supported by anonymity, and necessitates a careful balancing of the rights of the speaker with the interests of law enforcement. In stark contrast, in *Verizon*, the district court blithely rejected this view, observing:

> [T]his is not a case where Verizon's customer is anonymously using the Internet to distribute speeches of Lenin, Biblical passages, educational

---

391 *In re* Verizon, 257 F. Supp. 2d at 259; *see also* Sony Music Entm't Inc. v. Does 1-40, 326 F.Supp.2d 556 (S.D.N.Y. 2004).

392 *In re* Verizon, 257 F. Supp. 2d at 259.

393 *Id.* at 260.

394 Yet as one lawyer observes, "many people converse on the Internet anonymously unaware that they have become the subject of a subpoena seeking their identity before it is too late to quash the subpoena." *EFF & Liberty Project Defend Anonymous Poster Against Third-Party Identity Subpoenas to ISPs*, 14 EFFECTOR 1 (Feb. 7, 2001) (quoting Nicole Berner, counsel for the Liberty Project), *at* http://www.eff.org/effector/HTML/effect14.01.html#I.

395 514 U.S. 334, 357 (1995).

396 *Id.* at 347.

> materials, or criticisms of the government – situations in which assertions of First Amendment rights more plausibly could be made. . . . [T]he purpose of protecting anonymous expression is to safeguard those 'who support causes anonymously' and those who 'fear economic or official retaliation,' 'social ostracism,' or an unwanted intrusion into 'privacy.'[397]

Yet the court missed the significance of the issue at stake. By short-circuiting consideration of the appropriate balancing test that *McIntyre* advocates, the *Verizon* trial court assumed, without deciding, that the individual's activities in question constituted direct infringement, and thusly were undeserving of anonymity. By ascribing to the RIAA's private, extralegal determination of infringement, the court failed to perform the balancing test that *McIntyre* recommends, and deferred instead to the prior judgment of a private party.

One might rightfully ask why the law should even attempt to protect the interests of individuals who are engaging in massive, illegal (and often criminal) levels of copyright infringement. Shouldn't they be held accountable, and why should privacy matter here at all? The obvious answer to the former question is yes; indeed, it is absolutely true that the RIAA has restricted its use of the subpoena provision, to date, to the most egregious infringers, situations where a court would likely agree with the RIAA's assessment of liability in most cases.[398] However, aside from these cases, there is substantial confusion over what, exactly, constitutes "copyright infringement" in other contexts, and this is why privacy becomes so important. *Napster*'s immediate conflation of file sharing with copyright infringement masks a host of complexities regarding the extent to which fair use defenses, or space shifting, might conceivably apply in such contexts. While the

---

397 *In re* Verizon, 240 F. Supp. 2d at 43 (quoting, in part, Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150, 165 (2002)).

398 *Privacy & Piracy, Hearing Before the Senate Permanent Subcomm. on Investigations*, *supra* note 193, at 7-8 (testimony of Mitch Bainwol, Chairman and CEO, RIAA) ("RIAA is not seeking a subpoena as to everyone who is illegally distributing copyrighted recordings. Rather, at this time, RIAA is focusing on egregious infringers, those who are engaging in substantial amounts of illegal activity.").

RIAA has admirably shown some restraint in choosing to pursue only egregious uploaders of multiple files, the DMCA provisions allow *anyone* to invoke these procedures to unmask a speaker's identity. Aside from the risk of identity disclosure, in dealing with the large numbers of notice-and-takedown requests they receive, few ISPs have the time or ability to investigate whether the substance of the accusation is meritorious or not. As I have shown, mere *accusations* of infringement provide powerful mechanisms for silencing others under the DMCA.[399] So, although an *actual* infringer cannot assert a First Amendment defense, the DMCA's provision, coupled with the increasing spectre of piracy surveillance, wrongly presumes guilt before innocence, thereby eviscerating protection for anonymity.[400]

Moreover, aside from the failure to balance protections for anonymity with copyright, piracy surveillance also raises concerns about autonomous access to information. In real space, for example, a consumer of copyrighted material enjoys anonymity: the copyright owner does not know the identity of the person who reads, listens, or watches certain material.[401] However, some forms of piracy surveillance alter this critical balance of interests between the consumer and creator, permitting a copyright owner to have the right to unmask the identity of an end user.[402] In *Stanley v. Georgia*,[403] a case which suggested the importance of intellectual privacy, the Supreme Court held that the First and Fourteenth Amendments prohibited making private possession of obscene material a crime. In that case, the Court recognized that the valid

---

399 *See* Sony Music Entm't Inc. v. Does 1-40, 326 F.Supp.2d 556 (S.D.N.Y. 2004) (holding that Does had a limited First Amendment right to protection of identity). As Professor Jed Rubenfeld has emphasized, copyright restrictions inherently raise First Amendment concerns because they turn speech into property; and by doing so, they are capable of making people liable for speaking, thus creating a "private power over public speech." Jed Rubenfeld, *The Freedom of Imagination: Copyright's Constitutionality*, 112 YALE L.J. 1, 25 (2002) (emphasis omitted).

400 As one court observed, "If Internet users could be stripped of . . . anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights." Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, 1093 (W.D.Wash. 2001).

401 *See WIPO, Hearing on H.R. 2281 Before the Subcomm. on Telecommunications*, *supra* note 199, at 12 (statement of Marc Rotenberg, Director, Electronic Privacy Information Center).

402 *Id.* at 14.

403 394 U.S. 557 (1969).

governmental interest in dealing with the problem of obscenity could not justify its insulation from other constitutional rights, particularly those implicated in a statute forbidding the mere possession of obscene materials.[404] As the Court observed:

> This right to receive information and ideas, regardless of their social worth, is fundamental to our free society. Moreover, in the context of this case – a prosecution for mere possession of printed or filmed matter in the privacy of a person's own home – that right takes on an added dimension. For also fundamental is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy.405

Those values easily translate into the context raised in this Article, where the DMCA's provisions extend piracy surveillance into the home activities of many citizens, resulting in a tradeoff in terms of the autonomy and freedom of ordinary citizens to access information. This is particularly true with respect to DRM, but similar analysis could also underline the other surveillance techniques I have identified. In *Stanley*, the appellant asserted the right to read or observe what he pleases, to satisfy his own intellectual needs in the privacy of his own home.[406] Importantly, the Court rejected the proposition that the obscene character of the materials meant he had no right to possess them, observing, "[w]hatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home."[407] The same observations apply to the effects of piracy surveillance, where a person could be precluded from undertaking a host of activities involving the use and possession of copyrighted material in one's own home.

Even in a university context, private copyright enforcement thus exacerbates the risk of intrusion, where, as *Griswold* has pointed out, the "right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read and freedom of inquiry, freedom of thought, and freedom to teach –

---

404 *Id.* at 568-70.
405 *Id.* at 563-64 (citation omitted).
406 *Id.* at 565.
407 *Id.*

indeed the freedom of the entire university community."[408] As one university representative has testified regarding the DMCA:

> [T]he legislation's notice and takedown procedure would have a different impact on institutions of higher education than it would on commercial service providers. . . . Enforcing the "takedown" of material in response to a notice of alleged infringement would have the appearance of suppression of speech, particularly in a setting where fair use makes the legality or illegality of a particular infringement claim less than crystal clear 409

Consider the implications of the music industry's request to allow its computer experts to scan all computers at the University of Melbourne for sound files and email accounts so that it could gather evidence of copyright infringement.[410] Under *Stanley* and *McIntyre*, a court should have to perform a balancing test to examine whether the incursion of privacy was justified by the assertion of copyright infringement. "If the First Amendment means anything," the *Stanley* Court powerfully observed, "it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."[411]

B. DUE PROCESS AND FREEDOM OF EXPRESSION

A piracy surveillance advocate might argue that these areas of copyright enforcement and surveillance are no different than monitoring activities taken in real space to protect one's property. After all, if someone publishes something on the Internet, or makes certain files available, he or she should know that intellectual property owners will routinely monitor such uses in order to protect copyrighted work from unauthorized

---

408 Griswold v. Connecticut, 381 U.S. 479, 482 (1965) (citations omitted).

409 *See WIPO, Hearing on H.R. 2281 Before the Subcomm. on Telecommunications*, *supra* note 199, at 73-74 (1998) (statement of Charles E. Phelps, Provost, University of Rochester).

410 *See* Lamont, *supra* note 4, at 3.

411 Stanley v. Georgia, 394 U.S. 557, 565 (1969).

reproduction. But there is a difference in cyberspace: anonymity. Piracy surveillance creates a world in which copyright owners can set the terms of use, police consumers, record and expose their personal information, and penalize potential infringers – all, to a varying extent, outside of the boundaries of state control.

A further justification that may be offered for granting the province of piracy surveillance to individual copyright owners, rather than an ISP or the government, turns on institutional competence and efficiency considerations: A private copyright owner, rather than another entity, should internalize the costs of his detection of infringement because the copyright owner has the appropriate incentives to do so. Two concerns weigh against creating the type of privatized regime of copyright enforcement that currently exists under the DMCA: the first turns on identity; the second turns on the importance of judicial oversight and due process concerns.

Even if it is efficient and desirable to place the burden on a copyright owner to detect infringement, the need for robust judicial safeguards are obvious, particularly where values of speech, expression, and fairness are implicated. The point of copyright law is not to create a stand-alone, self-contained regime, where copyright issues are resolved without attention to other common law or constitutional values, like due process, freedom of speech, or privacy. Yet the DMCA propagates an isolationist tendency by failing to require copyright owners to conform to the constitutional protections normally afforded to citizens under the First, Fourth, or Fifth Amendments. The *Verizon* trial court maintained, in contrast, to this view:

> [T]he DMCA neither authorizes governmental censorship nor involves prior restraint of potentially protected expression. Section 512(h) merely allows a private copyright owner to obtain the identity of an alleged copyright infringer in order to protect constitutionally-recognized rights in creative works; it does not even directly seek or restrain the underlying expression (the sharing of copyrighted material). Thus the DMCA does not regulate protected expression or otherwise permit prior restraint of protected speech. It only requires production of the identity of one who has engaged

> in unprotected conduct – sharing copyrighted material on the Internet.[412]

This observation, at first glance, is rhetorically powerful, particularly as applied to the facts in *Verizon*. But the statement also overlooks the interplay of three other elements: (1) the gatekeeper role of the ISP, which faces the threat of contributory infringement if it does not act immediately to silence the offensive conduct; (2) the potential for strategic motives of a copyright owner, who may be tempted to file notices for spurious reasons; and (3) the fact that the subpoena provisions are not limited solely to individuals who upload copyrighted songs (an admittedly clearer issue of infringement), but apply to *anyone* who offers, obtains, or creates *allegedly* infringing material on the Internet. Since the words of the DMCA permit a preliminary unveiling of identity, Section 512 can give rise to serious due process concerns, for the accused herself as well as the ISP, if the subpoenaed party lacks the ability to object.[413]

As Professors A. Mitchell Polinsky and Steven Shavell explained, the rationale for public law enforcement often turned on the role of information about the identity of violators.[414] When victims of harm naturally know who injured them, allowing private suits for harm will motivate victims to initiate legal action and use that information to enforce law.[415] (That is why the enforcement of tort and contract law is private in nature.) In contrast, if victims do not know who injured them, or if it is difficult to identify or apprehend perceived criminals,

---

412 *In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 261 (D.D.C. 2003).

413 *See* Brief of Amici Curiae United States Industry Association et al. at 5, *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24 (D.D.C. 2003) (No. 02-MS-0323). See also Matthew Amedeo, *Shifting the Burden: The Unconstitutionality of Section 512 (H) of the Digital Millennium Copyright Act and Its Impact on Internet Service Providers*, 11 COMMLAW CONSPECTUS 311 (2003). The due process clause of the Fifth Amendment guarantees a party adequate procedural safeguards before a deprivation of a property or liberty interest. The seminal requirements of due process have been set forth for years: "notice reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and [to] afford them an opportunity to present their objections." Mullane v. Cent. Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950).

414 A. Mitchell Polinsky & Steven Shavell, *The Economic Theory of Public Enforcement of Law*, 38 J. ECON. LITERATURE 45, 46 (2000).

415 *Id.*

public enforcement may be more desirable.[416] According to Polinsky and Shavell, public enforcement is made even more desirable if inducements to private parties to supply information are somehow inadequate, in the sense that they encourage wasteful efforts to locate violators, or if they encourage the use of force in gathering information and capturing violators, for example.[417] Thus, public enforcement is usually preferred when effort is required to identify and apprehend violators.[418]

These observations become particularly important when we consider the effects of the DMCA subpoena power on citizen expression in cyberspace. The DMCA section, as it is written, empowers anyone who alleges "unauthorized" use of a copyrighted work to obtain a subpoena with the identity of any Internet user – without the institution of ongoing or anticipated litigation, or even notice to the user herself.[419] Moreover, piracy surveillance techniques, in and of themselves, do not demonstrate a predisposition towards the kind of discretionary non-enforcement that is typically demonstrated by public prosecutors and law enforcers.[420] Instead, piracy surveillance methods are calibrated to be overbroad by design in order to deter the widest possible breadth of infringement.

Returning to Polinsky and Shavell's point, the problem of anonymity, coupled with the low standard of proof, lays the groundwork for the possibility of "overfishing" for violators. The fact that it is of little cost for the copyright owner to file and serve a DMCA subpoena means that it is not necessary that the copyright owner have a high probability of success in filing suit.[421] Rather, the copyright owner only needs to have a high

---

416 *Id.*

417 *Id.*

418 *Id.*

419 Brief of Amici Curiae in Support of Appellant Verizon Internet Services and Urging Reversal at 2, Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) (Nos. 03-7015, 03-7053) (consolidated appeals). *Verizon* may have softened this risk, however. *See Verizon Internet Servs., Inc.*, 351 F.3d at 1236-37 ("[T]he subpoena power of § 512(h) [of the DMCA] applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.").

420 *See* William M. Landes & Richard A. Posner, *The Private Enforcement of Law*, 4 J. LEGAL STUD. 1, 42-43 (1975).

421 *See* Warren F. Schwartz, *Legal Error*, *in* ENCYCLOPEDIA OF LAW AND ECONOMICS, VOLUME I: THE HISTORY AND METHODOLOGY OF LAW AND ECONOMICS 1029, 1038 (Boudewijn Bouckaert & Gerrit De Geest eds.,

probability that the offending expression itself will be deterred after the notice is served. Given that the responsibility for enforcing a copyright rests with the ISP, who then faces the responsibility of "taking down" the infringing material, cutting off Internet access to the client, or facing contributory liability, the ISP might respond immediately, and in some cases fail to afford prior notice or enable an impartial, independent determination.[422]

Indeed, the need for judicial oversight becomes particularly pronounced where fair use and speech are concerned. As anyone who practices copyright litigation will attest, sorting out competing claims of infringement and fair use is time-consuming, fact-specific, and deeply prone to strategic manipulation. Yet piracy surveillance allows copyright owners to circumvent access to a fair, adversarial, and impartial forum. Mere accusations of infringement can displace court-ordered determinations. In sum, piracy surveillance techniques also fail to consider two significant costs to non-offenders: overdeterrence of speech and evisceration of fair use. These two elements, taken together, paradoxically convert copyright from a regime that governs the illegitimate uses of private properties into a regime that governs *all* speech and expression in cyberspace, even when it is only tangentially related to the copyright owner in question.

The effect of this transformation cannot be understated – both with respect to copyright law, as well as the nature of cyberspace itself. To understand its effects, it is helpful to recall that fair use cures a market failure in copyright that may be created because the possibility of consensual bargain may have broken down in some way, either because transaction costs are too high or because agreement is otherwise impossible.[423] Piracy surveillance, however, eclipses judicial enforcement of fair use, because a private entity's determination under the DMCA circumvents access to a fair and impartial forum. Because private, rather than public, entities are now capable of determining whether a use is fair or not, the correction of market failure is largely impossible. Instead, Section 512(h), the

---

2000) ("In general, the higher the costs which a victim must incur in suing an injurer the greater must the probability of success be for the victim to sue.").

422 *See Verizon Internet Servs., Inc.*, 351 F.3d at 1234.

423 *See* Wendy J. Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the* Betamax *Case and Its Predecessors*, 82 COLUM. L. REV. 1600, 1613 (1982).

subpoena provision at issue in *Verizon*, provides no protection for expression that may be determined, at a later point, to be fully protected speech.[424]

As I have discussed, *Napster* placed the responsibility to detect infringement upon intellectual property owners, and the DMCA's standard for a notice-and-takedown request is surprisingly subject to manipulative assertions of copyright infringement. Piracy surveillance advocates might respond by pointing out, first, that the subpoena provision does not target actual expression, only one's identity; and second, that most of the cases falling under the recording industry's purview concern actual infringement, which is traditionally outside of the purview of the First Amendment.[425] But these arguments also presume a clarity between infringement and fair use that is often illusory. This line may be fairly easy to draw if we are considering the liability of someone who is uploading hundreds of files of copyrighted music (something that courts generally agree constitutes infringement), but is much harder to draw in cases that involve someone who is downloading music for parody, fair use, space shifting, or transformative purposes.

Uncertain legal standards, as John Calfee and Richard Craswell remind us, deter socially desirable behavior through overcompliance.[426] In these circumstances, an extrajudicial determination of infringement is efficient, quick, but often prone to mistake, thus laying the groundwork for the uncertainty that may motivate an over-deterrence of speech. Applying Calfee and Craswell's observations, the rising probability of extrajudicial enforcement, coupled with the apparent uncertainty of an extrajudicial determination, risks deterring expression. Consider some of the following examples of "mistaken" DMCA notices, i.e. situations in which accusations of

---

424 *See* Brief for Appellant at 32, Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) (Nos. 03-7015, 03-7053) (consolidated appeals).

425 Brief of Amici Curiae Motion Picture Association of America, Inc., et al., in Support of the Recording Industry Association of America and Urging Affirmance at 12, Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) (Nos. 03-7015, 03-7053) (consolidated appeals) ("Infringers . . . do not create speech, they copy it.").

426 *See* John E. Calfee & Richard Craswell, *Some Effects of Uncertainty on Compliance with Legal Standards*, 70 VA. L. REV. 965, 966 (1984).

infringement were made in order to silence particular expression:

- Notice ID No. 232: Church of Scientology aims to remove links written by individuals who publish criticisms of its work.

- Notice ID No. 310: Individual attempts to use DMCA to assert trademark claims, rather than copyright claims, in order to take advantage of its takedown provisions.

- Notice ID No. 94: Copyright owner for the character Barney threatens a DMCA notice in order to try to remove photo that allegedly "incorporates the use and threat of violence towards the children's character Barney without permission."

- Notice ID No. 348: DMCA claim made against individual who posted public court records containing copyrighted images.[427]

In one recent case, an electronic voting machine company flooded ISPs with DMCA notices claiming copyright infringement in order to remove embarrassing internal e-mails that were critical of the company. Even though such documents were arguably covered by fair use, many ISPs removed the material without challenging the initial determination.[428]

---

427 *See* Brief of Amici in Support of Verizon's Opposition to RIAA's Motion to Enforce at 9-10, *In re* Verizon Internet Servs., Inc., 258 F. Supp. 2d 6 , No. 02-MS-0323, (D.D.C. 2003).

428 *See also* Paul Roberts, *Diebold Voting Case Tests DMCA*, PC WORLD NEWS, *at* http://www.pcworld.com/news/article/0,aid,113273,00.asp (Nov. 4, 2003). 17 U.S.C. § 512(f), which provides as follows: Misrepresentations.--Any person who knowingly materially misrepresents under this section-- (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it. These mechanisms are powerful vehicles to deter

As these examples demonstrate, the DMCA's notice-and-takedown provisions are often used for a host of reasons that do not match up with a meritorious assertion of copyright infringement. Moreover, the exceedingly complex, inconsistent, and ambiguous case law regarding copyright can often lead individuals to chill potential expression out of the fear of liability, particularly when they recognize the potential to unmask anonymous speech under the DMCA subpoena provisions.

IV. BALANCING PRIVATE AND PUBLIC ENFORCEMENT

In cyberspace, intellectual property and privacy are at an impasse. There is no way out – the enforcement of each area faces inherent conflicts with another. Throughout the development of copyright in cyberspace, intellectual property rights have slowly and quietly expanded to take precedence over the privacy and expressive rights of ordinary citizens. Part of this is due to the expansion of property rights over areas of intangible information and the absence of strong legislative protections of informational privacy. Yet, part of it is also due to a failure among lawmakers and judges to conceptualize a deeper relationship between property and privacy; there is a current tendency, shared by many, to separate intellectual property rights from privacy and to create a hierarchical relationship between the two. In other words, the law has displayed a persistent failure to recognize that expansions of control of intellectual property cause tradeoffs in other areas of consumer protection – particularly where privacy is concerned. As a result, we have created a world in which the property rights of copyright owners are valued over the liberty, property, and privacy rights of others, suggesting that those principles are somehow less valuable than those involving commercial self-protection.[429]

Today, even in the wake of *Verizon*, the rivalry between intellectual property and privacy persists, even though the factual scenario has changed. In prior sections, I argued that

---

Diebold-like situations, but they should be supplanted with the solutions outlined in Part IV. For more information on the case, *see http://www.eff.org/legal/ISP_liability/OPG_v_Diebold* (last visited Dec.16, 2004).

429 *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1390 (2000).

copyright law has been irretrievably altered by this panoptic transformation, because the DMCA (among other areas of copyright) enables content owners to patrol and monitor the end user's subsequent expression with little judicial oversight. In turn, as the *Napster* and *Verizon* cases suggest, copyright owners' ability to monitor peer-to-peer communications also incurs the potential to unmask the activities, identities, and expressions of *all* citizens who post information in cyberspace. Consequently, the risk of implicating non-offenders within the panoptic snare of piracy surveillance raises the danger of silencing speech and expression in cyberspace. Thus, rather than property rights taking precedence over privacy, this section will argue that the three rights in question – privacy, property, speech – should be equally valued and protected, rather than treated as stand-alone regimes.

An adequate starting point, then, is to reexamine copyright's relationship to privacy. Indeed, the great irony of this situation is not the intractability of the conflict between privacy and intellectual property in cyberspace, but the inability of legislators to fashion a solution that squares with other constitutional values of property, personhood, and autonomy under the DMCA. Thus, under my proposed solution, the law would attempt to reconcile these values with copyright enforcement by creating a series of entitlements based on the need for personal protection and anonymity in the face of piracy surveillance.[430]

As this Article has suggested, piracy surveillance implicates a curious type of private ordering that merges the boundaries of private and public. While the standards governing copyright infringement, fair use, and the DMCA were drafted by Congress (and the judiciary), the actual implementation of these rules often gets left to the amorphous and decidedly variant motives of copyright owners. Moreover, in most copyright cases, the Constitution rarely makes an appearance if both parties are private, non-state entities.[431] However, under the state action doctrine, constitutional guarantees can limit the activities of a private party if the conduct in question is entwined with traditional state functions,

---

430 *See* GANDY, *supra* note 91, at 235.

431 *See* John R. Thomas, *Liberty and Property in the Patent Law*, 39 HOUS. L. REV. 569, 592 (2002).

such as education, adjudication, fire, and police protection, or if the activity is controlled or substantially facilitated by the government.[432]

For these reasons, one sees strong arguments for the idea that state action is present in almost every stage leading up to a subpoena or takedown request in the DMCA context. Congress drafted the relevant provisions, and a judicial body enforces them after a cursory examination; indeed, the unveiling of a person's identity is performed by an ISP pursuant to a court order.[433] Moreover, much of these issues seem particularly poignant in light of *New York Times v. Sullivan*,[434] in which the Supreme Court overturned a libel decision regarding a paid advertisement that criticized a Montgomery city official. The Court resolved the state action issue by concluding that "although this is a civil lawsuit between private parties, the Alabama courts have applied a state rule of law which petitioners claim to impose invalid restrictions on the constitutional freedoms of speech and press."[435]

The very same concerns that animated the *New York Times* case are relevant here. The property rights of the original copyright owner can be used to trample the copyright/fair use rights of other creators. As I have suggested, piracy surveillance involves a clear delegation to the private citizen to determine what constitutes infringement and what constitutes fair use. As a result, the DMCA creates a silent web of public and private interdependence, in which public functions are virtually ministerial, and private determinations are largely adjudicative. Given the substantial risk of strategic enforcement of infringement, the only way to balance the increasing encroachment on privacy protections is to ensure some level of hybridity between public and private enforcement.

As I have suggested throughout this piece, laws protecting intellectual property must be harmonized with other, mostly constitutional, values. Here, the Fourth Amendment could serve as a guide, particularly since its jurisprudence has

---

432 *Id.* at 593 (citing Flagg Bros., Inc. v. Brooks, 436 U.S. 149, 161-63 (1978)).

433 *See id.* at 614 (describing the delegation of enforcement authority by the patent office to private entities).

434 376 U.S. 254 (1964).

435 *Id.* at 265.

historically sought to reconcile the tension between protecting the interests of the public with individual civil liberties. Following this view, pre-Internet laws that flow from the mantle of the Fourth Amendment, such as the Privacy Protection Act ("PPA") can offer a path to follow in creating some much-needed balance between privacy and intellectual property.

The PPA requires a special subpoena when First Amendment interests in news reporting might be affected by an ongoing investigation. The origins of the PPA echo of the same concerns raised by piracy surveillance strategies today. In 1971, a demonstration at Stanford University Hospital turned into a violent clash between the participants and police. *The Stanford Daily*, a campus newspaper, managed to photograph a number of participants in the demonstration.[436] Two days afterward, it published a series of photographs of the clash between the police and the demonstrators. After it published the photographs, the police obtained a search warrant to seize material that might constitute evidence of the criminal activity under investigation.[437] Hence, at *Stanford Daily*, the police searched wastebaskets and rummaged through photographic negatives.[438] The event so incensed the employees at *Daily* that they filed suit, contending that the First Amendment barred the use of a search warrant under circumstances where the entity in question is a news gatherer not implicated in the criminal conduct. The Supreme Court disagreed with their position and held that the First Amendment was not a bar to the use of a search warrant under those facts.[439] In that case, the Court held that the Fourth Amendment did not prohibit police from undertaking searches of evidence held by innocent third parties.[440]

Congress, reacting to the Court's opinion, enacted the PPA. The PPA requires intimate judicial involvement and oversight: It provides for a special subpoena in cases where there is a danger of interference with the First Amendment interests of an innocent publisher. It also establishes a general

---

436 Mark Eckenwiler, *Applications of the Privacy Protection Act*, 8 SETON HALL CONST. L.J. 725 (1998).

437 *Id.* at 725.

438 *Id.*

439 *Id.* at 726; Zurcher v. Stanford Daily, 436 U.S. 547, 567-68 (1978).

440 *Zurcher*, 436 U.S. at 567-68.

rule preventing the search and seizure of certain types of materials, specifically called "work product" materials, intended for publication:

> "Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce . . . ."[441]

The definition of "work product" excludes contraband, fruits, or instrumentalities of crime, and the PPA actively requires that suspects of crime be treated with the same probable cause guidelines that animate the Fourth Amendment.[442] Though the PPA has not regularly been applied to Internet-related disputes, it has been successfully employed in a case where the Secret Service, with the aid of several U.S. attorneys, seized a multitude of computer-related evidence owned by the operators and users of a computer bulletin board who also published books and materials.[443]

The PPA should serve as a baseline guiding force in response to the DMCA's overreach into privacy and First Amendment expression. For the reasons I have offered, DMCA subpoenas regarding file sharers on peer-to-peer networks can raise similar constitutional concerns that can activate PPA remedies. Moreover, the PPA balances the protection of individual civil liberties with those of expressive freedom: At the outset, the law is meant to be applied in conjunction with the Fourth Amendment, which provides for basic protections of probable cause and judicial oversight for suspects of infringement.[444] These basic Fourth Amendment principles –

---

441 42 U.S.C. § 2000aa(a) (2000).

442 *See* Eckenwiler, *supra* note 436, at 728.

443 Steve Jackson Games, Inc. v. U.S. Secret Service, 816 F. Supp. 432, 440-41 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994).

444 Under the PPA, materials may not be seized unless they constitute fruits or instrumentalities of crime, if there is a danger of physical injury, or if the person possessing the material probably committed a crime. *See* E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J.L. TECH. 10, ¶¶ 63-67 (2001).

probable cause, freedom from search and seizure, protection of privacy – can and should also serve as baseline governing principles to govern private modes of copyright enforcement.

Thus, if a copyright owner wanted to determine the identity of a person who might be transmitting or downloading materials for infringing purposes, the DMCA, like the PPA, could also require a similar subpoena that raises the standard of judicial oversight.[445] This provision should track the PPA in several major respects. First, following the PPA, the DMCA could establish that it is illegal for private piracy surveillance measures to force an ISP to seize or silence expression that falls under fair use or First Amendment protection without first requesting a court order. By making immediate seizures of protected material illegal, the proposed provision would shift the cost of mistaken surveillance and silencing to the copyright owner or bounty hunter. Moreover, by raising the costs of mistaken detection, and creating greater incentives to reduce their occurrence, this provision would also ensure greater protection for fair use and First Amendment interests. Thus, the proposed amendment would require copyright owners to request a preliminary injunction or specific court order before asking an ISP to take down material, remove the subscriber's access, or disclose a person's identity. It could also provide for compensation in the event of a mistaken determination or disclosure.

Second, the DMCA, following its own notice-and-takedown provision, could provide for a requirement of notice to be given to the end user *prior* to disclosure of identity, and could provide for specific procedures to challenge the disclosure of one's identity in the event of an asserted fair use defense. Some may argue that the outcome of *Verizon* accomplishes many of these goals by essentially requiring the filing of actual litigation prior to disclosure of the alleged infringer's identity. Yet, I would recommend that future courts go further than the *Verizon* court did, by also integrating the DMCA subpoena procedure with a constitutional concern for anonymity. Thus, just as the

---

445 Moreover, even though piracy surveillance, at present, involves private actors, a DMCA notice is signed off by a district court. Thus, state action is arguably present, from the moment of identity revelation to the moment where an ISP terminates the person's access to the Internet or disables the account and the specter of criminal copyright infringement under the NET Act could easily provoke Fourth Amendment concerns.

PPA or other "John Doe" actions require more than enough evidence to withstand a motion to dismiss, the DMCA's use of a subpoena should reflect the need for heightened standards of justification.[446] In such situations where First Amendment concerns are triggered, the DMCA could require the immediate appealability of any proposed termination of access, the use of specially trained magistrates or marshals to carry out Internet searches, and other procedures that reflect a concern for individual civil liberties and expression, instead of the unilateral goal of protecting copyright above all else.[447]

Third, it bears noting that none of the anonymity issues are particularly new in the Internet context – many courts have already dealt with the question of how to protect the anonymity of a speaker in the face of a civil suit. In defamation cases, for example, courts have continued to develop methods to integrate First Amendment protections of anonymity with the need for legal resolution. Those methods easily apply to the DMCA subpoena provision. In one such case, for example, the New Jersey Superior Court set forth a stringent test for the disclosure of one's identity, requiring the following elements:

> [T]he trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notification efforts should include posting a message of notification of the identity discovery request to the anonymous user on the ISP's pertinent message board.
>
> [Second, t]he court shall also require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech.
>
> [Third, t]he complaint and all information provided to the court should be carefully reviewed to

---

446 *See* Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

447 *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 806 (1994).

> determine whether plaintiff has set forth a prima facie cause of action . . . . [and] must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure . . . .[448]

Applying this test (the *Dendrite* test), if the plaintiff has presented a valid cause of action, the court must balance the First Amendment right of anonymous free speech against the strength of the prima facie case presented, and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed. The nature of this inquiry is therefore both substantive and procedural, but enables the speaker to remain protected from anonymous disclosure for spurious reasons.

The solution I have outlined accomplishes three primary goals. First, the special subpoena provisions operate to raise the standard of proof to protect against spurious claims, and deter the "overfishing" scenario I have described in Part III. Second, the proposed burden-shifting and damage award provisions help to compensate wrongly accused infringers, thereby making piracy surveillance and meritless accusations more costly.[449] Finally, there is another reason for the adoption of this test in piracy surveillance scenarios: the need to raise the standard of proof in DMCA subpoenas after *Verizon*. Traditional "John Doe" lawsuits require the presentation of enough evidence to withstand a motion to dismiss, whereas the *Dendrite* test goes a step further by requiring an additional level of scrutiny. The court observed that in cases that implicate First Amendment rights to anonymity, "application of the motion-to-dismiss standard in isolation fails to provide a basis for an analysis and balancing of Dendrite's request for disclosure in light of John Doe No. 3's competing right of anonymity in the exercise of his right of free speech."[450] Under the *Dendrite* test, those suspected of copyright infringement or other illegal acts would not receive extra protection behind the shield of anonymity, but

---

448 *Dendrite*, 775 A.2d at 760.

449 In this way, these procedures reflect similar concerns that are also governed by Federal Rule of Civil Procedure 11, which requires a lawyer to make a reasonable inquiry into the factual and legal grounds of any filed document. *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 586-91 (6th ed. 2003).

450 *Dendrite*, 775 A.2d at 770.

would receive an additional recognition of the need for actual (rather than asserted) proof to unmask potential infringers.

By raising standards of proof for copyright infringement, ensuring judicial enforcement, as well as the cost of mistaken detections, courts and legislators can aim to strike a much-needed balance between property, speech, and privacy. There must be greater public and administrative oversight over piracy surveillance. To allow private parties to circumvent constitutional safeguards in order to silence others' speech is precisely what the DMCA provisions were designed to prevent. Consequently, more process – a higher standard of proof, more judicial scrutiny, and the use of special subpoenas that embrace First Amendment values – is due. The answer is more regulation over surveillance, not less, and more judicial recognition of the value of anonymity to the marketplace of speech.

One may argue that these solutions are still somewhat narrow in the sense that they protect the anonymous speaker alone, and fail to address the other types of monitoring I have addressed that involve DRM and interference. As I have shown, piracy surveillance also, problematically, unilaterally permits private copyright owners to interpret the rules governing copyright and to prevent their violation.[451] Yet while the private copyright industry may be in the best position to invest in the technology to guard against and detect infringement, courts, not private entities, are in the best position to determine actual liability. To resolve these difficult scenarios, I propose the institution of alterations to the DMCA that seek to clarify the standard of fair use and help to ensure its protection from intrusion or evisceration by extrajudicial forms of surveillance. Here, the DMCA could also be revised to specify protection for the downloading of files containing small portions of copyrighted material (e.g., samples or film clips); or files exchanged for educational purposes; or even those that involve space shifting, commentary, parody, satire, or other purposes that have not yet

---

451 *See also* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1021 (1996) (suggesting that the public/private distinction that forms the basis of the state action doctrine is particularly problematic as applied to copyright law).

been expressly clarified for protection in the technological context.[452]

Clarification of the scope of fair use in such contexts is necessary for several reasons. First, clarification helps to provide notice to future individuals of allowable activities in the face of new technologies, and it helps to clarify the many "grey areas" that often arise in difficult cases, like those listed above. This reduces the likelihood that individuals will engage in overcompliant behavior and avoid exercising their rights of freedom of speech and fair use. Second, clarification also enables *all* parties to recognize the importance of protecting an individual's entitlement to fair use in the face of technologies that may impede or prohibit it. It forces individual manufacturers to carve out certain areas for allowable uses, and allows the individual to engage in those uses without risking liability. Third, it also helps to reduce the power, significance, and scope of extrajudicial determinations. By ensuring that certain activities remain protected for fair use purposes, private copyright owners will be prevented from defining for themselves what constitutes fair use, and will instead be forced to ask a court to make a particular determination when needed.

Finally, defining the scope of fair use under the rubric of greater public oversight also advances the goal of due process.[453] As this Article has suggested, piracy surveillance implicates serious due process concerns, particularly in the scenarios that I have outlined here: the risk of error is exceptionally high; the likelihood of strategic, spurious enforcement is similarly pronounced; and the standard to protect individuals from unwanted surveillance or extrajudicial determinations is exceptionally low. Moreover, the reach of piracy surveillance extends beyond actual copying of an existing work in its entirety, and could potentially reach the full gamut of expression on the Internet that implicates fair use of copyrighted works (like text files that use titles that correspond to copyrighted works, or written text that builds on prior

---

452 *See* Julie Hilden, *Should Universities Crack Down on File Swapping?*, *at* http://writ.news.findlaw.com/hilden/20030304.html (Mar. 4, 2003).

453 Traditionally, due process principles require courts to balance the government's interest in using the procedures at issue, the risk of error in those procedures, and the private interest that is affected by the challenged procedures. *See* Matthews v. Eldridge, 424 U.S. 319, 334-35 (1976).

references). In short, the DMCA provisions govern much more than piracy – they govern the very essence of speech itself. As I have suggested, however, by clarifying the scope and entitlement of fair use, and by precluding extrajudicial determinations, we can come to a greater balance between privacy, property, and protection of expression.

V. CONCLUSION

In this Article, I have argued that our need to expand intellectual property protections must be reconciled with the existing protections for informational privacy and personal expression. As this paper has argued, it is imperative that we begin to restore the fragile balance between property rights and privacy protections by creating parity between real place and cyber space. If we fail to strike the proper balance between intellectual property rights and privacy, our constitutional values of freedom of speech, the "inviolate personality," and due process—may be sacrificed.

As this Article has suggested, both the protection of privacy and intellectual property are in crisis in cyberspace, permitting one to erode protections for the other. Unfortunately, rather than resolving the conflict between privacy and property, the law has created an entirely disparate and hierarchical regime favoring the expansion of property rights at the expense of consumer privacy and permitting growing incursions into personhood, autonomy, and the expressive expectations of consumers. As I have suggested, the only way to resolve these tensions is to return to the values that animated the letter and spirit of our constitutional protections, and attempt to use those values to return some desperately needed balance to the relationship between privacy and intellectual property.

In sum, this paper has sought to reconfigure our understanding of intellectual property so that it comports with our long-established traditions of protecting individual autonomy, privacy and expression. In doing so, we can come to a greater understanding of the need for limits on the power of intellectual property to govern our everyday lives, and the need for a more nuanced understanding of how the expansion of property rights can deleteriously affect the prosperity of privacy in cyberspace.