July 15, 2003

Draft-in-progress—Please do not quote, cite, or circulate without permission

Privacy vs. Piracy

Sonia K. Katyal*

Introduction

A massive change to cyberspace is set to happen. Instead of the relative anonymity that has characterized the online world, the most sacred areas of personal information are about to be exposed. This fundamental change in the nature of cyberspace is being driven by commercial interests, and in particular, the music industry. The opening salvo in this battle was fired in late July of last year, when 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."[1] Verizon, citing consumer privacy concerns, refused to provide the information, and the RIAA filed suit under the Digital Millennium Copyright Act (DMCA), amidst a flurry of media attention.[2] The upshot of the *Verizon*

* Associate Professor, Fordham University School of Law. The author would like to thank to the participants at the Fordham Workshop series, in addition to Jonathan Barnett, George Conk, Dan Capra, Jill Fisch, Hugh Hansen, Robert Kaczorowski, Neal Katyal, Thomas Lee, Joel Reidenberg, and Esther Lucero; and John Farmer, Allison Schilling, and Susan Cordaro for extremely helpful research assistance. Financial support was generously provided by Fordham Law School.

[1] Brief for RIAA at 1, *In re* Verizon Internet Services, Inc., 240 F.Supp.2d 24, (D.D.C. 2003).

[2] 17 U.S.C. § 512 (2000).

lawsuit is a decision that exposes the tension between protecting consumer privacy and intellectual property. 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."[3]

A few years ago, it seemed quite fanciful to imagine a world where intellectual property owners—record companies, software owners, publishers--were capable of invading the most sacred areas of the home in order to track, deter, and control uses of their products. And yet, today, it appears that the unthinkable, once a faraway risk, is swiftly taking place.[4] In recent months, private strategies of copyright enforcement have rapidly multiplied, each strategy more invasive than the last. Today, the 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.[5] Many schools, responding to threats from the RIAA, have implemented monitoring and searching programs throughout networks to track and report the exchange of copyrighted files.[6] A few have even decided to audit and actively monitor files traded by their students on the RIAA's request.[7] Yet, rather than responding to the increasingly invasive spectre of intellectual property enforcement, the legislative response has been equally misplaced: last session, there were proposals before Congress which placed intellectual property owners in a virtually unrestrained position of authority over ordinary consumers.[8] Just days ago, Senator Orrin Hatch proposed destroying the computers of individuals who illegally download material, pointing

---

[3] Chris Marlowe, *RIAA, Verizon Tiff revolving around Customer Privacy*, HOLLYWOOD REP., August 22, 2002.

[4] Just days after the attacks of September 11, 2001, lawmakers assembled a proposed list of anti-terrorism devices, which, taken collectively, herald a drastic erosion of privacy in cyberspace. One of the proposed provisions, for example, made it possible for ISPs to identify "computer trespassers"—individuals who downloaded MP3s, for example, or who otherwise violated the terms of their Internet Service Agreement—for federal monitoring of their computer activities. USA Patriot Act of 2001, Pub. L. No. 107-56, § 217, 115 Stat. 272, 291. *See also* Declan McCullagh, *Bush Submits His Laws for War*, WIRED NEWS (September 20, 2001), *at* http://www.wired.com/news/politics/0,1283,47006,00.html; Heather Jacobson & Rebecca Green, *Computer Crimes*, 39 AM. CRIM. L. REV. 273, 279-88 (2002) (describing changes to federal criminal computer laws in light of the Patriot Act); Steven J. Osher, *Privacy, Computers and the Internet*, 54 FLA. L. REV. 521, 539 (2002); and H.R. 5211, 107th Cong. (2002).

[5] See Part II.

[6] *See* Leonie Lamont, *Firms Ask to Scan UniversityFiles* , THE SYDNEY MORNING HERALD, February 19, 2003, at 3.

[7] Id. Just a few months ago, the RIAA took a further step: it filed suits against four college students accused of copyright infringement. See *RIAA Sues College File Traders*, WIRED NEWS (April 3, 2003), *at* http://www.wired.com/news/technology/0,1282,58340,00.html.

[8] Representative Howard Berman, for example, introduced a bill in 2002 that would exempt copyright owners from computer fraud laws if they target infringers using measures such as interdiction, decoy, and file-blocking to disrupt file-sharing. Another congressman, Republican John Carter recently suggested that jailing college students for piracy would deter other infringers, observing, "What these kids don't realize is that every time they pull up music and movies and make a copy, they are committing a felony under the United States code," Carter observed. *See* Katie Dean, *Marking File Traders as Felons*, WIRED NEWS (March 19, 2003), *at* http://www.wired.com/news/business/0,1367,58081,00.html (quoting Representative Carter).

out that damaging someone's computer "may be the only way you can teach somebody about copyrights."[9]

Clearly, the war over copyright has taken a new turn. The irony, of course, is that both areas of law—intellectual property and privacy--are facing enormous challenges because of technology's ever-expanding pace of development. Yet, courts often exacerbate these challenges by sacrificing one area of law for the other—by unilaterally eviscerating time-honored principles of informational privacy for the sake of unlimited control over intellectual property. The motivation behind these activities may lie in the protection of copyrighted works, a laudable goal, but the end result sacrifices the most valuable aspects of cyberspace itself.[10]

As a result, we are approaching a world in which our usage of cultural products will become increasingly and resoundingly confined by the panoptic gaze of their owners. And this outcome is not solely attributable to the development of peer-to-peer technologies, as some might suggest, but rather, 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. To date, courts have applied territorially-based doctrines with wooden precision, completely failing to notice how--or why—the nature of cyberspace makes a difference. As a result, intellectual property owners have found themselves largely unconstrained in cyberspace: empowered by courts and legislators, copyright owners can now undertake an unprecedented degree of control over cultural products through the guise of piracy detection.

How could this transformation occur so quickly, and so silently? The answer is simple. Right now, there is a prescient need for a theoretical reassessment of the relationship between the protection of property and privacy in cyberspace. While both areas of law have enormously rich and well-developed areas of scholarly work and doctrinal support, their interactions, particularly across the Internet, have been underappreciated by scholars. For property rights in real space—as social, legal, political, and economic institutions--assume a complementarity, or at least a mutually separate coexistence, with the protection of privacy.

Yet today—the use (or misuse) of digital intellectual property in the widely ungovernable realm of cyberspace has shattered the once-respectful coexistence between privacy and property, signaling its increasingly contested terrain. The Internet has created a broadcast media that is permeated with both private and public spaces, each filled with potential for creativity and communication, and yet is

---

[9] Ted Bridis, *Senator Takes Aim at Illegal Downloads*, ASSOCIATED PRESS (June 18, 2003).

[10] *See* Jane Black, *Finally, A Fair Fight with Big Music: Telecom Giant Verizon is Battling the Industry's Bid to Make it Name a File-Sharing Subscriber. It's also defending your right to privacy*, BUS. WK. ONLINE, September 12, 2002 (stating, "If the RIAA wins this legal skirmish, as it has so many others over the last three years, the Net will fundamentally change.").

permeated with lawlessness, particularly where the protection of intellectual property is concerned. As a consequence, the law has unwittingly invited intellectual property owners to cast an increasingly wider swath of private enforcement over the online activities of ordinary citizens, leading to a host of invasive self-protective measures from intellectual property owners that I call "piracy surveillance."

In the past, legislators and scholars have placed their attention on other types of surveillance relating to employment, marketing, and national security.[11] Yet piracy surveillance is completely distinct from these other types, and remains incompletely theorized, technologically unbounded, and, potentially, legally unrestrained. 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 enforcement of copyright; and third, to suggest some ways that the law can 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 for 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 second, it enables a private regime of copyright enforcement that, thus far, compromises individual rights involving privacy, expression, and due process that most citizens enjoy from state-sponsored invasion.

Currently, it is unclear how defenders of privacy will respond to these trends. For the nature of cyberspace has offered us a world that yields clashing conceptions of the proper relationship between property and privacy: we are transfixed by these competing descriptive and normative visions of the meaning and function of each, just as we are bemused by their increasing evanescence in cyberspace. Towards that end, 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 challenges posed by modern technology.

Consequently, 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 destablized a preexisting balance between privacy and property by eliminating the material conditions that permit the exercise of spatial privacy. Unlike ownership in real space, which presupposes a degree of privacy by virtue of material

[11] David Lyon, *The World Wide Web of Surveillance: The Internet and Off-World Power Flows*, from INFO., COMM. & SOC'Y, at 91-105 (asserting the proliferation of three main categories of cyberspace surveillance relating to employment, to security and policing, and to marketing).

seclusion, the public and private nature of property in cyberspace often comes into conflict with one another, interacting within a sphere of confusing uncertainty.

Nowhere is this best illustrated than in the context of peer-to-peer transmissions, which has 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, as well. By making one's online activities, identities, and preferences transparently visible, peer-to-peer frameworks also 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 of ways in which private entities have successfully monitored transmissions in cyberspace to control uses of their copyrighted materials. Following the DMCA, I argue that *Napster* has unwittingly facilitated the creation of a private regime wherein owners engage in self-help surveillance of consumer activities. 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 copyrighted material; *management*, which involves a host of actions taken in real space and cyberspace to limit certain uses of cultural products; and *attack*, which involves a degree of preventative actions taken to disable 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 authors and creators are essentially monitored by third parties for the infringement potential of their activities. 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 *all* cultural products in cyberspace, both illegitimate and legitimate. This has occurred in three primary ways: first, piracy surveillance overdeters the risks of copyright infringement, affecting both the consumer expression and fair use of non-offenders; second, piracy surveillance forces ISPs to monitor and record the activities of their subscribers, thereby affecting the autonomy, anonymity, and privacy individuals enjoy in cyberspace; and third, piracy surveillance affects an individual's ability to access information without government interference.

In the fourth section, I argue that the law must restore a critical balance between copyright law and civil liberties. Private methods of copyright enforcement cannot be used to displace and circumvent constitutional values. Along those lines, I suggest that the Digital Millennium Copyright Act—and copyright law generally--must be reinterpreted to square with principles of privacy, personal autonomy and fair use that flows directly from our constitutional tradition. The answer, then, favors a greater

hybridity between private and public copyright enforcement. Towards that end, I argue in favor of greater judicial oversight over the DMCA, and offer a potential solution that is derived from the Privacy Protection Act, which adequately balances protections for freedom of speech and privacy with the interests of law enforcement. In short, rather than justifying a hierarchy of property over privacy, this paper suggests that the law must step in to regulate the balance between copyright and civil liberties that our Founders originally intended.

Part I: A Dialectical Relationship Between Privacy and Property

For the most part, scholars who write about the relationship between privacy and property have concentrated on the proprietary aspects of privacy, arguing that privacy originated as a type of property right. Yet at the same time, in their endless zeal to uncover the proprietary underpinnings of privacy, they have often failed to grapple with the conceptual richness of the reverse proposition: the privacy-ensuring dimensions of property ownership. While both property and privacy protect different interests, they enjoy a mutually reinforcing relationship that has been historically validated by the law governing real space.

Things dramatically change, however, when one enters the intangible domain of cyberspace. As this section will argue, 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. This section will therefore describe how cyberspace transforms the nature of property, and demonstrates how these transformations are inextricably linked to informational privacy.

A. Real Space: Some Basic Points on the "Private" Nature of Property Ownership

Both property and privacy have assumed venerable positions in American constitutional law. As Bruce Ackerman has pointed out, the core of both rights implicates the same abstract right: the right to exclude unwanted interference by third parties.[12] Yet while our allegiances to the protection of property are always stated outright throughout constitutional law; our commitment to privacy has been slightly more elusive. As William Blackstone has written, "[t]here is nothing which so generally strikes the imagination, and engages the affections of mankind, as the right of property; or that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe."[13] Of course, ownership implies a panoply of other

[12] See Ackerman, LIBERATING ABSTRACTION at 347.
[13] *See* Blackstone, *Commentary on the Laws of England*, Vol. 2-11 (1766), reprinted in Ellickson, et. al, eds. PERSPECTIVES ON PROPERTY LAW 37 (1995).

rights, by enabling an owner to consume her 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.[14] Private property is sacred; it is the critical element that ensures human self-actualization.

At the same time, the panoply of different rights enjoyed by property owners also rests upon another, crucial facet of self-actualization: the protection of privacy. In real space, tort, trespass, and contract law exists to ensure that individuals remained respectful of each others' private spaces, even when they involved a third-party's self-protection of real or personal property. Property ownership itself confers a certain measure of privacy, and privacy rights derive their judicial force from the same array of *Lochner*-era cases that also established a right to property.[15] Yet curiously, to the extent that any relationship between privacy and property has been mentioned, it has mostly been presumed.[16] For example, in his treatise *Of Property*, written in the last decade of the seventeenth century, John Locke observed that, "Though the Earth and all inferior Creatures be common to all Men, yet every Man has a Property in his own Person. This no Body has any right to but himself."[17] 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, suggesting that protection of bodily privacy also involves a metaphor of ownership.[18]

Adding to this, Locke also powerfully recognized that property rights should extend to the products of one's labor; "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.[19] 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.[20] Because of the intermingling of her labor with these objects, she may be said to have obtained a "property right" in the objects themselves.[21] In turn, others have a duty to restrain themselves from gathering the fruits of her labor and

---

[14] *See* Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1530, 1608 (1993).
[15] *See* Radhika Rao, *Property, Privacy, and the Human Body*, 80 B.U. L. REV. 359, 418 (2000).
[16] Carol Rose, *Possession as the Origin of Property*, 52 U. Chi. L. Rev. 73-88 (1985).
[17] Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 14, 26-28 (1996).
[18] See Rao, 80 B.U. L. Rev. at 422.
[19] *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 "labor 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.").
[20] Gordon, *supra* note 19 at 1544-45.
[21] *Id.*

to leave these objects alone.[22] Under this formulation, Locke considered 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.[23]

Thus, just as the term 'private property' suggests, both property and privacy enjoy a symbiotic relationship: every person enjoys a property right in her person, just as she enjoys the right to exclude others from treading or trespassing on her privately owned property.[24] 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.[25] Property rights confer a certain amount of spatial sovereignty in the property owned,[26] 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."[27] 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.[28]

Citing this passage, Professor Radhika Rao has asserted that precisely the same observation could be made regarding the right of privacy.[29] She observes that the right to property, like privacy, decentralizes decision-making power by placing it into the hands of owners, thereby policing "the fragile boundary between individual autonomy and government authority."[30]

---

[22] *Id.*

[23] 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. 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] *See* Waldron, supra note 23 at 158.

[25] See Rao, 80 B.U. L. Rev. at 425.

[26] Scholars also cite this passage for the concept of defining the body as property. *See, e.g.*, RUSSELL SCOTT, THE BODY AS PROPERTY (1981).

[27] Rakas v. Illinois, 99 S.Ct. 421, 430 (1978).

[28] Charles A. Reich, *The New Property*, 73 Yale L.J. 733 (1964).

[29] Rao, 80 B.U. L. Rev. at 419.

[30] Id.

However, while the ownership of property is inextricably linked to spatial considerations of privacy and autonomy,[31] the two do not always share a perfect correspondence. Property rights, for example, protect an owner's autonomy over that which is owned, whereas privacy safeguards the exercise of autonomy itself.[32] Property rights support market relationships, whereas privacy supports more spiritual ones.[33] And, as Julie Cohen has emphasized in a recent paper, not every invasion of a residential property interest is an invasion of privacy, offering the example of a nuisance like excessive noise or noxious fumes. Likewise, some individuals may have privacy expectations in places that they do not own or rent, like dressing rooms, restrooms, and telephone booths.[34]

These questions become further complicated when we turn to intellectual property, which poses a host of interesting variations regarding the relationship between property and privacy.[35] For one thing, intellectual property lacks the "thinglike" tangibility of real property; thus, architectural elements like borders and fences have different capabilities when they are protecting information, rather than tangible goods.[36] While seclusion of property can be created, it isn't always necessary. Thus, in some circumstances, privacy can be more important, or less important, depending on the type of intellectual property in question. For example, privacy may be less important for owners of communicative properties that are expressive in nature, i.e. books, music, software, and other forms of digital content. In contrast, privacy may be very important for an owner of a trade secret, because the value of the information stems from its seclusion. And, in the case of database collections of personal information, there is an additional twist: the *subject* of the information might desire privacy, even if the collector, or owner, of the information does not.

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. Yet, despite these differences within the two-sided relationship between privacy and property, both entitlements are equally necessary in the law: one cannot exist without the other. 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

---

[31] Consider the Court's formulation of the relationship between property and privacy in *Griswold*, where it observed "Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship." 381 U.S. 497, 548 (1961). Here, the Court derived the protection of individual autonomy from notions of spatial privacy.
[32] See Rao, 80 B.U. L. Rev. at 429.
[33] Ackerman, LIBERATING ABSTRACTION at 347.
[34] Cohen, *DRM and Privacy* at 2 (draft on file with author).
[35] 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.
[36] Wendy Gordon, *An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory*, 41 STAN. L. REV. 1343, 1378-84 (1989).

property.[37] For example, there is no specific constitutional right to privacy, informational or otherwise.[38] Cases like *Griswold* and *Roe* postulated a substantive type of privacy that is thought to be a "right held against the state's power to legislate,"[39] 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 reticent to extend the same rationale to the protection of informational privacy, drawing a firm line between informational and substantive privacy. In the late 1970s, for example, the Supreme Court dealt with the question of whether the collection, storage and dissemination of information in government databases in *Whalen v. Roe* implicates a constitutional right to privacy.[40] At issue in the case was whether the state-sponsored collection of names and addresses of persons who had various prescriptions violated a constitutionally protected "zone of privacy."

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 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

---

[37] 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).

[38] Instead, the Supreme Court has developed a limited, "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).

[39] *See* 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) (stating, "privacy involves a struggle to control information. Personal privacy is one's desire, right, or ability to control, withhold, and reveal at will information about one's person and activities."); and Jed Rubenfeld *The Right to Privacy*, 102 HARV. L. REV. 737, 748-50 (1989).

[40] 429 U.S. 589, 605 (1977). *See* Francis S. Chalpowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 145-50 (1991); 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 informational privacy").

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."[41] 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.[42] However, since the New York statutory scheme 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.

As the following sections will point out, the unanswered question left open in *Whalen*—that is, whether there is a constitutionally protected right to informational privacy—is the very question that animates the relationship between intellectual property and privacy in the digital age.[43] Instead of definitively providing an answer to this question, the law has opted to confer property rights on third parties who collect such information for commercial purposes, rather than to create a comprehensive scheme to protect individuals from unwanted surveillance. As the next sections will describe, the absence of effective protections for informational privacy has spawned the explosive growth of private strategies of consumer surveillance, permitting intellectual property frameworks to grow stronger and more expansive, and privacy protections to become substantially weakened as a result.

B. Rethinking Property in Cyberspace

Property in cyberspace is almost always wholly intangible in nature, thus, the material 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. Writing on the future of the Internet, John Perry Barlow triumphantly declared, "legal concepts of property, expression, identity, movement and

---

[41] *Whalen*, 429 U.S. at 605.

[42] *Id*. *See also* SOLOVE AND ROTENBERG, INFORMATIONAL PRIVACY 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).

[43] 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 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 AND ROTENBERG, *supra* note --, at 191 (citing Smith v. City of Artesia, 772 P.2d 373, 376 (N.M. Ct. App. 1989) (observing its resemblance to common law prohibition against unreasonable publicity)).

context do not apply to us. They are based on matter. There is no matter here."[44] As Barlow's powerful rhetoric suggests, the nature of both property and identity have become transformed by their intangible, evanascent 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.[45] Cyberspace is often characterized in terms of "private" and "public" spaces: some parts of the Web are public, as are many chatrooms, whereas email is private.[46] The law, too, has embraced this temptation: recent case law is replete with examples of territorial metaphor, as well.[47]

On one hand, our 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.[48]

Yet the nature of cyberspace also ushers 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

---

[44] John Perry Parlow, *A Declaration of the Independence of Cyberspace*, *in* CRYPTO ANARCHY, CYBERSTATES, AND PIRATE UTOPIAS 27 (Ludlow ed., 2001).

[45] See Dan Hunter, Cyberspace as Place and the Tragedy of the Digital AntiCommons, 91 Cal. L. Rev. 439, 453 (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.

[46] Hunter, 91 Cal. L. Rev. at 454.

[47] See Hunter, 91 Cal. L. Rev. at 480-493.

[48] See Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-65 (1999);and Natalie L. Regoli, *A Tort for Prying Eyes*, 2001 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."). According to Lawrence Lessig, two elements characterize traditional privacy considerations: the "monitored" and the "searchable." The monitored refers to "the part of one's life that is watched," that is, the regular or persistent watching of people or machines, irrespective of whether the activities are considered public or not. However, the searchable refers to "the part of one's life that leaves…a record," which comprises both the technologies of searching and the legal protections against the use of such technologies. While the monitored is transient and erasable from memory, the searchable establishes a permanent record largely available over time and therefore deserving of some protection.

others, but also subject to a great degree of surveillance. Put another way, the Internet portends 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.

Consider the illusory power of near-perfect anonymity. Cyberspace allows for a level of anonymity that is practically impossible to procure in real space. This ability to shield one's identity, in turn, allows for the creation of a kind of intellectual property that is permeated with and infused with anonymity as a precondition for creative possibility. Perceptions of anonymity in cyberspace have enabled a level of participation in public discourse unlike anything before; allowing similar individuals with limited financial resources to "publish" information and opinions on matters of public concern.[49] The stronger 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. 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."[50] 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.[51] In other words, virtual space allows individuals to construct identities they choose for themselves, rather than the ones they are born with.[52] This ability to adopt transitory and multiple identities is at the heart of cyberspace's limitless possibility.[53]

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.[54] Yet today, the perception of informational privacy extends, at least in cyberspace, to something quite different: it covers the very act of creating fictive personalities, in addition to the possibility of anonymously publishing information online. Suppose person Y chooses to open an email account under an assumed name, and with that identity--surf the Web, make purchases, sign on to listserves, 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,

---

[49] *See* Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 861 (2000).
[50] 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 177 (1995).
[51] *Id*. at 212.
[52] *Id*. at 226, 240.
[53] 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).
[54] Philip E. Agre, *The Architecture of Identity*, INFORMATION, COMMUNICATION & SOCIETY, at 1-25, 3 (1999).

shopping habits, web searches—are all "private" in the sense that she might prefer them to be secluded from public knowledge.

Since the law confers property rights over profiles of consumer information to collectors, rather than the individual subject herself, it creates substantial incentives for surreptitious monitoring of consumer activity.[55] 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.

Consider, for example, the collection of clickstream data: here, the increasing commodification of such information can often create incentives that result in serious invasions of personal information, often without the knowledge of individual subscribers. The best example of this, particularly in the Internet context, is a recent case involving "cookies," which are small text files placed into personal computers by Web sites that can be used to identify a specific computer and possibly the user herself to create personalized marketing information.[56] DoubleClick is a company that uses this technology.[57] Every time a user 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.[58]

In *DoubleClick*, the plaintiffs contended that DoubleClick's cookies collected information that Web users considered to be personal and private information—including a user's name, email address, home and business addresses, telephone number, searches performed, and DoubleClick affiliated Web sites visited.[59] Consequently, a number of plaintiffs filed suit in federal court under federal and state law, alleging that DoubleClick violated the Electronic Communications Privacy Act (ECPA), the Federal Wiretap Act, various state laws governing privacy, and common law invasions of privacy and trespass to property in its ongoing collection of consumer information.

Here, the court used the rhetoric of property to displace the importance of privacy in rejecting each of the plaintiffs' claims, marking the first time a court dealt substantively with surreptitious online

---

[55] *See also* Shibley v. Time, 341 N.E. 2d 337 (1975); and *In re* DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d 497 (S.D.N.Y. 2001).
[56] Seth R. Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, 607 PLI/PAT 141, 144 (2000); Matthew C. Keck, *Cookies, the Constitution, and Common Law: A Framework for the Right to Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 88-93 (2002).
[57] *See In re* DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d 497 (S.D.N.Y. 2001).
[58] Seth R. Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, 607 PLI/PAT 141, 144 (2000).
[59] *In re DoubleClick*, 154 F.Supp. 2d at 503.

consumer surveillance. It concluded that an individual's personal identifying information is the property of the company that harvests it, not of the consumer.[60] Moreover, the court reasoned that the site visitation itself suggested consumer consent over such monitoring.[61] It 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 state law.[62] Finally, and most significant, the court suggested that the presence of profit motives or commercial customs could immunize trespass of a person's confidential information. In other words, because the court determined that DoubleClick's motives were commercial in nature, not illegal or tortious, the plaintiffs had no evidence to raise the question of whether DoubleClick acted with a tortious purpose, and the court dismissed the claim.[63]

Such techniques of data collection are especially pernicious because they are subtle, ongoing, largely unregulated, and inextricably linked to a person's online activities.[64] But they are also important for another reason: as I will show, these methods of consumer surveillance can often provide the blueprint for strategies of piracy surveillance that I explore in the next several sections. Today, 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.[65] Web sites use "tracking software" that logs information about its users, which is then used toward a variety of purposes.[66] ISPs are capable of tracking software

---

[60] *Id*. at 510-11. *See also* Alexander H. Burke, *Information Harvesting on the Net*, 14 LOY. CONSUMER L. REV. 125, 134 (2002); and *see* Chance v. Avenue A., Inc., 165 F. Supp.2d 1153, 1160 (W.D. Wash. 2001).

[61] The court analogized that a cookie was akin to a barcode placed on a business reply card, meaningless to the consumer, but meaningful to the company. *Id*. (noting, "bar-codes and identification numbers," like cookies, "are meaningless to consumers, but are valuable to companies in compiling data on consumer responses.").

[62] *Id*. at 514; 18 U.S.C. § 2511 (2000).

[63] *Id*. at 519 (observing, "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."). 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. *Id*. at 519-20. 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.

[64] See Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); and Jonathan Krim, *Web Firms Choose Profit over Privacy*, Washington Post (July 1, 2003) (noting that many web sites promise to protect consumer information from sale to a third party, but often rent the information instead to others).

[65] One study conducted by the FTC found that 92 percent of the 674 websites it visited collected personal information from its visitors, but 86 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 Privacy: Spinning Lies on the World Wide Web*, 18 N.Y.L. SCH. J. HUM. RTS. 609, 610 (2002) (citing *FTC Releases Report on Consumers' Online Privacy* (June 4, 1998), *available at* http://www.ftc.gov/opa/1998/9806/privacy2.htm).

[66] 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 is 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. Hall, *supra* note 126, at 616.

downloaded by individuals.[67] And 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.[68] Others use "Web bugs" which are small, invisible graphics placed on Web sites or email messages to monitor the activities of individual users.[69] 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.[70] 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.

C. Peer-to-Peer Panopticism

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. Add to this another element: peer-to-peer file-sharing programs that permit the anonymous exchange of copyrighted content from each other's hard drives. As I will show, peer-to-peer transmissions facilitate a crisis of both property and privacy in cyberspace, and often create a conflict between the two.

Generally, 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; and the central server transmits the information to the user.[71] In this model, visitors to a web site do not interact with each other.[72] Information simply passes from one entity to another, and the recipients of the information do not connect.[73] Consumers connect to the Web sites from intermittently connected PCs, which are usually at the edges of a network.[74]

---

[67] *See* Marc Waldman, Lorrie Faith Cranor, and Avi Rubin, *Trust*, in PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 244 (Andy Oram, ed., 2001).
[68] *Id*.
[69] John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval*, 39 ALBERTA L. REV. 346, 355-56 (2001) (describing the various ways third parties employe "web bugs" online).
[70] Lynn Chuang Kramer, *Private Eyes are Watching You: Consumer Online Privacy Protection—Lessons From Home and Abroad*, 37 TEX. INT'L L.J. 387, 394-45 (2002). *See also* ELECTRONIC PRIVACY INFORMATION CENTER (hereinafter EPIC), PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS, 60 (2002).
[71] William W. Fisher III & Christopher Yang [hereinafter Yang], *Peer-to-Peer Copying*, (November 18, 2001), *at* http://cyber.law.harvard.edu/ilaw/P2P.html, at *Introduction*.
[72] *Id*.
[73] *Id*.
[74] Clay Shirky, *Listening to Napster*, in PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 35 (Oram ed., 2001).

This form of client-server web architecture, predicated on hierarchical principles, has yielded extremely successful ISPs, which serve clients from servers always connected to the Internet.[75] Over time, a few of these privileged servers, serving millions of clients, have increasingly dominated the Internet.[76] This model works for almost all content, from streaming videos to interactive games to online shopping.[77] As a result, ISPs have become a relatively new form of governance in cyberspace because they maintain a substantial amount of private, consumer information regarding users' online activities, and they often transmit the requested information.[78] 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.[79] A peer-to-peer model creates a mode of communication that treats each machine as a separate and equal entity in the sharing of information.[80] This model enables individual computers to interact with one another by making it possible for one computer to "ask" other computers for a specified type of file.[81] Each computer then forwards the request to a second tier of computers, which in turn forward the request to a third tier, and so on.[82] When the requested file is located, it is automatically transmitted to the original user.[83] In this manner, peer-to-peer fragments transform each node on the network into both client and server, allowing

---

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

[76] Nelson Minar & Marc Hedlund, *A Network of Peers*, in PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 3 (Oram, ed., 2001).

[77] Id at 9.

[78] *See* SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (hereinafter, SIIA), STRETCHING THE FABRIC OF THE NET: EXAMINING THE PRESENT AND POTENTIAL OF PEER-TO-PEER TECHNOLOGIES 3 (2001) (observing "[w]hatever entity controls the central server also controls the information—a valuable commodity.").

[79] *See* Minar, *supra* note 76, at 3. There are three main categories of peer-to-peer systems, centrally coordinated, hierarchical, and decentralized. *Id.* In a centrally coordinated system, a central server, like Napster, mediates coordination between peers. See note ---. A *hierarchical* peer-to-peer system organizes peers into different hierarchies, and a local coordinator mediates communication between one group of peers. *Id.* 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.*

[80] *Id*. at 4.

[81] Yang, *supra* note 71, 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 74, at 22. *Id.*

[82] Yang, *supra* note 71, at *Introduction*. As one commentator explains:

> Before peer to peer, if you wanted to serve files from your PC you needed a permanent IP address, domain name, registration with DNS servers and properly configured Web server software on the PC. With peer to peer technology your computer storage, cycles and content are made available because the PC via modem becomes a node that operates outside the DNS [domain name] system, having significant autonomy from central servers with the ability to be accessed by other users. . . .At its simplest peer to peer creates an alternate file trading channel to the Web or a black market where what is traded is "free" but users of the network are subjected to shared codes of conduct.

Id.

[83] Kathy Bowrey and Matthew Rimmer, *Rip, Mix, Burn: The Politics of Peer to Peer and Copyright Law*, FIRST

a file transfer (or download) to be performed by a direct connection between both users, instead of through a single channel. [84]

Although peer-to-peer frameworks seem deceptively simple, their implications, both legally and socially, are extraordinarily complex, signaling, for some, the end to the efficacy of protections for 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 regulated or censored in some manner.[85] Just as peer-to-peer frameworks erase the distinction between client and server, they erase the distinction between producers and consumers of content, allowing both the author and the reader to share and exchange files without legal restraint.[86] Most intellectual property artifacts—books, music, movies, software—have a typical "flow" pattern beginning at the moment of creation with the author or creator. The next stage is publication: a work is then given to a publisher to produce and distribute. Finally, after being transferred to a retail establishment, it winds up in the hands of the consumer.

A peer-to-peer connection transforms this one-sided flow of information by making it possible for the creator to become the distributor and publisher simultaneously.[87] When an authorized distributor is no longer needed, information exchanges can be multiplied without limit. And, although music has attracted the most attention, such technology has also facilitated the illicit transmission of other types of content, including books, films, and software.[88] 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.[89]

Peer-to-peer networks, however, also create a crisis of privacy as well as property, because they potentially transform the boundaries between public and private. Indeed, from both an architectural as well as a philosophical perspective, peer-to-peer networks bear a potent similarity to a favorite metaphor throughout privacy discourse, Jeremy Bentham's 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

---

MONDAY, Issue 7, September 2002, *at* http://www.firstmonday.dk/issues/issue7_8/bowrey/index.html, at *Part One.*

[84] Yang, *supra* note 175, at *Introduction*. *See also* Gene Kan, *Gnutella*, in PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 94-95 (Oram, ed., 2001); Minar, *supra* note 76, at 17.

[85] *See* 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).

[86] Shirky, *supra* note 74, at 35. Theodore Hong, *Performance*, PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 204 (Oram, ed., 2001)..

[87] For this reason, peer-to-peer has been hailed as an artist's dream—because it allows artists to market their products directly to the consumer without the need for external management and intervention.

[88] In most "true" or decentralized peer-to-peer frameworks, the absence of a central server makes many of these programs virtually impossible to regulate, and constantly changing. Kan, *supra* note --, at 97.

[89] Yang, *supra* note 71, at *Introduction*.

of "conscious and permanent visibility that assures the automatic functioning of power."[90] The panoptic design, first mentioned by Bentham and then further developed by the French philosopher Michel Foucault, applied to many different types of disciplinary surveillance, including rehabilitation or education.[91] Its primary effect, however, involved a process in which individuals internalized the overseeing gaze of authority figures, and then eventually disciplined their behavior to comport with expectations of these figures, irrespective of whether or not they were actually present and watching at the time. As Daniel Solove commented, "[b]y 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 monitored but because of their fear that they could be watched. This fear alone is sufficient to achieve control."[92]

Panoptic architecture ensures perfect order and obedience by *suggesting* the continuous presence of authority, even if actual surveillance is not always present. The mere possibility of being watched facilitates compliance, rather than the continuous presence of enforcement. Moreover, the panoptic design, for Foucault, divided ordinary individuals into those who conformed their behavior with prescribed expectations and those who did not.[93] The more subjective ways through which an individual actively participates in transforming himself or herself into a disciplinary subject also empowers this system of classification.[94] According to Oscar Gandy, author of *The Panoptic Sort*, Foucault's observations have particular import as applied to the process of consumer surveillance because individuals willingly label themselves to identify with particular brands, products, and standards of consumption that elicit particular identities.[95] This process of "active self-formation," as denoted by both Foucault and Oscar Gandy, illustrates the power of consumer surveillance to affect the formation of human identity and expression through a three-tiered system of identification, classification, and assessment.

While the panoptic metaphor has been crucial to understanding disciplinary processes in real space, I would argue that, at least at this juncture in history, it is especially useful when applied to the effects of surveillance on the Web. In a world where individuals store more and more personal information on computers, peer-to-peer searches can become particularly intrusive, particularly since the protection of privacy depends on the strength of particular programs for their efficacy, and many

---

[90] *See* OSCAR GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 9 (1993).
[91] *Id.*
[92] Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1415 (2001)
[93] GANDY, *supra* note 90, at 10.
[94] *Id.*
[95] *Id.*

individuals often do not realize what they are sharing on line.[96] In a peer-to-peer environment, the traditional distinction between the private and the public readily collapses, leaving open a vast minefield of possibilities for invasion. Suddenly everything—communications, files, stored pictures, online activities—can be monitored, revealed and recorded at the same time. The file-sharing revolution renders certain files stored on individual computers to be potentially accessible,[97] from the most personal to the most public information, facilitating "invasion without physical invasion."[98] The identities and activities we adopt in cyberspace can become transparently visible, compromising privacy discussed in the previous section in cyberspace. 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. Consequently, the possibilities for informational gathering are enormous, irrespective of who authorizes or initiates the investigation.

Yet there is a crucial difference between panopticism in real space, as compared to panopticism in cyberspace: anonymity. As I argued in Section I, many individuals poorly assess the risk of online surveillance and continue to engage in online activities without realizing the risk of exposure.[99] In a word, people have no idea what they are sharing online, and with whom. In these circumstances, the law rarely steps in to validate consumer expectations. To illustrate this point, consider this case, which illustrates how swiftly the act of file-sharing eviscerates Fourth Amendment expectations of informational privacy. On July 2, 1999, a customer-support specialist for Road Runner, a high speed Internet service provider 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.[100] The computer's owner had activated its peer-to-peer file sharing mechanism, which allowed others to view the images stored on its hard drive.[101] The caller gave the specialist the computer's IP address, the directory, and the file names in which the images were located.[102] Shortly afterward, the specialist located the computer with the corresponding IP address and viewed two images of a sexual nature involving children.[103]

---

[96] Adler, 105 YALE L.J. 1096.
[97] 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 78.
[98] *Id*. at 58.
[99] See Nathaniel S. Good and Aaron Krekelberg, *Usability and Privacy: A study of P2P File-Sharing*, on file with author (observing serious privacy concerns for users of p2p networks).
[100] United States v. Kennedy, 81 F.Supp.2d 1103, 1106 (D. Kan. 2000).
[101] *Id*. at 1107 n. 7.
[102] *Id*. at 1106.
[103] *Id*.

Road Runner then contacted the FBI and recommended that it obtain a court order to procure the subscriber's information.[104] The United States Attorney's Office complied and located the subscriber's home address, telephone number, email address, and general account information.[105] 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.[106] 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."[107] 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 engaging in sexual acts.[108] He claimed not to know the identity of the person from whom he had downloaded the images, and he did not think that anyone would discover he had downloaded the pictures.[109] Shortly after a grand jury returned an indictment for his arrest, Kennedy turned himself in.[110]

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.[111] Here, the court presumed that a person who shares files lacks an expectation of privacy in his personal identifying information, as well as the information shared online.

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.[112] "'What a person knowingly

---

[104] *Id*. at 1107.
[105] *Id*.
[106] *Id*. at 1107.
[107] *Id*. at 1108.
[108] *Id*.
[109] *Id*.
[110] *Id*.
[111] *Id*. at 1110.
[112] *Id*. *See also* Luna, *supra* note --, at 793-95. Under *Katz*, 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. *Id*. In analyzing the second question, the court opined that "'[t]he 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. U.S., 466 U.S 170, 181-83). By setting forth this test, the Court struck a key balance between a person's subjective and objective expectations of

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*.[113] 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:

> 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.[114]

The court's recitation of *Katz* recognizes the central role technology plays in constructing social expectations of privacy, but it also 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, even though a court might reach the opposite conclusion. In turn, these disparate expectations transform the boundaries between private and public: rather than validating a person's expectations of privacy, the law eviscerates them. As this case illustrates, it is entirely possible for an individual to possess a subjective expectation of privacy, and for a court to dismiss those expectations in light of *Katz*.[115] Complicating this further is the territorial aspect of home computer use: several cases have held that a person can have spatial expectations of privacy in the content stored on her individual computer hard drive.[116] These factors combine to promote expectations of informational privacy, even though the activities of commercial entities and law enforcement may detract from those perceptions.

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, culturally speaking, many individuals persists in retaining this combination in cyberspace.[117] The court suggested that

---

privacy:

> [W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected....One who occupies…[a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

Katz, 389 U.S. at 351-52.

[113] *Kennedy*, 81 F.Supp.2d at 1110 (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)).

[114] *Id*.

[115] Cite to Hetcher.

[116] *See* Bailey, *supra* note --, at 524-29 (discussing cases that found expectations of privacy in computer hard drives).

[117] Smith v. Maryland, 442 U.S. 735, 741 n. 5 (1979). Moreover, as *Kenned*y demonstrates, the *Katz* test offers courts little guidance when new technologies of surveillance arise. The problem in *Kennedy* could be viewed as an informational one: Kennedy might have understood that the contents of his computer were private, even if they were accessible for public viewing—and possibly did not understand how swiftly an ISP might hand over his identity to law enforcement. *See* Plaintiff's Second Amended Verified Petition, Application for Temporary Restraining Order and Temporary Injunction, Universal Image v. Yahoo, Inc., No. 99-13839-A (Tex. Dallas County Jan. 18, 2000),

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.[118] As one author observes, a person's expectations of privacy 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 their subscribers.[119] 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.[120]

In sum, the *Kennedy* case, and others like it, often highlight the troubling contradiction I identified earlier regarding perceptions of informational privacy online: individuals poorly assess the risks of transparency, leading them to expect anonymity, even when engaging in illicit activities that are open to private surveillance. Using peer-to-peer technology, a third party can view files left available on a person's hard drive, and set in motion a series of investigations culminating in her arrest.[121] This possibility of unbridled private enforcement is precisely what animates copyright protection strategies, as the next section will describe.

Part II: Spectres of Piracy Surveillance

As the prior section suggests, the seduction—and danger—of the peer-to-peer world is that it allows the widespread recreation and distribution of content such as film, music, software, and text.[122] Unsurprisingly, the potential for unauthorized transmission of these copyrighted works has led some to characterize the Internet, for better or worse, as a "pirate utopia."[123] Indeed, the term "piracy" is now

---

available at http://legal.web.aol.com/decisions/dlpriv/univtro2.pdf (last visited May 21, 2003), cited in Natalie L. Regoli, *A Tort for Prying Eyes*, 2001 J.L. TECH. & POL'Y 267, 268 (2001; Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 82-83 (2000).

[118] *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).

[119] Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 101 (2000).

[120] The test of 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).

[121] 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. *Kennedy* 81 F. Supp. at 1111-12. The court soundly rejected this argument on the grounds that the government did not know of nor acquiesce in the intrusive conduct; and Kennedy had made no showing that the government involvement was significant enough to change them into government searches. *Id*.

[122] *See supra* note -- and accompanying text.

[123] Hakim Bey, in Ludlow, supra note X, at 238.

ubiquitous throughout 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. The use of the term "piracy" to refer to the unauthorized duplication of original commercial products[124] or counterfeiting[125] dates back to 1822.[126]

Yet today, however, the term also suggests the growing power of content owners to discursively define much more expansive controls over content itself. The confused and somewhat fearful way these entities have responded to peer-to-peer file-sharing reveals a site where the growing tensions between defenders of Internet privacy and harvesters of consumer information have come to a head.[127] As this section will argue, the DMCA, coupled with *Napster*, has expanded property frameworks over cyberspace, subordinating competing values like privacy, free speech, and fair use. It has done so by gradually expanding the law to control the dynamics of web architecture, informational privacy, and anonymity, and by conferring a nearly-unlimited power to intellectual property owners to detect and defend their products against unauthorized uses. And, just as undesirably, the problem of piracy has led both public and private entities to respond even more forcefully than necessary, seeking to destroy not only the peer-to-peer networks that have sprouted across the Net, but the very boundaries of privacy and autonomy in cyberspace. As a result, intellectual property owners have created a new mode of surveillance that crosses the boundaries between commercial self-help and the prurient intrusion of personal information. As a result, in the wake of *Napster* and the Digital Millennium Copyright Act,[128] peer-to-peer file-sharing has become the new proxy for criminality.[129]

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

---

[124] Anderson v. Nidorf, 26 F.3d 100, 101 n. 1 (9th Cir. 1994) (quoting from Piracy and Counterfeiting Amendments Act of 1982, S. Rep. No. 97-274, 97th Cong. 1st Sess. 3, *reprinted in* 2 U.S. CODE CONG. & ADMIN. NEWS 127, 129 (1982))

[125] 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 Medical Svcs., Inc., 43 F.3d 1119, 1125 (7th Cir. 1994).

[126] *See* Evans v. Eaton, 16 U.S. (3 Wheat.) 454 (1818) (describing an alleged use of a flour manufacturing machine as "piracy"); *see also* Recording Industry Association of America v. Diamond Multimedia Sys.[hereinafter *Diamond*], 180 F.3d 1072 (9th Cir. 1999). The Copyright Act of 1976, 17 U.S.C. § 101 et. seq., provides copyright protection to "musical compositions" and "sound recordings."

[127] *See generally* ANDY ORAM, PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES (2001).

[128] 239 F.3d 1004 (2001); and 17 U.S.C. 512.

[129] *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 an excellent treatment of the criminal implications of file-sharing) .

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—perpetuate a conflict between informational privacy and intellectual property.[130] As this section will argue, the *Napster* court's adoption of a knowledge standard for contributory liability has unwittingly transformed Internet Service Providers into a nation of potential copyright enforcers, a factor which has privatized the spectre of piracy surveillance on the Internet.

Until *Napster* hit the international media, 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—and to the protectors of informational privacy—when it issued its landmark opinion, which affirmed in part a preliminary injunction against Napster, Inc., a Redwood City corporation that developed software to facilitate the transmission of MP3 files between its users.[131] 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 also 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.[132]

In response, various plaintiffs, led most visibly by the RIAA, filed suit, claiming that Napster users were engaged in the "wholesale reproduction and distribution of copyrighted works, all constituting direct infringement."[133] In addition to Napster, the suit named a number of anonymous Jane Does—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.[134] The plaintiffs argued that these Napster users were infringers who were facilitated by the

---

[130] 239 F.3d 1004.

[131] *Napster*, 239 F.3d at 1011. *See* Stephanie Greene, *Reconciling* Napster *with the* Sony *Decision and Recent Amendments to Copyright Law*, 39 AM. BUS. L.J. 57 (2001); 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).

[132] In just a few months after the company was born, the Napster revolution spawned a network of millions of individuals, 44 million in total, all engaged in the massive sharing of music files.

[133] *Id*. at 1013. In April of 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. Napster complied, and blocked 317, 377 users from using its service the following month. Yang, *supra* note --, at *Case Study 1: Napster*.

[134] Bowrey and Rimmer, *supra* note --, at *Part One.* In September of 2002, the administrators of USC 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, September 13, 2002, *at* http://www.wired.com/news/mp3/0,1285,55159,00.html.

company's software and support.[135] On appeal, the Ninth Circuit agreed, observing that Napster's users violate two of the copyright holders' exclusive rights: the rights of reproduction and distribution.[136]

At the time, almost no scholars looked beyond the relationship between law and technology to focus on the effect of *Napster* and the DMCA on informational privacy and the protection of personal identity, an omission that has turned out to be a grave one four years later. For the extension of property frameworks over intellectual goods in cyberspace has created powerful implications for the enjoyment of civil liberties. As this section will argue, *Napster*, following the DMCA, has privatized the protection of copyright, unwittingly setting forth an implied series of incentives for content owners to engage in self-help surveillance of consumer activities through peer-to-peer frameworks. *Napster*'s neat standard of contributory liability created a power-sharing agreement of sorts, in which the content industries were given the responsibility to police the Internet for evidence of unauthorized use; and ISPs were given the responsibility to disable access to these works after receiving proper notice under the DMCA from content owners. Yet although the *Napster* court admirably attempted to set forth a framework for contributory liability for ISPs, building on the substantial body of literature and law on third-party liability, it failed to establish or suggest the need for any privacy protections for individual subscribers, nor did it offer any guidelines in detecting piracy.

Following the Digital Millennium Copyright Act, the *Napster* court established a set of directives for ISPs to follow in addressing the infringing activities of their users.[137] Under these provisions, an ISP is required to either identify the subscriber and/or take down the posting as long as minimal assertions of a "good faith" belief in infringement are met.[138] The governing law has held that "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer."[139] 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."[140] Moreover, if the ISP engages in any "personal conduct" that encourages or assists the infringement, it is also liable for contributory infringement.[141] The actual words

---

[135] *Napster*, 239 F.3d at 1013, *see also* S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081, 1085 n.3 (9th Cir. 1989) (stating, "[t]he word 'copying' is shorthand for the infringing of any of the copyright owner's five exclusive rights.... ").
[136] *Napster*, 239 F.3d at 1013-15.
[137] *See id*. at 1027-28. *See also* Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L. J. 1833, 1881-82. 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. DMCA, 17 U.S.C. §§ 512(c)(1)(A)-(C).
[138] *See* Yen, *supra* note --, at 1881.
[139] Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2nd. Cir. 1971).
[140] *Napster*, 239 F.3d at 1021.
[141] *Id*. at 1019. In applying these tests, the court concluded that Napster "knowingly encourages and assists the infringement of plaintiffs' copyrights," because Napster had both actual and constructive knowledge that its users

of the DMCA, however, 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.[142] 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."[143]

Taken together, these 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's clear something is missing from this picture: an asserted commitment to informational privacy. Consider, for example, the difficult relationship that ISPs have with their subscribers after *Napster*. 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.[144] Yet the vast array of ways in which consumers' online activities have been subjected to monitoring (as the next section will detail) clearly demonstrates that this provision has been violated regularly—not by ISPs directly, but by intellectual property owners who have embarked on an endless journey through the Internet to detect allegedly unauthorized uses of their material. In so doing, their activities have raised a myriad of privacy concerns.

Why has this occurred? There are several reasons. The first reason is that the *Napster* court required evidence of actual knowledge of specific acts of infringement to hold an ISP liable for contributory copyright infringement, but it failed to explain what constituted acceptable methods of searching for such information.[145] As a result, an entire industry has sprung up, seemingly overnight, that searches through individuals' hard drives, web sites, and chat rooms to find evidence of infringement, as the next section details.

Second, under the DMCA's "safe harbor" provisions, codified at 17 U.S.C. § 512, certain service providers may avoid contributory liability if they comply with a section of the DMCA called the "notice and takedown" provision, which requires the provider to "expeditiously remove or disable access to" infringing material upon receipt of a "notification of claimed infringement" from a copyright owner that complies with certain requirements. Once proper notice is given, however, the burden of compliance then

---

exchanged copyrighted music. *Id*. at 1020. *See also* Religious Tech. Center v. Netcom On-Line Communication Services, 907 F. Supp. 1361, 1375 (N.D. Cal. 1995).

[142] Yang, *supra* note --.

[143] *Id*. (quoting the DMCA, 17 U.S.C. § 512(d)).

[144] DMCA, 17 U.S.C. § 512(m).

[145] *Napster*, 239 F.3rd at 1021 (observing, "[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*.

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.[146] As a result of these guidelines, intellectual property owners have invented an increasingly invasive programme of surveillance over citizens; 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.

As I have suggested, 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 to either take down the infringing material or to terminate Internet access to the subscriber. Thus, they are often the only barriers between protecting ordinary citizens from the invasive measures used by content owners to identify them. As a result, the unique power of peer-to-peer technology has spawned a host of concerns from ISPs, which are often caught between two conflicting motivations: the need to protect others' intellectual property and the need to protect their consumers' privacy.

Consider the Verizon case discussed at the outset of this paper. This year, the RIAA issued a notice to Verizon regarding one of its subscribers' activities in a test case that involved the reach of the DMCA's special subpoena provision, known as Section 512(h).[147] In the past, these subpoenas almost always involved individuals who stored the infringing material on the servers. However, the Verizon case was substantially different from these prior scenarios, because the "infringing" information was stored on the user's *own computer hard drive*, not on Verizon's own servers.[148] In response, Verizon refused to comply with the subpoena, explaining, "[n]o files of the Customer are hosted, stored, or cached by [Verizon]."[149] According to Verizon, the DMCA did not authorize a subpoena 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]

---

[146] *See* Richard Raysman and Peter Brown, *Notice and Takedown under the Digital Millennium Copyright Act*, N. Y. LAW JOURNAL, February 11, 2002, 3, col.1.

[147] This provision authorizes district courts, at the request of a copyright provider, to issue subpoenas to service providers such as Verizon when they need further information to identify a particular individual. In order to obtain a subpoena, the copyright owner is required to supply "a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title." 17 U.S.C. § 512(h)(2)(C).

[148] *See* Brief for RIAA at 7, *supra* note 1. 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 Internet Services, Inc., 240 F.Supp.2d 24, (D.C. Cir. 2003).

[149] *Id*. at 8. Section 512(a) limits an Internet service provider's liability for copyright infringement when its activities are limited mostly to routing, transmitting, or providing connections for material, and that material is not stored on its network. *Id.*

service provider."[150] 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)."[151] It claimed that the subpoena was limited only to "[i]nformation residing on systems or networks at direction of users."[152] 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," not just ISPs who stored infringing material on their networks.[153] According to Verizon, 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."[154] Instead, 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.[155]

In response, the RIAA threatened that Verizon would be subjected to potential contributory infringement, explaining that the safe harbor provisions 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 one of its subscribers.[156] In response, Verizon claimed that the DMCA provisions clearly demonstrate that Congress contemplated the material residing on its system. If the material was stored on the person's individual computer, and not Verizon's network, Verizon explained, 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 at all.[157] Had Congress intended such a result, Verizon pointed out, it would have drafted a clearer statute towards that

---

[150] *See* Section 512(c)(3)(A), and Brief for Verizon, supra note ---, at 3, and slip op. at 6 (quoting Verizon as stating that "The allegedly infringing contents of the [downloaded files] do not reside on any system or network controlled or operated by [Verizon], but . . . are stored on the hardware of the Customer." For this reason, Verizon argued that neither § 512(c)(3)(A) or §512(h) is applicable for this reason alone. *Id.*

[151] *Id.* at 3,7.

[152] *See* 17 U.S.C. § 512.

[153] Brief for Verizon, *supra* note ---, at 3.

[154] *Id. at* 3-4, 20 (stating, "[e]ven 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.")

[155] *Id.*at 5.

[156] Brief for RIAA, *supra* note ---, at 14.

[157] *Id.*

intention.[158] "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."[159]

Given the fact that almost everyone can be a copyright owner, and that every transmission on the Internet implicates activities that fall within the scope of the exclusive rights of copyright owners, Verizon contended that the RIAA's construction would result in a world where anyone who contrives can assert copyright infringements, and can gain the identity about another person through the DMCA's subpoena power.[160] The result would transform Internet Service Providers into the copyright police.[161]

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* Internet Service Providers within the scope of the DMCA, not just those providers which store information on a system or network at the direction of a user.[162] The court rejected, first, 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.[163] 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, or provision of connections; and those that stored information on its servers.[164] The court argued that one had to evaluate the DMCA and its subpoena applicability in line with the statute as a whole, not by a piecemeal, constrictive interpretation.[165]

Yet as *Verizon* shows, the DMCA and *Napster* failed to issue 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. Is an ISP required to turn in an individual who is notified by a copyright owner that he or 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

---

[158] *Id*. at 16.
[159] *Id*. at 21.
[160] *Id*. at 21-22.
[161] *Id*. at 23.
[162] *Verizon*, 240 F.Supp.2d at 26.
[163] *Id*. at 32.
[164] *Id*. at 31.
[165] *Id*. at 32. 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.

notice?[166] ISPs face a classic difficulty in this context: whether they should side with their customers, requiring a court-ordered injunction to terminate her subscription under the rubric of protecting her privacy; or whether they should remain ever-vigilant against piracy and terminate an account holder's subscription based on mere notice from the copyright owner instead. Largely due to this conflict, many ISPs have refrained from engaging in active content detection of their users' accounts, choosing instead to wait until they receive notice of infringement or other illegal material from law enforcement officials. Others, of course, have relented at the first accusation of infringement, handing over their subscribers' identities at the first possible opportunity.[167]

Perhaps most important, aside from *Verizon*, there is substantial confusion over what, exactly, constitutes 'copyright infringement' in other contexts. *Napster*'s immediate conflation of file-sharing with copyright infringement masks a host of complexity regarding the extent to which fair use defenses, or space-shifting, might conceivably apply in such contexts. In actuality, in dealing with the host of notice and takedown requests they receive, few ISPs actually pay attention to whether the substance of the accusation is meritorious or not, and assume that the copyright owners are making their accusations in "good faith." Yet there is substantial complexity within many instances of Net infringement, and this standard of copyright infringement offers no procedure for those who might wish to oppose or investigate such accusations of infringement or to challenge determinations made by an ISP, on behalf of a copyright owner.

For example, 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, for example, declined to impute liability to Napster on the basis of its peer-to-peer file-sharing technology alone. "We are compelled," the court observed, following *Sony*, "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."[168] Absent specific information which identifies infringing activity, the court

---

[166] Since *Napster*, three cases have noted substantial confusion regarding this point. *See, e.g.*, Hendrickson v. Ebay, Inc., 165 F.Supp.2d 1082 (C.D. Cal. 2001); ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001); and Arista Records, Inc. v. Mp3Board, Inc., 2002 WL 1997918 (S.D.N.Y. August 29, 2002).

[167] *See* 17 U.S.C. §512(c)(3)(A)(iv)-(v), and *Napster* 239 F.3d at 1027. 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, 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." The *Napster* court failed to further clarify these provisions, referring only to the need for copyright owners to refer to "specific infringing files."

[168] *Id.* at 1020.

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.[169]

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.[170] Yet this decision to shift the burden to the music industry to identify infringing material symbolizes a crucial, and overlooked, transition from consumer surveillance into piracy surveillance, highlighting the potential intrusiveness of anti-piracy measures. The back-and-forth disputes between Napster and the music industry's special master foreshadowed a deeper debate that was just beginning to unfold in the wake of the decision, demonstrating what was at stake—and what was unspoken—in *Napster*: privacy. 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.

In sum, rather than recognizing the substantial chilling potential of private network monitoring on expressive activities in cyberspace, the *Napster* court quietly resolved each conflict between copyright owner and consumer in favor of the content industry. Its only concession was in carving out a standard of contributory liability that required some notice be given to the ISP. Yet, this 'notice' requirement is hardly a model of clarity, and instead, as the next section will describe, accomplishes a marvelous exclusion of consumer interests by placing the burden on copyright owners to police their works, and then by forcing ISPs to act immediately or face charges of contributory liability. As a result, the critical difference between private and public enforcement of copyright appears to have disappeared. For the act of file-sharing transforms private citizens into a nation of potential law enforcers—at significant cost to informational privacy.

As the next section will describe, *Napster*'s incomplete solution, coupled with the DMCA's lack of clarity 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. Their methods of searching are facilitated by the increasing absence of privacy protections on the Internet, raising—and reifying—questions about the conflict between privacy and property in the digital age.

B. Methods of Piracy Surveillance

This year, the Recording Industry Association of America (RIAA), a trade association whose membership produces 90 percent of all sound recordings in the United States, proclaimed that it fights "a

[169] *Id.* at 1020-21.
[170] *Id.* at 1027.

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."[171] The RIAA's suggestion of constant activity is a grave understatement; its armies of anti-piracy investigators routinely crawl through the Internet, including university networks, searching and logging presumed unauthorized uses of copyrighted material. As part of this program, parties have equated Internet piracy with other types of undesirable criminality and therefore subjected it to a zealous campaign of enforcement that strains the boundaries of corporate propriety.

Perhaps as part of its attack on consumer downloading, the RIAA appears to demonstrate an unnatural and ample reliance on using the term "piracy" to denote an alarmingly expansive array of activities. Suddenly, for the RIAA's purposes, downloading music for personal purposes is 'piracy,' equated by 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, fall under the stigmatized spectre of "piracy," a metaphor suggesting that these acts are somehow contemporaneously equivalent to crossing the high seas, invading a ship, stealing its contents, and threatening life. The RIAA's web site, for example, declares that piracy is "old as the Barbary coast, new as the Internet."[172] 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.[173]

---

[171] *Diamond*, at 1074. *See RIAA Releases Mid-Year Anti-Piracy Statistics*, *at* www.riaa.com/News_Story.cfm. Such activities are not limited to trade associations with respect to music. For example, Disney's involvement in the recent bill sponsored by Ernest Hollings to require copy-prevention technologies on digital devices is just one example of how media companies often play a key role in the legislative debates about counteracting piracy on the Internet. *See* Brad King, *Disney's Peer-to-Peer Pressure*, WIRED NEWS (October 24, 2001), *at* http://www.wired.com/news/business/0,1367,47806,00.html. The bill would make it illegal to sell or distribute a digital media device that doesn't "utilize certified security technologies" approved by the U.S. Congress Dept. *Id.*

[172] *See* RIAA, *Anti-Piracy*, *at* http://www.riaa.com/protect-campaign-1.cfm, at *What is Piracy?*, (last visited May 21, 2003).

[173] *Id.* 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 isn't resold), or certain uses of "streaming" technology from the Internet. *Id.*

In the first half of 2001, the Recording Industry Association of America announced that its efforts led to a record number of arrests, product seizures, and guilty pleas and convictions.[174]

Piracy surveillance activities are almost always extralegal, and usually reflect the law's predisposition towards the protection of property, rather than the protection of consumer privacy and autonomy. To protect their interests, owners of intellectual property have attempted to propagate the notion that downloading MP3s, or copying other copyrighted works, is simply another form of theft.[175] Today, private companies routinely team forces with law enforcement officials to prosecute, investigate, and to charge individuals with trafficking in pirated materials.[176] The No Electronic Theft Law (the NET Act), for example, provides for criminal prosecutions for infringement, even where no monetary profit or commercial gain can be derived from the infringing activity.[177]

The constant drumbeat of threats of suits, both direct and contributory, have resulted in a host of activities taken by ISPs out of fear of liability for copyright infringement. Today, 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.[178] Some colleges refuse to permit individuals to send MP3 files at all, irrespective of whether

---

[174] *See* RIAA, *Anti-Piracy*, *at* http://www.riaa.com/Protect-campaign-6.cfm, at *Statistics*, 2 (last visited May 21, 2003).

[175] Generally, with a musical recording, there are usually two different types of copyrights involved. The first copyright involves the actual musical composition, or the musical notes and lyrics. A music publisher or songwriter usually owns this copyright. The second copyright involves the actual recording of the performer singing or playing the given song—the record company usually owns this copyright. Titles 17 and 18 of the U.S. Code cover these copyrights, protecting copyright owners from unauthorized distribution, adaptation, or reproduction of sound recordings. There are state anti-piracy laws that make it illegal to copy, reproduce, and distribute sound recordings without authorization, and there are unfair competition laws that also address unauthorized uses of copyrighted material. *See* RIAA, *Anti-Piracy*, *at* http://www.riaa.com/protect-campaign-4.cfm, at *Penalties* (last visited May 21, 2003).

[176] *See* RIAA, *Anti-Piracy*, *supra* note ---, at *Statistics*, 2. The RIAA claims that it works closely with federal, state, and local officials, and aided in 1,762 arrests and indictments in the first six months of 2001. *Id*. 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. 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." Ashbel S. Green, *Net Piracy Gets First Conviction: UO Student*, PORTLAND OREGONIAN, August 21, 1999, at A1; Jacobson & Green, *supra* note 6, at 290 n.120; Bailey, *supra* note ---, at 476.

[177] *See* No Electronic Theft (NET) Act, Pub. L. No. 105-147 (1997) (codified in sections of 17 & 18 U.S.C.). Under these provisions, individuals can also be held civilly liable for actual damages of lost profits. Online infringement of copyrighted music is punishable by up to 3 years in prison and $250,000 in fines, or 6 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); Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 250-52 (1999); Jacobson & Green, *supra* note 6, at 288-92 (2002).

[178] Huffstutter, *supra* note X (quoting Frank Creighton of the RIAA, declaring "We will know who these students are."). 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

or not they fall under fair use or are taken from the public domain.[179] A multitude of ISPs have acted almost immediately after receiving notice from intellectual property owners, taking down web sites and revealing the identities of their subscribers without any concern for whether or not the accused infringement is actually meritorious in character.[180]

For this reason, such strategies raise concerns that extend beyond bandwidth saturation, and stem from the panoptic potential of such surveillance to control the use of cultural products entirely. An illustrative example: in August 2001, the Ninth Circuit, in a debate of unprecedented visibility, refused to install certain software that would enable its monitoring of their computers to detect the downloading of music, streaming video, and pornography.[181] 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 uses 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, culminating in a passionately written opinion editorial by Judge Alex Kozinski:[182]

> 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.[183]

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 left a sour taste in the mouths of many federal workers, highlighting the tradeoffs that many universities and employers have made in order to prevent being saddled with a lawsuit for contributory liability.[184]

> 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.

See Rodney Erickson, Provost, An Important Message on a Key Issue From the Provost, (March 31, 2003) (on file with author).

[179] *See* email from Rebecca Tushnet from Fordham University, dated March 15, 2003 (on file with author).

[180] Let me emphasize here that I am not arguing for the protection of the anonymity of copyright infringers at any cost. Instead, I am arguing that strategies of surveillance are overbroad by design; thus, they ensnare both offenders and non-offenders, and provide little protection to those harmed by such technologies. See Part III.

[181] *See Rebels in Black Robes Recoil at Surveillance of Computers*, N.Y. TIMES, August 8, 2001.

[182] *Id.*

[183] Alex Kozinski, *Privacy on Trial*, WALL STREET JOURNAL, September 4, 2001.

[184] *See Judges Bar Use of Court Computers for Pornography, Large Personal Files*, 70 U.S L. WK. 2183, September 25, 2001. The administrative court claimed that it had found no legitimate court use for Gnutella, Napster, Glacier, and Quake, and therefore banned them from court computers. *Id.*

There are two reasons for this heightened degree of enforcement, one architectural, and one practical. First, as I have suggested, the preexisting equilibrium between property and privacy that exists in real space has disappeared in cyberspace, enabling the creation of limitless techniques of surveillance techniques that are often used to monitor consumer activities. Second, despite the immense leverage that the Ninth Circuit granted to the recording industry to protect their works from unauthorized transfer through *Napster*, profits from the music industry have dropped dramatically. Even though Napster is now completely defunct—having filed for bankruptcy after a long standstill while it tried to launch a legitimate service—a host of replacements, each more decentralized than the previous one, have risen up to take its place. Kazaa, for example, has sixty million users around the world and 22 million in the United States, and has enabled far more illegal downloading than Napster ever did.[185]

Consequently, the seemingly intractable problem of piracy has led to the silent creation of massive offensives—criminal, civil, international—spearheaded by private intellectual property owners in recent years against pirated material across the Internet and through regular public channels. The desperate attempts of the music industry to try to save itself have spawned a calculated attempt to shift the political and economic costs of copyright enforcement onto third parties, particularly Internet Service Providers.[186] The RIAA has attempted to threaten ISPs and universities with contributory infringement suits if they do not act immediately to reveal the identity of subscribers, terminate their Internet connections, and issue generalized threats of criminal prosecution to the student body. And just recently, the RIAA took another step: it filed suits against four college students accused of using internal college networks to facilitate file-trading, and announced its plan to sue others.[187]

All of these strategies have one thing in common: they use online piracy surveillance mechanisms to monitor potential copyright infringement of music, film and software. Like consumer surveillance, piracy surveillance uses similar systems of panoptic identification, classification, and assessment in order to affect the development and expression of online personae.

Towards these ends, peer-to-peer technology has ironically turned out to be the industry's greatest weapon, as well as its greatest foe, in deterring piracy, enabling intellectual property owners to model their efforts to replicate methods of consumer surveillance. Techniques of piracy surveillance can be used, either directly or indirectly through an intermediary, to detect infringement or to penalize perceived

---

[185] *See* Todd Woody, *The Race to Kill Kazaa*, WIRED, FEBRUARY 2003, at 106, *available at* http://www.wired.com/wired/archive/11.02/kazaa.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 Died*, WIRED, FEBRUARY 2003, at 92, *available at* http://www.wired.com/wired/archive/11.02/dirge.html. At the same time, sales of blank CDs jumped 40 percent last year. *Id*.

[186] The RIAA has attempted, with little success, to compel the government to invoke its prosecutory mechanisms to attack illegitimate peer-to-peer file-sharing.

[187] *See RIAA Sues College File Traders*, WIRED NEWS, , April 3, 2003, *at* http://www.wired.com/news/technology/0,1282,58340,00.html.

infringers. Most significant, each of these techniques are private in character, in the sense that each of these methods are administered and utilized by a non-government entity, and are 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 erroneous accusation.

1. Monitoring

Copyright owners in cyberspace rely heavily on the use of 'smart agents' to identify acts of perceived infringement; and, coupled with the outcome of *Verizon*, copyright owners can now quickly identify and contact a perceived infringer directly. In cyberspace, the RIAA maintains a team of Internet specialists and an automated 24-hour web-crawler, a "bot" that continually crawls through the Internet to identify allegedly infringing activities.[188] 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).[189] One Web crawler, run by Copyright.net, essentially crawls through a person's hard drive looking for uploaded copies of particular songs lurking in peer-to-peer networks like Gnutella, Aimster, and Napster.[190] Another report stated, "the Ranger [bot] is scouring the globe—Web sites, chatrooms, newsgroups, and peer-to-peer file-sharing sites—scanning 60 countries, searching in English, Chinese, and Korean….Ranger is 24-7. Ranger is relentless."[191] 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. Once it locates the song, it notifies the Internet Service Provider to terminate the person's online connection until she removes the offensive copy.[192] The RIAA's software robot, dubbed Copyright Agent, has served more than one million copyright violation notices to ISPs on behalf of 750 song writers and performers.[193]

---

[188] *See* RIAA, *Anti-Piracy*, *at* http://www.riaa.com/protect-campaign-5.cfm, at *What We're Doing* (last visited May 23, 2003). In the first half of 2001, 8,716 online auctions offering illicit sound recordings on their sites were removed from online auction sites, a 418 percent increase on the number removed a year prior to that date. *See* RIAA, "RIAA Releases Mid-Year Anti-Piracy Statistics," at 2.

[189] *See What's a Bot*, *at* http://www.botspot.com/common/whats_bot.html.

[190] *See* Dawn C. Chmielewski, *Tennessee Firm's Software Tracks Down Bootlegged Music, Bans Users*, SAN JOSE MERCURY NEWS, February 28, 2001.

[191] Frank Ahrens, *'Ranger' Vs. the Movie Pirates; Software Is Studios' Latest Weapon in A Growing Battle*, WASHINGTON POST, June 19, 2002, at H1.

[192] *Id.*

[193] *Id.* The Motion Picture Association of America and the Business Software Alliance use similar technologies. Robert Gibbons & Lisa M. Ferri, *The Legal War Against Cyberspace Piracy*, N.Y. L.J., August 5, 1999, at 1, col. 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.)

In this strategy, following *Napster* and the DMCA, these strategies of private enforcement utilize a brilliantly 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.[194] Once it identifies the site operator, the RIAA may send that person a warning email, it may send messages to the Internet Service Provider, or it may even institute litigation against the operator.[195] At schools, automated web crawlers detect where downloading takes place. When it is located, the RIAA sends letters asking the school to take action against the alleged infringer.[196] 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.[197]

Aside from demonstrating panoptic strategies of identification and assessment, such surveillance techniques also replicate public modes 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.[198] Yet it declined 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.[199] 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. The risk of detection and disclosure, in turn, is precisely what facilitates compliance.

Before the *Verizon* case was handed down, 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. After *Verizon*, peer-to-peer networks are no longer anonymous, amorphous communities characterized by unique social norms and noncompliance to copyright laws. Rather, the use of smart agents, coupled with the risk of identity disclosure, has pierced the veil of anonymity that many file-sharers expect.

---

[194] *See* RIAA, *Anti-Piracy*, *supra* note ---, at *What We're Doing*.
[195] *Id*. At universities, the RIAA has instituted a "Soundbyting campaign," which it claims to have resulted in a 55% drop in the number of music sites on University servers offering illegal downloads. *Id*.
[196] Liza Porteus, *Beware of the Music Downloading Spies*, U-WIRE, October 26, 2000. 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. Healey, *supra* note ---. Still other companies such as Cyveillance, Ewatch and Cybercheck, assist customers to protect their brands by using customized software to track trademark, copyright infringement, counterfeiting, and bootleg music and movies. *See* Gibbons & Ferri, *supra* note ---. These companies may also search for any association of brand names with pornography, and searches for any damaging rumours in chat rooms. *Id*.
[197] *Id*.
[198] See Katie Dean, Are you in RIAA's Cross Hairs, www.wired.com (June 26, 2003).
[199] Id.

The use of private enforcement strategies is deceptively appealing. From the copyright owner's perspective, it allows for near-perfect, automated detection, and creates a risk of disclosure that deters would-be infringers from sharing files. On the other hand, significant problems plague this technology, because it can easily mistake legitimate files for copyrighted works.[200] These examples pose great burdens for the freedom of speech of their authors and creators. 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*.[201] The Business Software Alliance, just recently, targeted a company who used a software called *Open Office*, sending it a false, form notice that it was making copies of Microsoft Office available simply because its "bot" detected the use of the word "office" in the program.[202]

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.[203] 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 the artist Usher.[204] In another example, the RIAA apologized to a national broadband provider for sending a cease-and-desist letter that alleged illegal activity on a subscriber's FTP site.[205] Yet the form contents of the letter read that the site illegally "offers approximately 0 sound files for download."[206] In another instance, Wal-Mart sent a Section 512(h) notice to a comparison-shopping website that allowed consumers to post prices of items sold in stores, claiming incorrectly that its prices were copyrighted when they were uncopyrightable facts.[207] Other "bots" have generated DMCA notices for films or court documents that are part of the public domain.[208]

One might rightly wonder if such monitoring techniques raise privacy implications at all, especially considering that the "bots" are programmed to specifically search the Internet only for information that is publicly available, and not restricted in a particular fashion. The question might be asked like this: why is a "bot" any different in cyberspace than the use of a camera in real space? The answer is simple: monitoring techniques in cyberspace *do* operate like cameras in real space, except that

---

[200] *See* Gigi B. Sohn, *Intellectual Property Theft Online*, Testimony before Congress, 2002 WL 100237623 (September 26, 2002).
[201] *See id*.
[202] *See* Declan McCullagh, *BSA (Microsoft) Screws Up, Targets OpenOffice Distribution*, POLITECH, February 28, 2003, *at* http://www.politechbot.com/p-04511.html.
[203] Gil Kaufman, RIAA Admits Piracy Goof, Rolling Stone.Com (May 14, 2003).
[204] Id.
[205] Declan McCullagh, RIAA Apologizes for Erroneous Letters, CNET News (May 13, 2003).
[206] Id. The letter allegedly continued, "Many of these files contain recordings owned by our member companies, including songs by such artists as Creed."
[207] See Amicus on Appeal at 12.
[208] Id. In one instance, the Internet Archive was sent a DMCA notice by a copyright owner who mistook films in the

they are more akin to facial-recognition cameras than casual observation. In this sense, they have implications for both privacy and autonomy. Consider Lawrence Lessig's commentary on this point:

> 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 them 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.[209]

Under *Verizon*, the same is true here: a person's communications, their pseudonymous address, and the material stored on their home computer is largely rendered transparent, without notice to the consumer, as long as a bare accusation of infringement is made. The DMCA contains no protection for anonymous speakers in the face of accusations of infringement; thus, anyone claiming to be a copyright owner can use a subpoena to determine the identity of a proposed infringer.[210] For this reason, the prevalence of monitoring techniques, coupled with the import of *Verizon*, make it effectively impossible to speak anonymously; at all times, the watcher is made potentially aware of the speaker's identity.

2. Management

Digital rights management (DRM) is another kind of piracy surveillance that, importantly, does not draw on ISPs alone for their enforcement, but utilizes similar trajectories of monitoring and record collection. Unlike the technology explored in the previous section, DRM requires an affirmative act by the consumer to inform the company of his or her identity prior to using a copyrighted product. Thus, in this sense, DRM cannot function without a complete encroachment on a user's privacy: some copyrighted products cannot operate without constant verification of the user's identity.[211]

Some DRM strategies are designed to set and automatically enforce limits on user behavior, like a music delivery format that prevents copying (even for "space shifting" purposes) or restricts the type of devices used for playback.[212] Today, DRM involves the encryption of 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

---

public domain for a copyrighted movie. Id.

[209] Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501, 504-05 (1999).

[210] I will elaborate on this point in Part III.

[211] Howe, *supra* note ---, at 147. 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 International, May 6, 1999.

[212] *See* Julie Cohen, *DRM and Privacy*, draft at 4 (on file with author).

digitally shared with others.[213] Content scrambling system algorithms (CSS) can also add a further, geographic restriction that ensures that DVDs only play in designated regions.[214] Still other technologies can report back to the information provider on the activities of individual users, which can be used for a variety of purposes, including marketing.[215] 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.[216]

It makes sense, both economically and practically, to ask a copyright owner to internalize the costs of enforcement through such management systems. Yet many of these strategies fail to recognize the importance of protecting consumer privacy, and thus display a striking convergence of piracy and consumer surveillance. Consider the use of antipiracy technologies that prevent users from converting, or "ripping" software tracks into an MP3 format from a CD. Such technology, called Digital Content Cloaking Technology (DCCT), requires users who desire digital copies to provide personal information in order to track the customer's listening habits.[217] 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, and that the music would not work on portable MP3 players.[218] In the end, the copyright owners relented, eventually agreeing 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.[219]

---

[213] Jeff Howe, *Licensed to Bill*, WIRED, October 2001, at 142; Associated Press, *Privacy Advocates Slam Industry Plan for Hard Drives*, WALL STREET JOURNAL EUROPE, January 18, 2001. The code, however, that enables the anti-piracy software is widely believed to be installed in home and office hard drives, thereby opening the door to more draconian anti-piracy measures. *Id.* Makers of hardware appear to support such restrictions. For example, 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, *Company Town TV Makers Take a Side on Anti-Piracy Technologies Media*, L.A. TIMES, May 16, 2001, at C5. 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.*

[214] *Cohen, supra note – at 7.*

[215] Id. at 7.

[216] Id. at 9. Software companies have faced much more successful outcomes in subordinating consumer privacy to the protection of intellectual property. 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; and another provision permitted the use of other self-help remedies as long as they could be accomplished without a breach of the peace. See Section 2-2517 and 2-2518, and Craig Dolly, The Electronic Self-Help Provisions of UCITA: A Virtual Repo Man?, 33 J. Marshall L. Rev. 663 (2000).

[217] See Benny Evangelista, *Suit Challenges CD Copyright Scheme*, San Francisco Chronicle (September 11, 2001).

[218] John Iverson, Consumer Counterattack, Stereophile (September 10, 2001).

[219] See Consumers Win One Against Copy Protection Press Release, on www.mediachannel.org (dated February 11, 2002).

Such lawsuits raise the important question of how courts, legislators, and intellectual property owners can balance these interests of privacy and prevention of piracy. In many situations, however, the law either fails to step in, or, when it does, it 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 this example.[220] ReplayTV makes digital video recorders, which enable television viewers to make digital copies of copyrighted television programs, to skip commercials, and to send copies of televised programs to other ReplayTV users.[221] 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.[222]

In the suit, the plaintiffs demanded all documents and information that SONICblue possessed on its customers, particularly the TV shows they recorded, and other data showing their viewing habits.[223] Even though SONICblue did not possess this information, the plaintiffs demanded that it reengineer its product in order to collect the data. SONICblue refused, contending that they feared the information gathered could be used to file a host of suits against private individuals for acts of direct infringement. 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.[224] 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.[225] 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."[226]

Although the surveillance issue was not directly decided, the outcome of the dispute illuminates the tradeoff between privacy and piracy identified in this paper. Creators of intellectual property may seek to utilize consumer surveillance methods to detect instances of piracy surveillance. In the wake of *Verizon*, copyright holders may be able to force ISPs to reveal private information, including logs of the

---

[220] *Paramount Pictures Corp. v. ReplayTV*, 2002 WL 1315811 (C.D. Cal. April 29, 2002).
[221] *Id*.
[222] *Id*.
[223] 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* ELECTRONIC PRIVACY INOFORMATION CENTER, COVERT ELECTRONIC SURVEILLANCE OF TV USAGE, *at* http://www.epic.org/litigation/replaytv.
[224] *Id*.
[225] *See Court Reverses Order for ReplayTV to Collect and Turn Over Customer Usage Information, at* http://www.adlawbyrequest.com/in thecourts/ReplayTV061002.shtml.

programs downloaded by individuals, any record of consumer activity, and web sites visited. And it may not matter whether or the individual actually committed acts of copyright infringement—the mere accusation may be sufficient to warrant exposure of one's personal identity, as the DMCA examples illustrate.

3. Attack

A final method, significantly more unilaterally aggressive than the others, involves the use of smart agents to *interdict* transmissions. Here, companies use similar "bot" technology to 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.[227] Other technologies simply interrupt a download as it occurs.[228] According to one company that produces software interdiction software:

> MediaDefender's computers hook up 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.[229]

Note how the speaker (wrongly) assumes that all ten connections involve infringing activities. Still other software creates *spoofing*, which involves the creation of phony media files and dumping them, en masse, onto peer-to-peer networks.[230] Spoofed files are often corrupt or damaged, and produce static, popping, cracking noises, or complete silence.[231] Another strategy involves *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.[232]

Interdiction and spoofing are currently widely used throughout the peer-to-peer file-sharing community, and have vastly increased in use the last several months. They were also the primary subjects

---

[226] *See Order* dated May 30, 2002 at 3.
[227] *See* Gigi B. Sohn, *Intellectual Property Theft Online*, Testimony before Congress, 2002 WL 100237623 (September 26, 2002) (discussing Interdiction); and *see* Matt Bai, *Hating Hilary*, WIRED MAGAZINE, February 2003, at 97 .
[228] Jon Healey, *New Technologies Target Swapping of Bootlegged Files*, L. A. TIMES, February 20, 2001, at C1. 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 won't identify the sender or the recipient, for privacy reasons. *Id.* In contrast, Vidius does identify the Internet addresses of the senders and recipients, and can often access names and contacting information if the Internet Service Provider complies with the request. *Id.*
[229] See Edward W. Felten, Testimony Submitted to U.S. House of Representatives, Committee on the Judiciary, hearing on "Piracy of Intellectual Property on Peer-to-Peer Networks," (September 26, 2002).
[230] *See* Bai, *supra* note --, at 97.
[231] See Stephanie C. Ardito, The Peer-to-Peer Piracy Prevention Act: will the ability to conduct Intermediary Searching Soon Be at Risk?, Information Today (September 1, 2002).
[232] Id.

of a bill introduced in the summer of 2002 by Congressman Howard Berman, that would award copyright holders an exemption from various laws proscribing computer break-ins when seeking Net pirates.[233] (Interdiction, for example, is simply another name for a "denial of service attack," which some consider illegal under state and federal anti-hacking statutes, including the Computer Fraud and Abuse Act). Rep. 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," citing examples of digital rights management to support his position.[234]

One possible advantage to these "attack" 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. 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.[235] It could also be programmed to replicate itself as others accessed certain files, and could be passed on to other infringers.[236] This incriminating information could conceivably be used to generate cease and desist letters or criminal referrals.[237]

As these strategies suggest, the creation of safe harbors for such "corporate vigilantism" efforts involve clear risks that copyright owners might easily overstep their boundaries by invading the private sphere of a person's hard drive, and damage a computer or Internet connection with their efforts. While these activities fall within the twilight boundary between the protection of privacy and the protection of 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, as I will discuss in the next section.

Part III. Theorizing Private Enforcement of Copyright

In the prior section, I outlined a number of ways in which intellectual property owners have sought to privately enforce copyright restrictions on cultural products and to detect unauthorized uses of

---

[233] *See* Alex Salkever, *Taking the Piracy Fight Too Far*, BUSINESSWEEK ONLINE, July 9, 2002.
[234] *Id*. See Press Release from Howard L. Berman, *Berman Introduces Legislation to Foil Peer to Peer Piracy* (July 25, 2002) (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).
[235] See Joseph D. Schleimer, *Electronic Countermeasures to Copyright Infringement on the Internet: Law and Technology*, JOURNAL OF INTERNET LAW (November 2001).
[236] Id.
[237] Id.

their products.[238] As this section will argue, piracy surveillance confers an unprececented level of technological control to third parties in order to extrajudicially determine the boundaries of authorized and unauthorized uses of cultural products, often not their own. And this result has significant effects on consumer privacy. Put another way, as the protection and control of intellectual property expands, the protection of informational privacy shrinks. As a result, speech suffers. Consumers will be forced to internalize the costs of their loss of privacy; and will curb their expression in order to avoid the risk of punishment and disclosure by restricting their conduct to that which is unquestionably insulated from liability.

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 his or her identity from disclosure, and the interests of a third-party copyright enforcer in preventing this transaction from taking place. At the same time, however, the individual may place a high value on protecting his or her privacy or autonomy from invasion, just as a third-party enforcer may place a high value on protecting his or 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 theorize 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 programs on non-offending individuals. Obviously, the benefits to piracy surveillance are somewhat clear—a reduction in the harm caused by copyright infringement. But these benefits must also be weighed against the various costs involved, which involve, among them: its potential to block access to certain types of information, prevent fair use of cultural products, expose anonymous speakers, mistake legitimate files for illegitimate ones, and to cast a wide net of groundless accusation. As this section will argue, proponents of such systems often fail to recognize the substantial costs of compliance for non-offenders, such as risk-aversion, the possibility of mistake, and overdeterrence of speech, expression, and fair use.

The very purpose of copyright is to ensure that a balance exists between control over private ownership and expression in order to create incentives for more speech, and more creation. Yet piracy surveillance eviscerates this balance between control and expression, leading into an inescapable logic of vigilantism by conferring a type of unlimited predatory control over copyrighted cultural products. In turn, piracy surveillance has transformed the nature of copyright from a liability regime into a regime that potentially governs *all* cultural products in cyberspace, both illegitimate and legitimate. Thus, instead of thinking of copyright as a regime that protects the creation of cultural products, this section argues that

[238] This system of monitoring is not limited to music alone (although music has been the most visible of the commodities protected.

piracy surveillance has transformed copyright into a regime of panoptic publication, where copyright owners are legally empowered with a variety of means to 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.[239]

A. Real Space Analogies

The underlying logic behind piracy surveillance seems tied to real space principles, suggesting that intellectual property is equivalent, in both form and content, to other types of properties in real space. For example, although one 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.[240] In other words, intellectual property is not real property, and a number of particularized rules govern the use of intellectual property, and a host of statutory exceptions (including fair use) limit an owner's exclusive control over intellectual property.[241]

But there is also a difference in cyberspace. Unlike piracy surveillance strategies in real space, piracy surveillance implicitly suggests that a perceived "trespass" on a person's copyright justifies another "trespass" on a person's expectations of anonymity, autonomy, and freedom of speech. This eye-for-an-eye, invasion-for-an-invasion mentality is precisely why self-help analogies from real space often translate ineffectively, because they fail to consider the costs of such invasion on a non-offending individual.

Proponents of piracy surveillance respond by pointing 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.[242] 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 the same 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 destroy, an architecturally-created balance between spatial protections for privacy and protection of property discussed in Part I of this paper. Indeed, both the common law and the U.C.C.

---

[239] Raymond Ku, *Think Twice Before You Type*, 163 N.J.L.J. 747 (Feb. 19., 2001) (observing such strategies lead to a world "in which the only privacy we are guaranteed is the privacy found in the confines of our own minds.").
[240] Bailey, *supra* note --, at 488 (quoting a musician); and Dowling v. United States, 473 U.S. 207, 217 (1985) (observing, "interference with copyright does not easily equate with theft, conversion, or fraud").
[241] *Id*. See 17 U.S.C. § 107 (2000).
[242] See Statement of Rep. Berman on Declan McCullagh, Politech, dated September 4, 2002.

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 only where some degree of consent or acquiescence has been shown; and usually, in circumstances where an existing contract has been breached.[243]

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.[244] Other cases require some notification before taking unilateral action.[245] Even case law from real space suggests that trespassers do enjoy some expectations of privacy from unreasonable searches and seizures.[246] 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.[247] And no case has ever held that an entry into one's home, without the consent of the owner, is justifiable self-help.[248]

In contrast, the use of piracy surveillance scenarios in cyberspace shatters this traditional balance between the protection of property and the protection of privacy. 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 and carry the potential to invade spatial expectations of privacy as well as anonymity.[249] The Supreme Court 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,[250] pointing out that the

---

[243] *See* Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1101-02; and Pamela Samuelson, *Embedding Technical Self-Help in Licensed Software*, 1997 WL 9941285, Communications of the ACM (1997).

[244] *Id*. See also, Douglas Brandon and Melinda Cooper, et. al. *Self-Help: Extrajudicial Rights, Privileges, and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845 (1984).

[245] See 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).

[246] See People v. Schafer, 946 P.2nd 938 (Colo. 1997); Comment, Luke M. Milligan, The Fourth Amendment Rights of Trespassers, 50 Emory L.J. 1357 (2001);

[247] Id. at 861, see also Restatement (Second) of Torts, Section 198 (1965*), Entry to Reclaim Goods on Land Without Wrong of Actor.*

[248] See Eugene Mikolajczyk, *Breach of Peace and Section 9-503 of the Uniform Commercial Code—A Modern Definition for an Ancient Restriction*, 82 DICK. L. REV. 351; and 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 Dearman v. Williams, 109 So.2nd 316, 320 (Miss. 1959); Kirkwood V. Hickman, 78 So.2nd 351 (Miss. 1955); Butler v. Ford Motor Credit Co., 829 F.2d 568 (5th Cir. 1987).

[249] Consider a real space analogy. 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. If a company only licensed two copies of a particular software program, but fifty signals were detected, that company could be in trouble for breaking copyright rules. *See New British Anti-Piracy Solution Based on Intelligence Techniques*, TELECOMWORLDWIRE, March 2, 1998.

[250] Kyllo v. United States, 533 U.S. 27, 34 (2001)

very core of Fourth Amendment jurisprudence involved the right of a man to retreat into his own home, free from governmental intrusion.[251]

Proponents of piracy surveillance, particularly where monitoring, blocking, and filtering are concerned, rightfully point out, 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. Technically, this point is correct, but it fails to consider the other policy concerns that turn on the importance of protecting non-offending individuals from unwanted surveillance in cyberspace. Unlike analogies in real space, piracy surveillance does not entail formal notice, consent, or negotiation between the parties. Thus, 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 gaze of a copyright owner. 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:[252]

> 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 they way people experience intellectual goods.[253]

Even if a person does not necessarily enjoy an expectation of privacy under *Katz* in their subscriber information, or the material posted on the Internet—many individuals continue to expect anonymity in cyberspace, and the DMCA makes few allowances to protect aginst the possibility of erroneous or strategic accusations of infringement. Under the DMCA, it does not matter whether or not the person has actually infringed on a copyright or not—all that matters is that the owner has a "good faith" belief that the infringement has occurred. The potential for copyright owners to exploit the DMCA for the purposes of unmasking one's identity is staggering, particularly since there is no requirement that prior notice be given to the end user.

B. Institutional Competence

Another 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 should internalize the costs of his or her detection of infringement, rather than another entity, 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

[251] *See Id*. at 31. Indeed, *Kyllo* suggests that use of devices that are not in general public use to explore details of a home is presumptively unreasonable without a warrant. *Id*. at 40.
[252] Cohen, DRM and Privacy at 5.
[253] *See* Julie Cohen, DRM and Privacy, SSRN Working Paper at 4.

currently exists under the DMCA: the first turning on identity; the second turning on the importance of judicial oversight.

In an important paper, Professors Polinsky and Shavell have explained that the rationale for public law enforcement often turned on the role of information about the identity of violators.[254] When victims of harm naturally knew who injured them, allowing private suits for harm will motivate victims to initiate legal action and use that information to enforce law.[255] (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 its difficult to identify or apprehend perceived criminals, public enforcement may be more desirable.[256] 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.[257] Thus, public enforcement is usually preferred when effort is required to identify and apprehend violators.[258]

These observations become particularly important when we consider the effects of the DMCA subpoena power on citizen expression in cyberspace. DMCA notices are served and signed off with almost no judicial oversight. The DMCA section 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.[259] Moreover, piracy surveillance techniques, in and of themselves, do not demonstrate a predisposition towards the kind of discretionary nonenforcement which is typically demonstrated by public prosecutors and law enforcers.[260]

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. Moreover, 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.[261] Rather, the copyright owner only needs to have a high 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 or cutting off Internet access to the

---

[254] See A. Mitchell Polinsky and Steven Shavell, *The Economic Theory of Public Enforcement of Law*, JOURNAL OF ECONOMIC LITERATURE at 3.
[255] Id.
[256] Id.
[257] Id.
[258] Id.
[259] See Amicus Appeal brief at 2.
[260] See Landes and Posner, The Private Enforcement of Law, 4 J. Legal Stud. 1, 42, 43 (1975).
[261] See Warren F. Schwartz, Legal Error, at 1038 ("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.").

client, (or facing contributory liability), the ISP, in most cases, responds immediately, in some cases failing to afford prior notice or an impartial, independent determination.[262]

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. The need for judicial oversight becomes particularly pronounced where fair use and speech are concerned. Yet the DMCA power allows copyright owners to circumvent access to a fair and impartial forum, instead, mere accusations of infringement can displace court-ordered determinations. Moreover, piracy surveillance techniques also fail to consider two significant costs to third-party non-offenders: overdeterrence of speech and evisceration of fair use. These two elements, taken together, paradoxically converts copyright from a regime that governs the illegitimate use 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. I have concluded that copyright has been irretrievably transformed by this development into a regime of "panoptic publication."

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.[263] In the situation of piracy surveillance, judicial enforcement of fair use is made impossible, because a private entity's determination under the DMCA is capable of circumventing access to a fair and impartial forum. Here, 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 of a scenario where an individual's claims of fair use are sorted out by a judicial body, the DMCA creates an extrajudicial method to resolve claims by permitting the copyright owner to silence others.

Overdeterrence of speech is a relatively straightforward, and realistic, risk. Where there is an uncertain legal standard, John Calfee and Richard Craswell have demonstrated that individuals may deter socially desirable behavior in order to overcomply and thereby escape liability.[264] Applying their observations to copyright law, we see significant risks of uncertainty, particularly outside of judicial fora. Judicial determinations of infringement are often time-consuming, fact-laden determinations that often turn on the jurisdiction involved. In contrast, an extrajudicial determination is efficient, quick, but often prone to mistake, thus laying the groundwork for the uncertainty that motivates potential overcompliance.

---

[262] Cite to Ebay case.
[263] 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).
[264] *See* John E. Calfee and Richard Craswell, *Some Effects of Uncertainty on Compliance with Legal Standards*, 70 VA. L. REV. 965 (1984).

How would this overcompliance take place? Consider some of the examples that I have provided of mistaken DMCA notices. As I have argued, *Napster* placed the responsibility to detect infringement with intellectual property owners, and the DMCA's standard for a "notice and takedown" request is surprisingly low, requiring only a "good faith" assertion of copyright infringement. Consider, also, various examples in which accusations of infringement were made in order to silence particular expression under the DMCA:

- 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 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.[265]

As these examples demonstrate, the DMCA's notice and takedown provisions are often used for a host of reasons that do not always 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.[266] For, as I have shown, any activity that raises the risk of accusation automatically translates into a disclosure of identity under the DMCA. Thus, individuals who wish to remain anonymous will alter their speech to avoid accusation and detection, and speech will suffer as a result.

C. Privacy, Autonomy, and Anonymity

The factors I have identified above flow evenly into a third area of concern, which stems from constitutional values. 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, speech, or privacy. Yet the DMCA propagates an isolationist tendency by failing to require an ISP to conform its efforts to the privacy, anonymity, due process, and

[265] *See* Amici Brief, *supra* note --, at 10 (collecting examples).
[266] Id.

free speech protections normally afforded to citizens under the First, Fourth, or Fifth Amendments. For example, the *Verizon* court maintained:

> …[T]he DMCA neither authorizes governmental censorship nor involves prior restraint of potentially protected information. Section 512(h) merely allows a private copyright owners 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.[267]

This observation, at first glance, is rhetorically powerful, particularly as applied to the facts in *Verizon*. But it also overlooks the interplay of three other elements: first, the gatekeeper role of the ISP, who faces the threat of contributory infringement if it does not act immediately to silence the offensive conduct; second, the potential for strategic motives of a copyright owner, who may be tempted to file notices for spurious reasons; and third, the fact that its observations are not limited solely to individuals who upload copyrighted songs (an admittedly clearer issue of infringement), but *anyone* who potentially offers *allegedly* infringing material on the Internet. Thus, even if the DMCA only requires a preliminary unveiling of identity, Section 512 can give rise to serious due process concerns, for the accused herself as well as the ISP.[268] In short, the DMCA provision enables copyright owners to circumvent access to a fair and judicial forum by using an ISP to silence offensive speech or conduct.

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 its credit, the *Verizon* court admitted that the First Amendment recognized a right to anonymity, both in real space and on the Internet.[269] But the court limited the scope of this right by pointing out that courts have usually embraced a right to autonomy in situations involving "core First Amendment expression," like political speech, and not situations that deal with copyright infringement per se.[270] 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 defenses.[271]

---

[267] Verizon, 2003 WL 1946489 at 14.
[268] *See* Brief of Amicus Curiae United States Industry Association, et. al. at 5, *In re* Verizon Internet Services, Inc., 240 F.Supp.2d 24, (D.C. Cir. 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. Central Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950).
[269] See 2003 WL 1946489 at 11.
[270] Id.
[271] Id.

While it is certainly true that the First Amendment does not provide a defense to copyright infringement, mere *accusations* of infringement, without more, implicate First Amendment values because they provide powerful mechanisms for silencing others under the DMCA. As Jed Rubenfeld has emphasized on this point, 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."[272] So, while it is certainly true that a known 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 justifying the absence of anonymity. As one court observed, "If Internet users could be stripped of . . . .anonymity by a civil subpoena enforced under liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights."[273]

Moreover, aside from the failure to balance protections for anonymity with copyright, piracy surveillance also ensnares non-offenders, raising concerns about autonomous access to information. Consider the implications of the RIAA's recent request to allow its computer experts to scan all computers at the University of Melbourne for sound files and email accounts so that they can gather evidence of copyright infringement.[274] The mere effect of these techniques of widespread searching, without probable cause, affects a person's right to receive information online, and runs the risk of chilling legitimate expression in cyberspace. And the potential, complementary role of law enforcement exacerbates these risks, particularly in a university environment, 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—indeed the freedom of the entire university community."[275]

Surely, extensive network monitoring poses significant, and chilling, implications for academic discourse if individuals face the risk of "bot" monitoring if their files include samples of music, song lyrics, or even mention film or song titles in their work. Consider the observations of Justice Brennan in *Lopez v. United States*, an electronic surveillance case involving a pocket wire recorder:

> The risk of being overheard by an eavesdropper or betrayed by an individual or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society….But as soon as electronic surveillance comes into play, the risk changes crucially. There is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy. . . . Electronic

[272] See Rubenfeld, 112 Yale L.J. at 25.
[273] Doe v. 2theMart.com, 140 F.Supp.2nd 1088, 1093 (W.D.Wash. 2001).
[274] *See* Leonie Lamont, *Firms Ask to Scan UniversityFiles* , THE SYDNEY MORNING HERALD, February 19, 2003, at 3.
[275] *Griswold*, 381 U.S. 479, 482 (1965).

> surveillance strikes deeper than at the ancient feeling that a man's home is his castle; it strikes at freedom of communication, a postulate in our kind of society. . .[F]reedom of speech is undermined where people fear to speak unconstrainedly in what they suppose to be the privacy of home and office….Electronic surveillance destroys all anonymity and all privacy; it makes government privy to everything that goes on.[276]

As I have argued, many individuals operate under constant expectations of anonymity on line. To say that the mere accusation of copyright infringement rightfully eviscerates those expectations flies in the face of the numerous discussions, assurances, and guidelines that often actively support the opposite conclusion.[277] As a result of *Verizon*, a person who offers her subscription information to an ISP is expected to hand over every expectation of privacy in all of the information that she may transmit from or receive at her IP address. 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."[278]

In sum, the premise of electronic self-help, particularly in the piracy surveillance context, suggests the need to revisit the importance of recognizing the cost of technologies of invasion on consumer autonomy and access to information. In *Stanley v. Georgia*, a case which suggested the importance of the right to receive information, the Supreme Court held that the First and Fourteenth Amendments prohibit making mere private possession of obscene material a crime.[279] In that case, the court recognized that the valid 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.[280] As the *Stanley* 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 added dimension. For also fundamental is the right to be free, except in very limited circumstances, from unwanted intrusions into one's privacy.[281]

---

[276] Lopez v. United States, 373 U.S. 427, 465-71 (1963) (Brennan dissenting).

[277] *See* Declaration of Peter Swire, *supra* note 402, at 2, observing:

> At the time the DMCA was enacted in 1998, the dominant uses of the Internet from home were e-mail and surfing on the World Wide Web. Congress simply did not intent the subpoena provisions in the DMCA to be triggered by home use of e-mail or web surfing. Based on my own experiences in government, including with the outcry over e-mail surveillance by the FBI's Carnivore program, I do not believe that Congress in the DMCA was authorizing a private party to force an ISP to reveal the identity of senders of e-mails and surfers of web sites.

[278] *See* Electronic Frontier Foundation Newsletter, New Anonymity Case (February 7, 2001) (quoting Nicole Berner, counsel for the Liberty Project).

[279] 394 U.S. 557 (1969).

[280] *Id*. at 568-570.

[281] *Id*. at 563-564.

Those values easily translate into the context raised in this paper, where the DMCA's provisions extend piracy surveillance into the home activities of many citizens, resulting in a tradeoff in the autonomy and freedom of ordinary citizens to access information. 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.[282] 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."[283]

The very same observations could apply to the DMCA, where a person could be accused of a host of activities involving the use of infringed material in one's own home. The right infringed upon by piracy surveillance is no less sacred; the effect of such surveillance is precisely the same harm *Stanley* seeks to avoid. Thus, under *Stanley*, a court would 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 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."[284] Indeed, the access to information is considered to be a right that is so fundamental it demonstrates a critical linkage of informational privacy with other, more substantive areas of privacy, namely, the right to engage in certain activities and to make certain decisions without government interference. If *Stanley* is to mean anything at all in the modern-day context, then we must consider the ways in which the propertization of information has affected the rights of ordinary citizens to access certain types of information and to express themselves in particular ways. Allowing the DMCA's subpoena provisions to interfere into these zones of privacy, liberty, and expression flies in the face of the very values *Stanley* upholds.

Part IV. Reconciling Privacy and Property

As this Article has demonstrated, in cyberspace, intellectual property, privacy, and personhood are at an impasse. There is no way out—each area faces inherent conflicts with another. Yet, as the cases in this Article suggest, throughout the development of copyright in cyberspace, intellectual property rights have slowly and quietly expanded to take precedence over the privacy rights of ordinary citizens. Part of this is due to the expansion of property rights to cover 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

[282] *Id.* at 565.
[283] *Id.* at 565.

lawmakers and judges to conceptualize a deeper relationship between property and privacy: in other words, their failure to recognize that expansions of control of intellectual property cause tradeoffs in other areas of consumer protection—particularly where privacy is concerned.

As Professor Jonathan Zittrain points 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."[285] This similarity creates expectations of protection and control of data on both the side of the consumer as well as the collector. Yet there is a current tendency, shared by many judges and scholars, to separate property rights from privacy and to create a hierarchical relationship between the two.

As this paper has suggested, there are a host of real-life consequences to this separation. One obvious, and real-life, result of this expansion involves the creation of regimes of consumer surveillance: as I have argued in Part I, the extension of property rights in the collection of personal information can often eviscerate the efficacy of protections for informational privacy. A second result, discussed in Parts II and III, involves the creation of another type of surveillance, what I have called "piracy surveillance," which attaches a kind of private, predatory character to intellectual property. Both types of surveillance implicitly suggest that commercial self-interest and the presence of intellectual property entitlements justify any measure, no matter how invasive or intrusive, to identify and collect personal information.

Thus, instead of property rights taking precedence over privacy, this paper has suggested that the two rights in question should be equally valued and protected. The only way to do this is to reexamine copyright's relationship to privacy. For, treating copyright protection (and the DMCA) as a stand-alone regime obscures all of the ways in which its regulatory mechanisms affect constitutional areas like expression, privacy, and due process. Moreover, as the *Napster* and *Verizon* cases suggest, extending copyright to control the governance of peer-to-peer communications in cyberspace has a tremendously invasive potential on the activities and expressions of *all* citizens who post information in cyberspace. We have created a world in which the property rights of copyright owners are valued over the liberty, property, and privacy rights of individuals, suggesting that those principles are somehow less valuable than those that involve commercial self-interest.[286]

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 judges, scholars, and legislators to fashion a solution that squares with constitutional values of property, personhood, and autonomy. Today, the rivalry between intellectual property and privacy persists, even though the factual scenario has changed.

---

[284] *Id*. at 566.
[285] Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201 (2000).
[286] *See* Cohen, *Examined Lives*, *supra* note --, at 1390.

Reconciling the two requires the balancing of contemporary intellectual property law with constitutional values. Thus, this concluding section will suggest two potential ways judges, legislators, and individuals can protect against exposure of personally identifiable information in this increasingly peer-to-peer world. These changes are meant to serve as overlapping, reinforcing, and non-mutually exclusive methods to alter and enforce the scope of privacy at the hands of invasive third parties, and to highlight the necessity of thinking of informational privacy as an entitlement based on need, rather than expectation.[287]

A. Balancing Copyright, Privacy, and Freedom of Expression

As I have suggested, part of the problem lies in the law's failure to conceptualize the DMCA in conjunction with other values, particularly constitutional ones. Yet some laws have already reached a balance between constitutional values and law enforcement. Consider, for example, the Privacy Protection Act as one possible guide. The Privacy Protection Act requires a special subpoena when First Amendment interests in news reporting might be affected by an ongoing investigation. Here, the very same interests in ensuring the First Amendment right to broadcast might be applicable to the Internet, particularly in a peer-to-peer context, because everyone "publishes" information on the Web.

The genesis of the Privacy Protection Act is illustrative because it echoes the very concerns raised by piracy surveillance strategies today. In 1971, a demonstration at Stanford University Hospital turned violent, as police clashed with demonstrators. The Stanford Daily, a campus newspaper, managed to photograph a number of participants in the demonstration, which was of great interest to police.[288] 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.[289] Hence, at the Stanford Daily, the police searched wastebaskets and rummaged through photographic negatives, but did not (by all accounts) open any locked containers.[290] Nevertheless, the event so incensed the employees at the 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.[291] In that case, the Court held that the Fourth Amendment did not prohibit police from undertaking searches of evidence held by innocent third parties.[292]

---

[287] *See* GANDY, *supra* note --, at 235.
[288] *See* Mark Eckenwiler, *Applications of the Privacy Protection Act*, 8 SETON HALL CONST. L.J. 725 (1998).
[289] *Id*.
[290] *Id*.
[291] *Id*. at 726; *see also Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).
[292] *Id*. at 567-68.

Congress, reacting to the Court's opinion, enacted the Privacy Protection Act (PPA), attempting to protect materials protected by the First Amendment from police seizure. The PPA, therefore, establishes a general 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 similar form of public communication, in or affecting interstate or foreign commerce….[293]

The Act, therefore, provides for a special subpoena in cases where there is a danger of interference with the First Amendment interests of the publisher. Plaintiffs have employed it 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.[294]

There are many reasons for why the PPA should serve as a baseline guiding force in response to the DMCA's overreach into privacy and First Amendment expression. 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. Moreover, the spectre of criminal copyright infringement under the NET Act could easily provoke Fourth Amendment concerns.[295] For this reason, DMCA subpoenas can raise constitutional concerns that can activate PPA remedies.

One might object that the PPA is designed to protect news reporting, not individual expression in cyberspace. However, I would argue that this distinction between formal news reporting and individual expression has disappeared: on the Web, everyone is an author, a news reporter, and everyone has the possibility to broadcast messages to others. Consequently, the values that animated the passage of the Privacy Protection Act are the very same values implicated when we consider the degree to which piracy surveillance affects legitimate types of expression in cyberspace. The DMCA may have empowered a host of private speakers to silence the expression of others, but the PPA suggests the need for a coherent and careful response that embraces, rather than silences, protections for privacy and freedom of expression. As I have argued, the risk of implicating non-offenders within the panoptic snare of piracy surveillance raises the danger of silencing speech and expression in cyberspace. The risks of strategic silencing are simply too strong; and the DMCA's protections are simply too weak.

---

[293] 42 U.S.C. § 2000aa(a).
[294] *See* Steve Jackson Games v. United States Secret Service, 816 F. Supp. 432, 440-41 (W.D. Tex. 1993).
[295] Recall that the RIAA has threatened to utilize such measures against "substantial" infringers, which also implicates the NET Act.

Third, in similar situations, economists have stressed the value of raising the standard of proof to raise the costs of accusations and prevent the "overfishing" scenario I identified earlier. The same should be utilized here, in order to ensure the validity of accusations of copyright infringement. Thus, one possible solution involves under-girding the subpoena provisions with some judicial oversight that matches the procedures used in the PPA, or in other "John Doe" actions that require enough evidence to withstand a motion to dismiss.[296] These procedures are often used in other cases that involve anonymous speech, and they should also apply to govern similar situations under the DMCA. In such situations, where First Amendment concerns are triggered, the DMCA's interpretation should reflect the need for heightened standards of justification, in addition to requiring the immediate appealability of any proposed termination, the use of specially trained magistrates or marshals to carry out the search, and other procedures that reflect a concern for individual civil liberties, instead of the unilateral goal of protecting copyright above all else.[297]

B. Balancing Private and Public Copyright Enforcement

[In this concluding section, I will argue that judicial determinations of copyright infringement in cyberspace are preferable to the private, extralegal regimes currently created by DMCA subpoenas. I will argue, first, that copyright law has traditionally envisioned a robust, protective role for the state in ensuring compliance and the ability to exercise fair use privileges; and second, that the tradeoffs between private and public law enforcement of copyright imposes social costs that are unwarranted and untenable. In the end, I suggest the need for a greater degree of hybridity between private and public enforcement with respect to intellectual property].

Conclusion

In this Article, I have argued that our ceaseless expansions of 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 and privacy that real space originally intended. 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

[296] *See* Dendrite International. Inc. v. John Doe No.3, 342 N.J.Super 134 (App. Div. 2001).
[297] *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 806 (1994).

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.