BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 16 SUPPLEMENT SUMMER 2001

TABLE OF CONTENTS

ARTICLES

COMMENT

BACK FROM THE FUTURE: A PROLEPTIC REVIEW OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

By David Nimmer[†]

Some years back, I was privileged to offer a trio of ancient copyright decisions in the celebrated case of *Achilles v. Zeno*. David Nimmer, *An Odyssey Through Copyright's Vicarious Defenses*, 73 N.Y.U. L. REV. 162 (1998). More recently, while meditating upon the blank spaces between the lines of the Digital Millennium Copyright Act, I fell into an ecstatic trance in which the boundaries between myself and the universe faded. Vaulting ahead centuries, I chanced upon a judicial opinion from the far future. As on that earlier occasion, I present these matters unedited—except that, as an artifact of time travel, all citations to post-2001 authority seem to have mysteriously vanished.

---

† Visiting Professor, UCLA School of Law; Distinguished Scholar, Berkeley Center for Law and Technology; Of Counsel, Irell & Manella LLP. I presented an earlier version of this article as Distinguished Visiting Scholar in Law and Technology at the University of Dayton School of Law in November 1999. My thanks to Bob Kreiss for the kind invitation to Dayton; to Dick Lanham, Peter Menell, and Mark Lemley for helpful leads and suggestions; and to Alison Hajdusiewicz for research assistance.

IN THE TRIBUNAL
FOR THE NEAR GALACTIC MASS
(NOVO THERMOPYLAE DIVISION)

In the matter of	)	
	)	Case No. CV 5761
	)	
1,934 CORTICALLY ACTIVATED TRANSPONDING DEVICES COMMONLY CALLED "Havona Servitals"	)	MEMORANDUM AND ORDER (HUMAN TRIAL REQUESTED)

SEER: Samuell ix9

Six centuries ago, the United States Congress passed the Digital Millennium Copyright Act. Two years ago, the Saturnine Standards Society promulgated technical measures to be followed by those now-ubiquitous devices first popularized by Caligastia Lanonandek, known to kids (and their external mindbots) everywhere as "Havona Servitals."

Respondent manufactures devices that do not comply with the stated measures. Hence, this action.

There is an undeniable irony in prosecuting an action in 2657, based on the failure to take measures promulgated only in 2655, when the statute under which this cause of action arises dates all the way back to a law passed in 1998. I have therefore adopted the utterly strange expedient of issuing an opinion in this matter, instead of merely effectuating judgment through the court's corps of superuniverse functionaries. In my own defense for such an outré denouement, let me protest that, historically speaking, it was actually not all that unusual for jurists in centuries past to prepare opinions in individual cases. (Strangely, some even divided the page in half, writing one commentary on the top and another on the bottom in smaller type, even though it would seem *prima facie* that the resulting product would be incomprehensible. *See* Abner J. Mikva, *Goodbye to Footnotes*, 56 U. COLO. L. REV. 647 (1985).).

I. INTRODUCTION

A. The Late Twentieth Century

On October 28, 1998, Congress passed an amendment to the Copyright Act called the Digital Millennium Copyright Act ("DMCA")—a much more modestly entitled corpus than succeeding amendments to the Copyright Act, such as the Universally Applicable Decree Mandating Self-Evident Goodness of 2103, or the Open-Your-Brain Ecphrasis of 2418. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998) (codified as amended in scattered sections of 17 U.S.C.).

Little is known at present of the DMCA's gestation period encompassing the end of the 20th Century. The consensus among historians holds that it was an ascetic and reticent period, almost monastic in tone, in which the supreme emphases were on contemplation and self-abnegation. Extreme modesty was highly prized.

The haziness of our current knowledge of that time period reflects a great irony. Evidently, the DMCA looked forward to a rosy digital future. Yet only scant decades later, the folly of that reliance became apparent after an electromagnetic catastrophe erased most knowledge of the past. That was the so-called Y2K+38 Bugaboo, whence the current proverb. *See* Jack E. Brown, *Portents of the Year 2000 Computer Problem*, 15 SANTA CLARA COMPUTER & HIGH TECH. L.J. 109, 115 n.20 (1999) (anticipating disaster, inter alia, as of Jan. 18, 2038). As stated by Deutero-Jacqueline Susann, "even contemporaries recognized the danger from the 'Rollerball scenario' in which 'a mad computer hacker were to destroy the total electronic memory of central libraries,' HENRY PETROSKI, THE BOOK ON THE BOOKSHELF 214 (1999). Yet the authorities failed to take the prospect seriously until it was too late. With the universal return of papyrus as the medium of record, the future is once again safe-guarded."

Of course, one of the surviving facts from that general time period was the Great Economic Meltdown, also called the Mycterismus of 2050. When it was over, as is well known, there were only three corporations left, two of them controlled by Bathsheba Berlusconi. Those considerations return to the fore below regarding the discussion of Macrovision Corp. and its regulation via the DMCA.

B. Passage of the Digital Millennium Copyright Act

What was the contemporary need as of 1998 for this massive enactment? Was it events of the past? Of the present? Or of the future? Someone named Jack Valenti testified on behalf of the Motion Picture Association of America (we don't know what "motion pictures" were, but they

must have been important). He told Congress in 1997 that the threat to his industry from digital exploitation of movies was "real and immediate." *The WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act*, *Hearing Before the Subcomm. on Courts and Intellectual Property*, *House Comm. on the Judiciary*, 105th Cong. 79 (1997) (statement of Jack Valenti, President and CEO, Motion Picture Association of America) ("Internet piracy is not a 'maybe' problem, a 'could be' problem, a 'might someday be' problem. It is a 'now' problem."). A year later, someone else testified on behalf of that same trade organization, the MPAA, that its "nightmare scenario" lay in the future: "Digital networks will *soon* make this complex and dangerous undertaking cheap and simple;" the danger, "*if it is realized*, will drive a stake through the heart of our hopes for the healthy growth of electronic commerce." *The WIPO Copyright Treaties Implementation Act*, *Hearing Before the Subcomm. on Telecommunications, Trade, and Consumer Protection, House Comm. on Commerce*, 105th Cong. 55 (1998) (statement of Steven J. Metalitz, on behalf of the Motion Picture Association of America) (emphasis added). Present and future, it seems, were impinging on one another even in the bill's past.

Of the legislative history leading up to the DMCA, few direct fragments have survived. *See* UMBERTO ECO, MISREADINGS 15 (William Weaver trans., Harcourt, Brace & Co. 1993) (1963). Enshrined at the Planetary Archives is the one surviving fragment of the original legislative history that led to this epochal enactment: "[W]hat was it that Wade Greski said, . . . I am trying to skate to where the puck is going, and not where we are today." *WIPO Copyright Treaties Implementation Act, Hearing Before the Subcomm. on Courts and Intellectual Property, supra*, at 111.

Though that catchphrase has become familiar to tyke-brains throughout the sector, it is not absolutely certain what Zoe Lofgren (whose subsequent celebrity I need scarcely rehearse here) meant by it. Popular wisdom has it that the Speaker of the House at that point was a certain otherwise unremembered Greski, who first instituted the Parliamentary device of recognizing speakers on the chamber floor through the ceremonial passage of a small silicon discus. But other theories abound—including the happenstance that an ancient player of a game called "hockey" bore the slightly similar name "Wayne Gretzky" (the only problem being that no one has ever been able to link that game to the DMCA).

C. Prolepsis

I would like to propound my own theory. Congress, I am speculating, passed the DMCA not based on where current reality was on the day of

passage. Instead, it was self-consciously trying to skate to where reality would be located in the future.

The term for this is *prolepsis*. An ancient dictionary contemporary with the DMCA defines *proleptic* as "[t]he use of a descriptive word in anticipation of the act or circumstance that would make it applicable." WEBSTER'S ENCYCLOPEDIC DICTIONARY 1351 (1990). The source gives as an illustration: "[t]hat gambler is a dead man: Sam Sneak has sworn to get him." *Id*.

The example is a felicitous one. Just as the gambler is alive now, but proleptically dead because of Sam Sneak's threat, the argument in this case is that Havona Servitals were lawful as of 1998 (none but the most visionary could even imagine their existence at that early date) but proleptically dead, *i.e*., unlawful for the future, because of the DMCA's threat.

(There is a vital distinction, though. In the posited case, at the moment of speaking, Sam Sneak has already targeted his ire against the gambler. In the case of the DMCA, by contrast, it did not target the Havona Servitals as of its enunciation in 1998. Instead, Congress said in 1998 that steps would be taken in the future, and that when that future dawned, those steps would gain the force of law.)

Speaking of death and prolepsis, there seems to be mystical bond between the two. Even the standard work on the subject illustrates the latter through an example of the former. *See* RICHARD A. LANHAM, A HANDLIST OF RHETORICAL TERMS 120 (2d ed. 1991) (drawing an example of prolepsis from 1 COR. 15: 35-37, "How are the dead raised up?"). The link is more ancient still—just consider *Deuteronomy* 17:6. According to the regnant *Oprah Winfrey Pesher*, the translation is "the death penalty requires two or three witnesses." The antique *King James Version* of the Bible comes closer to the original, though: "[a]t the mouth of two witnesses or three witnesses shall he that is worthy of death be put to death." But its rendition of "he that is worthy of death" misses the mark. The original Hebrew reads *yumat hamet*, *i.e.*, "the dead shall die." Of course, that formulation implicates a logical contradiction—if already dead, then the sinner will not be able to die again, so the future tense becomes inapposite; whereas saving the future tense deprives the sinner of his current "dead" moniker. The rabbis noted the solecism, of course, and thereby derived a homiletical lesson—one who sins has already committed spiritual suicide. BABYLONIAN TALMUD, TRACTATE SANHEDRIN 41a. Otherwise stated, the sinner is proleptically dead.

The Bible, of course, teaches timeless lessons, for our age no less than those past. One of its central strategies is "proleptic exposition or future-directed retrospect." MEIR STERNBERG, THE POETICS OF BIBLICAL NARRA-

TIVE: IDEOLOGICAL LITERATURE AND THE DRAMA OF READING 280 (1985). Prof. Sternberg enunciated that insight in his chapter *à propos* the instant inquiry, entitled *Temporal Discontinuity, Narrative Interest, and the Emergence of Meaning*. He noted that "retrospective incoherence signals (guarantees, invites) prospective coherence." *Id.* In that spirit, the instant opinion attempts to draw current coherence from the DMCA's retrospective incoherence.

II. FEATURES OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

The Digital Millennium Copyright Act contains almost no instance of the word "future." Yet large swaths of it are intimately bound up in a prediction of how the world will subsequently unfold. Besides isolated features buried in elaborate provisions, *see* MELVILLE B. NIMMER & DAVID NIMMER, 2 NIMMER ON COPYRIGHT § 8.22[D][1][c] ns.311, 331 (2001) (future-oriented provisions of statutory license for subscription digital audio transmission services), whole features are devoted to future developments. The discussion below considers three.

A. Section 1201

1. Basic Provision

The single most potent pronouncement of the DMCA is contained in section 1201. *See* David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 675 (2000) [hereinafter Nimmer, *A Riff on Fair Use*]. That section commands at the outset: "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(1)(A) (Supp. 2000). When Congress passed that provision in 1998, what "technological measure" did it have in mind "that effectively controls access to a work"?

Congress itself concedes that it passed this provision in the expectation "that technological measures will most often be developed through consultative, private sector efforts." H.R. REP. NO. 105-796, at 64 (1998). It singled out for praise "multi-industry efforts to develop copy control technologies" that had been underway since 1996 and "strongly encourage[d] the continuation of those efforts. . . . " H.R. REP. NO. 105-551, pt. 2 at 41 (1998).

In short, Congress acted proleptically.

2. Exemptions

Another relevant aspect of Section 1201 is that it contains a plethora of exemptions. *See* Nimmer, *A Riff on Fair Use, supra*, at 692-702. Two relate to parental efforts to keep pornography from minors and the authority to disable cookies. 17 U.S.C. §§ 1201(h), 1201(i) (Supp. 2000) (essentially defining cookies as technological measures that "contain[] the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person seeking to gain access to the work protected"). The fascinating thing about both those features is that they address problems that were nonexistent at passage of the DMCA. Congress included them lest a need arise in the future.

The nonsensical nature of a law that allows parents to hack into a domain to express their desire to remain aloof from that domain has already been noted. *See* David Nimmer, *Puzzles of the Digital Millennium Copyright Act*, 46 J. COPYRIGHT SOC'Y 401, 409-12 (1999). As of passage of the DMCA, Congress noted, "[a] variety of tools available now allow parents to exercise control in a manner consistent with their own family values, of their children's access to online materials." S. REP. NO. 105-190, at 14 (1998). Use of those extant tools afforded ample protection to parents as of that date, without ensnaring them in liability under section 1201. So why on Urantia did Congress need to add a specific exemption to that section in this regard? Because it was concerned that "*in the future*, any of these tools [might] incorporate[] a part or component which circumvents a technological protection measure." *Id.* (emphasis added). To reiterate, it acted proleptically.

Likewise, commentary has noted the "topsy-turvy upshot" of the cookie-disabling exemption: "if a consumer receives disclosure about a cookie, then she may not disable it; if she does not receive disclosure, then she may lawfully disable." 3 NIMMER ON COPYRIGHT § 12A.05[B][2]. By all accounts, there was no extant reason as of adoption of the DMCA in 1998 to include such a provision. As stated by the legislative history, "[n]o specific example of such a privacy-invasive technology in use today that would be affected in this way has been called to the Committee's attention." S. REP. NO. 105-190, at 18. Even if such a threat did exist then, "all commercially significant browser programs can be readily configured to reject 'cookies,' and such a configuration raises no issue of any violation of section 1201." *Id*.

So why did Congress act here? The motivation here equally lay in the future: "because of the privacy concerns expressed that existing or *future technologies may evolve* in such a way that an individual would have to

circumvent a technological protection measure to protect his or her privacy, the committee concluded that it was prudent to rule out any scenario in which section 1201 might be relied upon to make it harder, rather than easier, to protect personal privacy on the Internet." *Id*. at 18 (emphasis added). Again, prolepsis reigned.

3. Future Assurances

One of the oddest features of the DMCA is that it contains a welter of corporation-specific features, relating to Macrovision Corp. 3 NIMMER ON COPYRIGHT § 12A.07[D][2]. The features in question relate to section 1201's controls on consumer analog devices. *See* 17 U.S.C. § 1201(k) (Supp. 2000). On that score, the House-Senate conferees acknowledged that numerous activities were underway in the "private sector to develop, test, and apply copy control technologies, particularly in the digital environment" and encouraged "their continuation, including the inter-industry meetings and working groups that are essential to their success." H.R. REP. NO. 105-796, at 68.

Unlike the features canvassed above, in which Congress enacted in 1998 whatever those inter-industry groups would develop in the future, the instant features unfolded differently. Congress declined to provide its advance imprimatur here, but instead foresaw that to the extent in the future "the participants request further Congressional action, the conferees expect that the Congress, and the committees involved in this Conference specifically, will consider whether additional statutory requirements are necessary and appropriate." *Id*. That reticence bespeaks a refusal to act proleptically. In this particular, therefore, it seems that a different sensibility was at work.

But before agreeing to this feature of the statute, the House-Senate "conferees assured themselves in relation to two critical issues." *Id*. One was that the analog copy control technologies that it adopted into law did not create "playability" problems on normal consumer electronics products. *See* 3 NIMMER ON COPYRIGHT § 12A.07[D][1][a]. The second is the one that implicates our current theme. The conferees assured themselves "that the intellectual property necessary for the operation of these technologies will be available on reasonable and nondiscriminatory terms." H.R. REP. NO. 105-796, at 68. On this score, the legislative history waxes at length:

> In relation to the intellectual property licensing issues, the owner of the analog copy control intellectual property—Macrovision Corporation—has written a letter to the Chairman of the Confer-

> ence Committee to provide the following assurances in relation to the licenses for intellectual property necessary to implement these analog copy control technologies: (1) that its intellectual property is generally available on reasonable and nondiscriminatory terms, as that phrase is used in normal industry parlance; (2) that manufacturers of the analog video cassette recorders that are required by this legislation to conform to these technologies will be provided royalty-free licenses for the use of its relevant intellectual property in any device that plays back packaged, prerecorded content, or that reads and responds to or generates or carries forward the elements of these technologies associated with such content; (3) in the same circumstances as described in (2), other manufacturers of devices that generate, carry forward, or read and respond to these technologies will be provided licenses carrying only modest fees (in the range of $25,000—in current dollars—initial payment and lesser amounts as recurring annual fees); (4) that manufacturers of other products, including set-top-boxes and devices that perform similar functions (including integrated devices containing such functionality), will receive licenses on reasonable and nondiscriminatory terms, including royalty terms and other considerations; and (5) that playability issues will not be the subject of license requirements but rather will be handled through an inter-industry forum that is being established for this purpose. The conferees emphasize the need for the technology's proprietor to adhere to these assurances in all future licensing.

Id. at 69. The sequel to those assurances is a fascinating historical chapter. Following the Mycterismus of 2050, all the assets of Macrovision wound up in a branch of the Berlusconi *famiglia* called Auxesis Parrhesia Enterprises ("APE"). APE promptly abandoned Macrovision's license fee, which in the interim had risen from $25,000 to $33,000, and announced that effective immediately it would charge $7,500,000.

The resulting suit ended up at the Supreme Judicature. Its decision concluded that, had Congress legislated a fee of $25,000 for Macrovision licenses, the resulting law would have been invalid as a Bill of Attainder. U.S. CONST. art. I, § 9, cl. 3; *see also Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 468 (1977) (defining a bill of attainder as "a law that legislatively determines guilt and inflicts punishment upon an identifiable individual without provision of the protections of a judicial trial[]"). It further noted that Congress cannot accomplish more through salting matters into reports than it could by enacting them into law directly. On that basis, the Court dismissed any claim against APE for violating Macrovision's representations to Congress.

As the Court noted, Congress itself had declared, almost contemporaneously with adopting the Digital Millennium Copyright Act, that "no voluntary commitment, however sincerely intentioned, can actually be enforced." S. REP. NO. 106-51, at 2 (1999) (Senate Commerce Committee report addressing satellite television). Had Congress truly wanted to sanctify Macrovision's representations into law, it knew how to do so; conversely stated, Congress knew exactly what it was *not* accomplishing whilst enunciating pious words about keeping license fees in the "modest" range.

B. Section 512

Another provision of the DMCA sets forth a safe harbor for the benefit of online service providers. In order to obtain eligibility under that feature, the provider must accommodate something that the statute denominates "standard technical measures." 17 U.S.C. § 512(i)(1)(B) (Supp. 2000); *see id.* § 114(d)(2)(C)(viii). What are those? Here, the statute affords some guidance: the reference is to "technical measures that are used by copyright owners to identify or protect copyrighted works." *Id.* § 512(i)(2). Inclusion of these "standard technical measures" reflects a belief "that technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age." H.R. REP. NO. 105-551, at 61. This provision "is intended to encourage appropriate technological solutions to protect copyrighted works." *Id*. This provision, like the one governing section 1201's "technological measures," was also proleptic—in the sense that no "standard technical measures" existed as of enactment of the DMCA in 1998.

To qualify, future technical measures were required to be "developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process." 17 U.S.C. § 512(i)(2)(A) (Supp. 2000). "The Committee anticipate[d] that these provisions could be developed both in recognized open standards bodies or in ad hoc groups . . . ." H.R. REP. NO. 105-551, at 61. Many of the former bodies "ha[d] substantial experience with Internet issues." *Id*. at 62. The latter groups had been "successful in developing standards in other contexts, such as the process that has developed copy protection technology for use in connection with digital video disk players." *Id*.

In any event, the experience under this provision was disappointing. A pan-industry conclave convened in a plush Bosian resort in 2120. Although sixty percent of those gathered quickly hammered out an agreement, the remaining holdouts refused to accede. After extravagant blan-

dishments were proffered, another ten percent caved. But the remaining thirty percent would not budge.

So the industry decided to follow the majority standard. But a rogue element continued to operate outside those "standard technical measures." A lawsuit resulted. Petitioners claimed that the new operating guidelines constituted multi-industry standards, which appropriately reflected "a broad consensus of copyright owners and service providers." Respondents replied that seventy percent does not a consensus make.

In 2145, the Intermediate Decisors handed down their decision. The court noted that beyond urging "all of the affected parties expeditiously to commence voluntary, inter-industry discussions to agree upon and implement the best technological solutions available to achieve these goals," H.R. REP. NO. 105-551, at 61, Congress had legislated no teeth to see its precatory language through to completion. Based on the failure of a sizable minority to accede to the majority approach, no consensus was reached, and therefore no operative "standard technical measures" governed. To this date, that aspect of the statute remains a dead letter—with scant prospect that it will ever spring to life.

C. Section 1202

Another feature of the DMCA protects copyright management information ("CMI"). *See* 17 U.S.C. § 1202 (Supp. 2000). The statute defines eight distinct classes that qualify as CMI, including a work's title, author, and conditions for use. *Id*. § 1202(c)(1)-(8). The last enumerated category specifies "[s]uch other information as the Register of Copyrights may prescribe by regulation . . . ." *Id*. § 1202(c)(8).

That feature also bears some future-oriented tendencies, insofar as a party had no way, as of passage of the DMCA in 1998, to know what category of information might become defined as CMI in 2316, for example. Is it for that reason proleptic?

Without question, the cited provision involves delegation of quasi-lawmaking authority to a government official outside of Congress. By itself, however, that delegation represents no innovation, even within U.S. copyright law. For instance, when Congress passed the Audio Home Recording Act, Pub. L. No. 102-563, 106 Stat. 4238 (Oct. 28, 1992), it authorized the Secretary of Commerce to establish by regulation the scope of a "professional model product" exempt from regulation thereunder. 17 U.S.C. § 1001(10) (1994); *see also* 2 NIMMER ON COPYRIGHT § 8B.02[A][2]. Even more directly, the antecedent statute authorized the Register of Copyrights "to establish regulations not inconsistent with law" for various purposes. 17 U.S.C. § 702 (1994); *see also id.* §§ 119(b)(1)

(directing satellite carriers whose secondary transmissions have been subject to compulsory licensing to deposit statement of account with Register of Copyrights "in accordance with requirements that the Register shall prescribe by regulation"); *id.* 104A(e)(1)(D)(i) (authorizing the Copyright Office to issue "regulations governing the filing under this subsection of notices of intent to enforce a restored copyright.").

But the instant section 1202 differs in kind from its predecessors. Those previous features of law enacted a policy desired by Congress, for instance to require libraries to prominently display a copyright warning adjacent to their photocopying machines. *Id.* § 108(d)(2). The details of the warning's verbiage were simply left to the Copyright Office to promulgate. *Id*.

Reverting to section 1202, by contrast, something basically different was at work. Consider that in the previously cited examples, Congress made the decision that satellite carriers would need to pay for secondary transmissions and foreigners wishing to resurrect their lapsed copyrights would need to file a notice of intent; it was simply the ministerial details of how to accomplish those goals that Congress left to the Register of Copyrights. *See* 17 U.S.C. §§ 119(b)(1), 104A(e)(1)(D)(i) (Supp. 2000). By contrast, the open-ended language in Section 1202 of the DMCA became a blank check.

The matter in question unfolded in litigation in 2098, when the Register of Copyrights used the authority vested in her by section 1202(c)(8) to prescribe by regulation the categorical requirement to include as part of CMI the name of the "director who is credited in the TV broadcast of an audiovisual work." The resulting litigation challenged that regulation, on the basis that Congress had already defined one category of CMI as follows: "*[w]ith the exception of public performances of works by radio and television broadcast stations*, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work." *Id.* § 1202(c)(5) (emphasis added). The complainant aptly noted that the categorical regulation effectively wrote out of the statute the italicized preamble to that category.

In response, the Register adjured, "[s]o what authority do you think Congress gave me to prescribe by regulation, huh? The statutory categories already include the work's title, author, copyright proprietor, *etc*. Am I expected to add the name of the author's mothers-in-law? Based on intervening technological advances, notably the death of the Intrenaut, it is only sensible now to expand the reach of directorial credit for audiovisual works to broadcast TV—which, as we all know, is poles apart from what the late 20th Century understood by that term." The court bought the ar-

gument. As a result, the DMCA applied to seven categories for its first century, and in addition to an eighth thereafter.

So it seems that section 1202's authorization for regulation produced a much greater upset to received expectation than all of its predecessors. Indeed, Congress legislated against the grain when it passed the DMCA. As mentioned earlier, the Audio Home Recording Act contained an authorization for the Secretary of Commerce to propound limited regulations. The original bill for that 1992 legislation would have gone much further. That version contemplated that the Secretary of Commerce would have the power to amend the basic standards regarding permissible copying, as the technology progressed. S. REP. NO. 102-294, at 23 (1992). Nonetheless, Congress ultimately deleted that authority, feeling that "this issue raises policy questions that are appropriately addressed in the future by Congress." H.R. REP. NO. 102-873 pt. 1, at 14 (1992); *see also* 2 NIMMER ON COPYRIGHT § 8B.03[B][1].

The value judgment that Congress expressed in the Audio Home Recording Act seems to have gone out the window by the time that Congress passed the DMCA—what it felt in 1992 "raised policy questions that are appropriately addressed in the future by Congress" became by 1998 the subject for present-implementation-via-the-future. In this facet as well, the DMCA evinced proleptic tendencies.

D. Distinction from Past Legal Schemes

It can be answered that it is anything but abnormal for the laws of Congress to enshrine a legislative approach today, based on past experience, to govern in the future. In some sense, the very constitutional purpose of copyright—"to promote the progress of science"—is future-oriented. Some particulars follow:

- In the Audio Home Recording Act of 1992, Congress regulated "digital audio recording devices." 17 U.S.C. § 1001(3) (1994). When the first case arose under that law six years later, the technology had greatly progressed, making it very difficult to predict whether a hand-held device used to play MP3 files fell within the regulation of the statute. *See Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072 (9th Cir. 1999).

- Congress in the past had relied on industry to work out solutions. An example is the Berne Convention Implementation Act of 1988, Pub. L. 100-568, 102 Stat. 2853 (Oct. 31, 1988), which Congress passed ten years before the DMCA to make U.S. law compliant with the Berne Convention. That law jettisoned the compulsory li-

cense for juke boxes, and substituted an interim statutory royalty, with concomitant incentives for industry to come up with their own alternative consensual scheme. *See* 2 NIMMER ON COPYRIGHT § 8.17[A]. Because that amendment itself provided that Congress's scheme would lapse into desuetude once the affected industries reached agreement, the result is that a law passed in 1988 exerted no more impact following an industry agreement in 1992.

- Over the decades, such performing rights societies as ASCAP and BMI have made themselves integral to the sound functioning of the copyright system. *See* Robert Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CALIF. L. REV. 1293, 1328-40 (1996). Even under pre-DMCA law, entities that wished to use music had no other option than to take out appropriate licenses from those entities. *See* S. REP. NO. 104-315, at 35 (1996) (minority views of Sen. Hank Brown, Member, Senate Comm. on the Judiciary) ("[U]nder the current system, it is impossible to choose only one: virtually anyone who chooses to play music in public will have to purchase a license from two, if not three music licensing organizations."). Those consortia therefore furnish a template for the pan-industry conferences that Congress contemplated when enacting the DMCA.

Because these examples nominally indicate that future-directed regulation, even to the extent of deferring to industry practice, is nothing new, that rebuttal concludes that the DMCA fits harmoniously into past schemes. But it is not so. To demonstrate, I must myself engage in the device of *prolepsis*—defined in rhetoric to mean answering an opponent's anticipated objections. LANHAM, *supra*, at 120. The examples just posited actually do not debunk my greater thesis.

Consider first the performing rights societies. One outstanding feature that pertains to them is that they obtain only non-exclusive rights from their member-composers. *See* 2 NIMMER ON COPYRIGHT § 8.19[A]. As a consequence, a party who wishes to exploit a given song always has the option (I am speaking now of pre-1998 law, continuing through the present) of ignoring ASCAP and BMI, instead dealing directly with the subject composer. Conversely, a composer retains the option of declining to join any performing rights society, and can choose instead to personally police all exploitation of her work. If she finds her works exploited by a television station—even one that has punctiliously maintained valid ASCAP and BMI licenses—she will prevail in an infringement suit. Those considerations debunk any notion that these societies, as a legal matter, imposed their will on nonconsenting members of the affected class.

Next comes the Berne Convention Implementation Act of 1988. In that amendment, parties could opt out of the statutory rates by mutual agreement. But the law did not bind nonagreeing parties! *See* 2 NIMMER ON COPYRIGHT § 8.17[C]. Thus, the innovation of the DMCA remains—it alone among Congress's amendments to the Copyright Act subjects even nonagreeing parties to the strictures of industry agreements, and conveys on those agreements the force of law.

Moving to the Audio Home Recording Act of 1992, Pub. L. No. 102-563, 106 Stat. 4238 (Oct. 28, 1992), it is true that even a visionary at passage of that Act would have had a hard time knowing how a Diamond Rio, to be developed years later, would fall within its framework. The difference, though, is that the DMCA beggars even those efforts. It was not merely difficult, but impossible, for someone at enactment of that law to predict its operation. Even imagining that someone was farsighted enough in 1998 to envision the development of Havona Servitals in 2600, the prophet still would have had no inkling as to their permissibility, absent further clairvoyance regarding industry standards to be developed in 2655.

The DMCA pursued a course radically different from previous enactments—it set forth a framework that Congress expected to be filled in through future conduct of the affected parties. In other words, the expectation at enactment was not simply that courts called upon to construe the statute would give concrete substance to the law's interstices. That phenomenon is universally applicable, as Publius noted long ago. *See* THE FEDERALIST No. 37, at 229 (James Madison) (Clinton Rossitor, ed. 1961) ("All new laws, though penned with the greatest technical skill, and passed on the fullest and most mature deliberation, are considered as more or less obscure and equivocal, until their meaning be liquidated and ascertained by a series of particular discussions and adjudications."). Nor was it a prediction that Congress's laws today would spark desirable conduct in the future—that, too, is implicit in any enactment designed "to promote the progress of science," as all copyright amendments constitutionally must be.

Instead, the distinctive feature of the DMCA was its expectation that future agreements among the affected parties would, in effect, gain the force of law. We have here a textbook example of a law being unclear not because of insufficient care in drafting or the failure of legislators to hammer out agreement; instead, the law itself was drafted in advance of the problems to be encountered in its application. *See* Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1253 (1998); Jack Schwartz & Amanda

Stakem Conn, *The Court of Appeals at the Cocktail Party: The Use and Misuse of Legislative History*, 54 MD. L. REV. 432, 435-36 (1995).

It takes little effort to uncover the fatal flaw in that methodology. Consider that the primary issue on Congress's agenda when deliberating the DMCA was the putative threat of a "pay-per-use" future. *See* Nimmer, *A Riff on Fair Use, supra,* at 717-19. To safeguard against that threat, Congress incorporated numerous features into the statute. One authorized the Copyright Office to promulgate rules releasing adversely affected users from the anti-circumvention bans that it otherwise imposed. *See* 17 U.S.C. § 1201(a)(1)(C) (Supp. 2000).

But already by 2000, the Copyright Office recognized how unwieldy was the task that the DMCA assigned to it. It complained that "the Commerce Committee Report does not state how future adverse impacts are to be evaluated." Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64555, 64559 (Oct. 27, 2000). It further quoted a leading proponent of exemptions as admitting that "the inquiry into whether users of copyrighted works are likely to be adversely effected by the full implementation of section 1201(a)(1) is necessarily 'speculative since it entails a prediction about the future.'" *Id*. at 64562-63 (quoting Peter Jaszi).

From the oracle at Delphi to last year's Andromeda Spectacle, no one has succeeded in reducing predictions of the future into a science. Enactment of the DMCA in 1998 has proven no exception to that rule.

III. APPLICATION TO FACTS OF THIS CASE

The history of copyright law is inextricably linked to the history of technology. Emblematic of the tension that arises here is the celebrated judgment of 2222 involving the oneirographlogisticon. That device, which for the first time allowed users to record the dreams of others, raised a host of copyright issues. Pitted on one side were the dreamers, who claimed to have originated the material at issue. Not so, responded the auditors—dreams, as is well known, emanate from across the noetic divide, so that the dreamers at issue cannot claim personal originality; moreover, the necessary ingredient of fixation in a tangible medium of expression comes from the auditor, not the dreamer, further depriving the latter of any copyright interest.

Happily, the case at bar raises problems a bit less metaphysical than those at issue in the oneirographlogisticon litigation. But the theme remains constant: technological advancements require ceaseless refinement of copyright doctrine.

A. Petitioner's Motion for Summary Judgment

Petitioner's argument at bar is extremely simple: the law forbids manufacturers from allowing users to "circumvent a technological measure that effectively controls access to a work;" recently, the Saturnine Standards Society has promulgated the requisite technological measures applicable to Havona Servitals; respondent manufactures Havona Servitals that do not comply with the stated measures. Hence, petitioner urges, we should grant summary judgment on its behalf.

At the current stage of factual development, I am left with certain questions. Why, if the Saturnine Standards Society truly represents an industry consensus, are respondent's devices outside its standards? Did respondent manufacture the subject Havona Servitals before the Society promulgated its standards, and if so, is there a "grandfather provision" under which it finds shelter. Until those questions are answered, I must withhold the requested grant of summary judgment.

B. Respondent's Motion for Summary Judgment

Respondent urges multiple objections to being forced to adopt the technology at issue. It, in its turn, seeks summary judgment on numerous bases.

1. Constitutionality

The first challenge to the DMCA is of constitutional magnitude. Respondent urges that the device of proleptic legislation as implemented via the DMCA violates the nondelegation principle implicit in that instrument.

To consider this challenge, it is useful to start with an opinion of the Supreme Court of the United States (as the High Tribunal was then known) regarding proleptic legislation. The case in question challenged the constitutionality of the Bituminous Coal Conservation Act of 1935. *Carter v. Carter Coal Co.*, 298 U.S. 238, 278 (1936). A part of that act "delegates the power to fix maximum hours of labor" to a commission composed of representatives of both sides, *i.e.*, "producers of more than two-thirds of the annual national tonnage production for the preceding calendar year," on the one hand, and unions representing "more than one-half of the mine workers employed," on the other. *Id.* at 310. The standards reached by that commission were to be binding not only on its own members, but also on dissenting companies. The Court evaluated that device in the following language:

> The power conferred upon the majority is, in effect, the power to regulate the affairs of an unwilling minority. This is legislative

> delegation in its most obnoxious form; for it is not even delegation to an official or an official body, presumptively disinterested, but to private persons whose interests may be and often are adverse to the interests of others in the same business. The record shows that the conditions of competition differ among the various localities. In some, coal dealers compete among themselves. In other localities, they also compete with the mechanical production of electrical energy and of natural gas. Some coal producers favor the code; others oppose it; and the record clearly indicates that this diversity of view arises from their conflicting and even antagonistic interests. The difference between producing coal and regulating its production is, of course, fundamental. The former is a private activity; the latter is necessarily a governmental function, since, in the very nature of things, one person may not be entrusted with the power to regulate the business of another, and especially of a competitor. And a statute which attempts to confer such power undertakes an intolerable and unconstitutional interference with personal liberty and private property. The delegation is so clearly arbitrary, and so clearly a denial of rights safegu[a]rded by the due process clause of the Fifth Amendment, that it is unnecessary to do more than refer to decisions of this court which foreclose the question.

Id. at 311. Based on that early decision, it would seem that the type of delegation in which the DMCA engages cannot withstand scrutiny. "Congress may not constitutionally delegate its legislative power to another branch of Government." *Touby v. United States*, 500 U.S. 160, 165 (1991). It would seem, a fortiori, that it may not delegate its lawmaking role to a nongovernmental body such as the amorphous standards-setting consortium envisioned by the DMCA. *Demko v. United States*, 216 F.3d 1049, 1054 (Fed. Cir. 2000) (upholding law because "Congress has provided sufficient boundaries to the ATF's authority").

Yet that very "delegation doctrine" has been reserved for what Judge Leventhal terms "the extremist instance." *Amalgamated Meat Cutters and Butcher Workmen of N. Am., AFL-CIO v. Connally*, 337 F. Supp. 737, 762 (D.D.C. 1971). It has been invoked on only the rarest of occasions. *See* Bernard W. Bell, *R-e-s-p-e-c-t: Respecting Legislative Judgments in Interpretive Theory*, 78 N.C. L. REV. 1254, 1308 (2000) (canvassing literature on nondelegation doctrine); David McGowan & Mark A. Lemley*, Antitrust Immunity: State Action and Federalism, Petitioning and the First Amendment*, 17 HARV. J.L. & PUB. POL'Y 293, 343-56 (1994) (examining parallel antitrust doctrine of state action). In 2001, for instance, the Supreme Court upheld delegation to the Environmental Protection Agency of

standards "for a discrete set of pollutants and based on published air quality criteria that reflect the latest scientific knowledge, [by which the] EPA must establish uniform national standards at a level that is requisite to protect public health from the adverse effects of the pollutant in the ambient air." *Whitman v. Am. Trucking Ass'ns,* 531 U.S. 457, 121 S. Ct. 903, 912 (2001) (internal quotation marks omitted).

The question arises as to how the DMCA stacks up against that delegation. As set forth above, the law itself bars circumventing "a technological measure that effectively controls access to a work," 17 U.S.C. § 1201(a)(1)(A) (Supp. 2000), and Congress expressed the hope that "technological measures will most often be developed through consultative, private sector efforts." H.R. REP. NO. 105-796, at 64 (1998). Did Congress cabin those private sector efforts, say, as much as it did the activities of the EPA approved by the Court way back in 2001? Absolutely not. In fact, beyond praising 1996-vintage "multi-industry efforts to develop copy control technologies," it offered no guidance whatsoever here. *See* H.R. REP. NO. 105-551, pt. 2 at 41 (1998). Previous laws have survived because the lawmaker "has exercised sufficient independent judgment and control so that the details . . . have been established as a product of deliberate state intervention, not simply by agreement among private parties." *FTC v. Ticor Title Ins. Co.*, 504 U.S. 621, 634-35 (1992). Yet that very defect characterizes the DMCA.

In sum, we have here "delegation running riot." *A.L.A. Schecter Poultry Corp. v. United States*, 295 U.S. 495, 553 (1935) (Cardozo, J., concurring). It would therefore seem that the DMCA might serve as the successor to the 1935-era decisions overruled by the Court as in conflict with the nondelegation doctrine. Were I writing on a blank slate, I might indeed strike down the DMCA on constitutional grounds.

But enough! Ever since the Great Chiasmus of 2313, as is well known, the role of courts has been to offer advisory opinions of a policy nature, rather than to adjudicate the lawfulness of enactments. *See* William N. Eskridge, Jr., *All About Words: Early Understandings of the "Judicial Power" in Statutory Interpretation, 1776-1806*, 101 COLUM. L. REV. 990, 1031 (2001) (quoting speaker on June 4, 1787, objecting with the quaint notion that "It was quite foreign from the nature of ye. Office to make them judges of the policy of public measures."). Accordingly, this court is without power to comment further on the seeming constitutional infirmities of the DMCA.

2. Advisability

In the foregoing spirit, this court limits itself to commenting on how advisable it might have been for Congress to adopt this provision in 1998. Already, the contemporary testimony given to Congress cast doubt on the wisdom of this provision:

> [S]uch an obligation is unreasonably onerous because hardware and software designers would be under an open-ended obligation to comply with any present or future technological marking, alteration, or distortion technology applied to any analog or digital signal. Such technologies might be technically unreasonable, inefficient, costly and unfair to consumers.

WIPO Copyright Treaties Implementation Act, Hearing Before the Subcomm. on Telecommunications, Trade, and Consumer Protection, supra, at 23 (statement of Seth Greenstein, on behalf of the Digital Media Association). Given those concerns, the question therefore arises: did Congress pass the DMCA against a background of parallel successes? In other words, had adverse parties often banded together before 1998 to implement Congressional directives, such that Congress had every confidence that they would do so again? Historical digging dispels that suspicion.

A few years before the adoption of the DMCA in 1998, Congress had passed copyright amendments designed to accommodate satellite technology. At that 1994 juncture, Congress relied on the parties to fill in the law's interstices. The Copyright Office produced a study, shortly before Congress passed the DMCA, commenting about the success of that methodology:

> Although the terms and conditions for conducting the measurements [of signal intensity] were not put in the statute, both broadcasters and satellite carriers promised Congress at the passage of the 1994 Satellite Home Viewer Act that they would privately negotiate the terms and conditions. They never did.

U.S. COPYRIGHT OFFICE, A REVIEW OF THE COPYRIGHT LICENSING REGIMES COVERING RETRANSMISSION OF BROADCAST SIGNALS 122-23 (1997). That baleful history formed the backdrop against which Congress passed the DMCA. Simply stated, the relevant parties from across divergent industries had never in the past agreed on the terms of extra-legislative decrees. There was no prospect as of 1998 that they would do so in the future. Subsequent events have only borne out the inexorability of what a sage observer would have predicted as of 1998—it took six centuries for these efforts to reach fruition!

Another problem with relying on industry to promulgate standards for technological measures was that of mutual incompatibility. One speaker posited that some copyright proprietors might in the future adopt measures that, as a technical matter, are directly inconsistent with other measures adopted by other proprietors. It would be technically infeasible under those circumstances "for a manufacturer to design a product that responds to or implements all such measures." *WIPO Copyright Treaties Implementation Act, Hearing Before the Subcomm. on Telecommunications, Trade, and Consumer Protection*, *supra*, at 23 (statement of Seth Greenstein). At bar, respondent maintains that they fall prey to precisely that predicament—it claims not to be able to comply with the technical measures promulgated by the Saturnine Standards Society without falling afield of the 2187 Decree of the Jovial Koinonia. Further investigation is required on this score. The court will appoint a special master from the Green Race to investigate that particular danger.

Respondents further maintain that even if that hurdle is vaulted, the danger of enforcing standards promulgated by the Saturnine Standards Society is that they "will freeze technology." *Id.* at 24. Certainly, the history of technology as applied to copyright is replete with numerous horror stories as to how various "advances" have in fact represented setbacks. *Cf.* Margaret Chon, *New Wine Bursting from Old Bottles: Collaborative Internet Art, Joint Works, and Entrepreneurship*, 75 OR. L. REV. 257, 261 (1996) (effectuating the "delete" command in the computer environment in order to avoid copyright infringement actually creates a new copy in an additional register, thereby implicating the owner's rights). The Green Master is admonished to sniff out parallel dangers in the instant context.

DECREE

Based on the foregoing, it is hereby ORDERED, ADJUDGED, and COMMANDED that:

- The parties will brief, within a fortnight of today's date, the question of whether the edicts of the Saturnine Standards Society truly represent an industry consensus by producing statistics showing exactly what percentage of manufacturers of which devices have subscribed to those standards;

- Such briefing shall also address when respondent began manufacture of its Havona Servitals vis-à-vis pronouncement of the edicts of the Saturnine Standards Society, and if so whether a grandfather ruling should protect respondent;

- Such briefing shall, in addition, address the conundrum whether, to the extent that respondent has manufactured devices outside those standards, and without benefit of any grandfather clause, and assuming that respondent's sales occupy a substantial portion of the market, it no longer can be the case that the edicts of the Saturnine Standards Society represent "technological measures . . . that effectively controls access to a work" with the imprimatur of a consensus of "multi-industry efforts."

- The Green Master shall report to the court regarding the matters outlined above (mutual incompatibility, freezing technology, k.t.l.) within one month of today's date.

- The final matter left dangling is the constitutionality of the DMCA under the nondelegation doctrine discussed above. I must relegate that determination to the traditional forum of talk radio shows. In light of the extraordinary interest that this issue has garnered, I am taking the unprecedented step of ordering a full four (4) Monday afternoons be granted to this topic. The results should be duly forwarded to the Great Commissioner.

- All parties to this action are again admonished not to activate their oneirographlogisticons until conclusion of the case.

NORM PROSELYTIZERS CREATE A PRIVACY ENTITLEMENT IN CYBERSPACE

By Steven A. Hetcher[†]

ABSTRACT

This article explores an important development in the informal regulation of online privacy. Privacy norm proselytizers have been the leading contributors toward the recognition by Internet users of a moral entitlement to privacy in cyberspace.

This article begins by examining the non-moral social meaning of the original personal data collection practices that emerged at the World Wide Web's inception in the early 1990s. Next, it analyzes methods by which privacy activists endeavored to moralize the social meaning of online data collection. It also emphasizes that other norm entrepreneurs, namely, the Federal Trade Commission and creators of new software privacy solutions, have subsequently supported an entitlement to privacy for reasons less selfless, but no less efficacious, in terms of helping to stimulate demand for increased privacy protections. The article concludes that even though a grundnorm of respect for consumer data privacy has generally emerged in American culture, American society is only at the beginning of the difficult task of incorporating this grundnorm into its social and business practices.

I. INTRODUCTION

This is not cattle.
This is a human being.
We do not spam human beings.
We respect human beings.
Respecting human beings is good business.

---

† Associate Professor of Law, Vanderbilt University School of Law. I am grateful for comment from Robert Ellickson, John Goldberg, Mark Lemley, Eric Posner, Bob Rasmussen, Randall Thomas, Bob Thompson, and Chris Yoo. I wish to thank the members of my Spring 2001 Law of Cyberspace course at Vanderbilt Law School, where many of the ideas in the article were first explored. I am especially grateful for the expert research assistance of Janet Hirt, Steve Jordan, Tatjana Stoljarova, and Angela Vitale.

-This is the code.[1]

Over the past few years, the norms governing personal data interactions between consumers and websites have changed dramatically. There is an increasing moral sensitivity regarding the commercial collection and use of personal data.[2] The social meaning has changed from a morally-neutral to a morally-charged status.[3] Consumers now perceive a general right to privacy in cyberspace that includes respectful treatment of personal data. This change arose not by accident or necessity, but from the intentional actions of actors possessing an interest in promoting online privacy. I will designate these actors as privacy norm proselytizers and privacy norm activists.[4]

---

1. Netcreations, Inc., Advertisement, INDUSTRY STANDARD, Jul. 10-17, 2000, at 150-51.

2. The connection between the collection of personal data and personal privacy is straightforward; the more personal data that websites collect, store, and use, the less privacy that data subjects have. *See* A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1465 (2000); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1283-1286 (2000). There are two broad categories of personal data: information that can be used to identify consumers (personal identifying information: including name, postal or e-mail address) or demographic and preference information (including age, gender, income level, hobbies, or interests). The latter can be used either in aggregate, non-identifying form for purposes including market analysis, or in conjunction with personal identifying information to create detailed personal profiles. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 20 (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf [hereinafter 1998 FTC REPORT TO CONGRESS].

3. *See, e.g.*, *The End of Privacy*, THE ECONOMIST, May 1, 1999, at 21; Rep. Asa Hutchinson and Rep. Jim Moran, *Industry Needs to Take the Lead on Protection,* ROLL CALL, Jul. 10, 2000, *available at* 2000 WL8734799; Adam L. Penenberg, *The End of Privacy*, FORBES, Nov. 29, 1999, at 182; Jared Sandberg, *Losing Your Good Name Online*, NEWSWEEK, Sept. 20, 1999, at 56 (describing the "alarming prospect" of identity theft—"the worst kind of privacy violation"); Celia Santander, *Web-Site Privacy Policies Aren't Created Equal*, WEB FIN., Dec. 11, 2000. Opinion polls show increasing public concern with respect to online privacy. *See infra* note 155.

4. Norm entrepreneurs are actors who promote the change of norms. Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 909 (1996). Norm proselytizers promote norms for moral reasons which they themselves accept. Norm proselytizers, then, are a sub-category of norm entrepreneurs. Privacy activists have functioned as norm proselytizers. Robert Ellickson seeks to develop a richer vocabulary by distinguishing among a variety of specialists who supply new norms. *See* Robert Ellickson, *The Market for Social Norms*, 3 AM. LAW & ECON. REV. at 10-12 (2001). "Change agents" are actors or enforcers who are relatively early in supplying a new norm. *Id.* He distinguishes among these subcategories of change agents: self-motivated leaders, norm entrepreneurs, and opinion leaders. *Id.* The following discussion will indicate that these

Social meanings attach to social norms; one method of changing social norms is to alter their social meanings.[5] For example, changing the social meaning associated with smoking is one way to regulate cigarette smoking among teens. As long as smoking retains a cool and rebellious mystique, it will be difficult to eradicate the practice.[6] Analogously, privacy norm proselytizers are in the process of changing the social meaning associated with websites' collection and use of personal data.[7]

---

subcategories may be aptly applied to norm creation in cyberspace. In addition, I will suggest that the norm proselytizer is aptly viewed as a distinct type of change agent.

5. *See* Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943, 951 (1995) ("Any society or social context has what I call here social meanings—the semiotic content attached to various actions, or inactions, or statuses, within a particular context."); Steven A. Hetcher, Norms (1991) (unpublished Ph.D. dissertation, University of Illinois) (on file with author) (defining a social norm as a pattern of rationally or morally governed behavior maintained in a community by acts of conformity). *But see* Sunstein, *supra* note 4, at 914 (defining social norms as "social attitudes of approval and disapproval, specifying what ought to be done and what ought not to be done"). Judge Richard Posner views law and norms theory as second-generation law and economics. *See* Richard A. Posner, *Social Norms, Social Meaning, and Economic Analysis of Law: A Comment,* 27 J. LEGAL STUD. 553 (1998). Ellickson views law and norms as representing a new paradigm within the traditional law and economic approach. *See* Robert C. Ellickson, *Law and Economics Discovers Social Norms,* 27 J. LEGAL STUD. 537 (1998). Social norms theory has been the subject of a number of important recent symposia. *See* Symposium, *The Informal Economy*, 103 YALE L. REV. 2119 (1994); Symposium, *Law, Economics, and Norms*, 144 U. PA. L. REV. 1643 (1996); Symposium, *Law and Society & Law and Economics*, 1997 WIS. L. REV. 375 (1997); Symposium, *The Legal Construction of Norms*, 86 VA. L. REV. 1577 (2000); Symposium, *The Nature and Sources, Formal and Informal, of Law*, 82 CORNELL L. REV. 947 (1997). Recent law and norms literature has included a number of significant case studies. *See, e.g.,* Lisa Bernstein, *Merchant Law in a Merchant Court: Rethinking the Code's Search for Immanent Business Norms,* 144 U. PA. L. REV. 1765 (1996); Robert Cooter & Janet T. Landa, *Personal Versus Impersonal Trade: The Size of Trading Groups and Contract Law,* INTL. REV. L. & ECON. 15 (1984); Richard H. McAdams, *Cooperation and Conflict: The Economics of Group Status Production and Race Discrimination*, 108 HARV. L. REV. 1003 (1995); Mark D. West, *Legal Rules and Social Norms in Japan's Secret World of Sumo*, 26 J. LEGAL STUD. 165 (1997). None of these case studies, however, has applied law and norms methodology in an online context.

6. *See* Lessig, *supra* note 5, at 950-52.

7. On some accounts, this process may come too late. In a now famous remark, the CEO of Sun Microsystems, Scott McNealy, advised the public, "[y]ou already have zero privacy—get over it." John Markoff, *Growing Compatibility Issue: Computers and User Privacy,* N.Y. TIMES, Mar. 3, 1999, at A5. McNealy's remark is self-serving, given that it was made at the launch of Jini software, which raised privacy concerns because it enabled all electronic devices to interconnect using an identification number. *Id.* One can imagine McNealy making a statement similar to that quoted above, albeit toned down in its rhetoric, as a defendant in a civil suit, or as a witness in a congressional hearing, with

The set of normative concepts that increasingly surround the practice in popular discourse is evidence that consumers are developing a more complex normative understanding. Notably, interactions between websites and their visitors are now framed in terms of privacy. Privacy is among the most potent normative concepts of the modern age.[8] Proponents of personal data privacy have won a substantial victory now that data is widely understood to raise concerns for a new species of privacy: informational or data privacy. Not long ago, these expanded privacy concepts did not exist in either popular discourse or the moral theory lexicon.

Privacy is generally conceptualized as a right.[9] In ordinary moral understanding, rights function differently than preferences. Our preferences do not imply the existence of desired rights. By contrast, we have rights even if we do not prefer to exercise them. This is true for many individuals regarding their right of religious expression. While they may have no desire to express their religious views, they may nevertheless place value in their right to do so. So, too, with personal data. Although many people may not desire to actively control their personal data online, they may nevertheless be inclined to support such a moral entitlement.

Increasingly, a consumer's entitlement to control his or her personal data is generally recognized.[10] Where does this growing sense of entitle-

---

the implicit message that if privacy is gone already, Sun Microsystems cannot be accused of its further degradation.

8. *See, e.g.*, A. S. Berman, *Reports of Gates' Death Greatly Exaggerated*, USA TODAY, Apr. 5, 2001, at 3D (noting that Microsoft spokesperson Beth Jordan stated, "[t]here's nothing more important to Bill [Gates] than the privacy of his family and children."); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174, 179 (1999) ("Privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century." (quoting Marc Rotenberg)).

9. *See infra* note 69; *see also, e.g.*, Louis D. Brandeis and Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Simon G. Davies, *Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143, 144 (Philip E. Agre & Marc Rotenberg eds., 1997) (noting a change in society's approach from privacy protection to data protection); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497-498 (1995) (arguing that a citizen's right to participate in government depends "on the ability to control the disclosure of personal information"). Some European Union Parliament and Council Directives dealing with privacy are based on a conception of personal data protection as a fundamental civil liberty interest. *See* Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

10. Paul Davidson, *Marketing Gurus Clash on Internet Privacy Rules*, USA TODAY, Apr. 27, 2001, at 1B ("'Such a system recognizes a 'subtle but important shift' in direct marketing,' says Hans Peter Brondmo, founder of Netcentives, an opt-in e-mail firm.

ment come from? It is primarily due to the efforts of privacy norm entrepreneurs proselytizing to consumers regarding their entitlement to control over personal data.[11] The word "proselytize" is appropriate because it would be unhelpfully reductionist to describe these entrepreneurs as merely fostering preferences for data privacy in the manner that Madison Avenue seeks to create preferences. Instilling a sense of moral entitlement to data privacy is fundamentally different from instilling a preference for Coke over Pepsi. Privacy norm proselytizers seek to arouse the moral consciousness of consumers *vis-à-vis* websites' collection and use of their personal data.[12]

As consumers increasingly perceive an entitlement, there is a corresponding tendency for them to feel moral outrage at websites that fail to respect data privacy. In terms of the emerging moral framework for governing online personal data, websites ought to respect the data privacy entitlements of consumers.[13] Websites that do so may earn the trust and confidence of consumers.[14] Consumers who feel that they are disrespected,

---

'Companies used to think of customer data as theirs. They're starting to realize they're really custodians, and the customer controls the information.'").

11. Matt Richtel, *When Computers Know What a Stranger Can't*, N.Y. TIMES, Mar. 12, 2000, at C9. Marc Rotenberg "believes that Web sites should make clear what information they are capturing and give users a clear option to decline to participate." *Id.*

12. Traditional economic analysis has shied away from the topic of preference formation. This is changing, however. *See* GARY S. BECKER, ACCOUNTING FOR TASTES 3 (1996) (noting in his study of individual preferences that "preferences or tastes play a crucial part in virtually all fields of study in economics . . . . [b]ut with few exceptions, economists and political scientists pay little attention to the structure of preferences"); *see also* JON ELSTER, SOUR GRAPES (1983).

13. Jeri Clausing, *Can Internet Advertisers Police Tthemselves? Washington Remains Unconvinced*, N.Y. TIMES, June 14, 2000, at C10 (reporting that Marc Rotenberg, director of the Electronic Privacy Information Center stated "Internet users should be able to have their profiles deleted upon request"); David Cohen, *Be sure you never take a cookie from strangers*, THE GUARDIAN (London), Apr. 1, 2000, at 22 ("Some of the UK's popular internet banks are eager to point out their respect for customer privacy. 'We do not passively track visitors to our website,' says Richard Thackray, UK country manager for first-e. 'Once a customer is signed up, we keep records of all communications and may use the information for special offers, but we don't trade customer information without their prior consent.'"); Rep. Edward J. Markey, *We must act soon to protect online privacy*, THE HILL, Feb. 7, 2001 ("I believe that Congress must enact meaningful privacy protections to reflect the fundamental value that the overwhelming majority of Americans place upon this core element of freedom.").

14. *See* Katie Hafner, *Do You Know Who's Watching You? Do You Care?*, N.Y. TIMES, Nov. 11, 1999, at G1.

> That's not to say that L. L. Bean executives think that people are ready to give up their privacy. To the contrary, L. L. Bean believes that, as always, people are willing to share private information with

however, may seek to punish websites by taking their business elsewhere, reciprocating the disrespect by providing the website with false personal information,[15] or sanctioning the website through negative gossip.[16]

Commercial websites are profit-maximizing entities, and thus morality has no intrinsic relevance for them. Nevertheless, they must engage in interactions with consumers who do have complex moral psychological states. Woe be unto the website that blithely carries on as if consumers merely have a preference for data privacy in the same manner they have a preference for, say, price discounts or free gift-wrapping.[17] Thus, while

---

> those they trust, and it believes that it has its customers' trust. The company may be right. It reports that customers love the convenience. In fact, one recent caller was so charmed by the personal treatment that she thought the saleswoman recognized her voice. "That's a trusting relationship with that business," said Marc Rotenberg, executive director of the Electronic Privacy Information Center, a privacy advocacy group in Washington. Mr. Rotenberg said L. L. Bean's customers had faith that the company would not abuse the information by reselling it.

Id.

15. *See* George R. Milne, *Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue*, 19 J. PUB. POL'Y & MKTG. 16, 16 (2000). Milne succinctly summarized several studies: "When Web sites require consumers to provide information to register, many consumers provide false information. Surveys report that half the Internet users report false information about a quarter of the time." *Id.* (citation omitted). *See also* Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661, 664-65 (1999) (citing a Boston Consulting Group consumer study stating that "40% of Internet users have provided false information at least once when registering at a website"); Jerry Guidera, *Online Shoppers Often Lie To Guard Privacy, Survey Says*, WALL ST. J. EUROPE, Mar. 16, 2000, at 28.

16. ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 213-14 (1991).

17. *See The Internet's Chastened Child*, THE ECONOMIST, Nov. 11, 2000, at 80. Kevin O'Conner, founder of DoubleClick, lost his job due to his insensitivity to the issue of privacy:

> Consumer watchdogs were slow to grasp the implications of the Abacus deal—and of the fact that, in its wake, DoubleClick had quietly dropped from its website its pledge to keep users' data completely anonymously. But they woke up in January when the company announced that it had created profiles of 100,000 individual surfers and was planning to sell them to advertisers. The resulting outcry triggered an FTC probe into whether DoubleClick had engaged in deceptive trade practices, leading to a 25% drop in the group's shares in a single day and eventually, to a pledge that it would not sell the profiles after all. DoubleClick's subsequent promise not to integrate its own database

websites are not themselves moral, they may nevertheless need to address moral concerns to effectively interact with consumers. They may even hire a morally-oriented executive: a Chief Privacy Officer.[18]

It may appear naive to assume that consumers could have a pseudo-moral relationship with a distant, uncaring, and profit-maximizing website. In other areas, however, the law is available to create relationships that simulate moral relationships: this is the notion of the fiduciary. Ideally doctors, lawyers, and accountants would legitimately care about their clients' well-being. At the very least, their clients expect and pay for these professionals to act as though they care. The reason clients may trust their fiduciaries to take their interests to heart is that this is part of their contractual agreement. Similar relationships may potentially be achieved via informal social norms rather than formal legal structures. We may be moving into a world where this occurs with respect to the relationships between websites and their visitors. Many websites now expressly promise to respect their users' privacy in statements loaded with moral language. This moral language arguably creates consumer expectations that may subsequently be interpreted as constituting special, legal relationships.

Among the strongest privacy guarantees are those found on financial services firm websites. Citigroup states that it is "committed to the Citigroup Privacy Promise for Consumers."[19] Note that Citigroup designates its assertions as a promise. Other websites typically entitle their commitments as a privacy "statement" or "policy."[20] The risk of making such statements is having the language used adversely against the firm should litigation ensue. Citigroup likely calculated that the positive value of the moral language offset the potential risk. The Citigroup Privacy Promise

---

> fully with that of Abacus turns the acquisition, in the eyes of many, into a monumental flop.

Id.

18. *See* John Schwartz, *First Line of Defense, Chief Privacy Officers Forge Evolving Corporate Roles*, N.Y. TIMES, Feb. 12, 2001, at C1 (explaining that lawyers are good at making sure that a company complies with privacy laws "but being a chief privacy officer is a lot more than simply compliance. 'You have to have a fundamental commitment to—dare I say it?—morality.'"); *see also* David Bicknell, *Directors Face E-Laws Overload*, COMPUTER WKLY., Feb. 24, 2000, at 16 (stating that the burdens of complying with European privacy policies has led some companies to be pro-active and engage in "self-help" through "privacy specialists").

19. *See* Citigroup Privacy Promise, *at* http://www.citibank.com/privacy (last visited Sept. 4, 2001) [hereinafter Citigroup Privacy Promise].

20. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 823 (2000) (noting that a privacy policy is a document that is often accessed through a hypertext link on a homepage which spells out how it collects and uses personal information).

contains additional language that would be useful to a plaintiffs' class action attorney in arguing that a legally enforceable promise was made.[21]

The legal enforceability of privacy policies is currently an unsettled area of the law.[22] Some websites claim that users who use the website agree to the terms of the website.[23] This language may promote contractual interpretations of the privacy statement. Others expressly disavow any contractual reading of the document.[24] Even if not contractually interpreted, these promises may still have legal significance. The Federal Trade Commission ("FTC") has used its jurisdiction to regulate unfair and deceptive trade practices by prosecuting failures to comply with the terms of privacy policies.[25] Websites' representations may arguably create privacy expectations such that promiscuous uses of customer data are tortious.[26] More generally, Congress has regulated particularly sensitive categories of personal information, including medical and financial data and information collected from children.[27] The more websites treat all consumer personal data in a similar fashion under their privacy policies, the more they

---

21. The Citigroup Privacy Promise reads: "our most important asset is our customers' trust. Keeping customer information secure, and using it as our customers would want us to, is a top priority for all of us at Citigroup." Citigroup Privacy Promise, *supra* note 19. It later states: "We will continuously assess ourselves to ensure that customer privacy is respected." *Id.* In the space of a one-page privacy statement, then, this document uses the normatively-loaded terms, "promise," "trust," and "respect." *Id.*

22. Larry E. Ribstein, *Law v. Trust*, 81 B.U. L. REV. 553, 588 (2001).

23. *See* http://www.jcrew.com (last visited Sept. 4, 2001) ("By visiting jcrew.com you are accepting the practices described in this privacy policy.").

24. *See* http://www.weather.com (last visited Sept. 4, 2001) ("This statement and the policies outlined here are not intended to and do not give you any contractual or other legal rights.").

25. *See infra* note 31; Steven A. Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2056-59 (2000).

26. The tortious relationship between the parties is expressed in terms of unfair competition and breach of confidentiality. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1154-57 (2000).

27. Nina Bernstein, *Welfare Officials to Search Records Of Drug Treatment*, N.Y. TIMES, Sep. 25, 1999, at A1 ("Marc Rotenberg, executive director of the Electronic Privacy Information Center, a civil liberties advocacy group based in Washington, said: 'Welfare recipients are among the first to lose their privacy. But the unfortunate consequences of these tracking and matching technologies tend to make their way up the line.' A Federal law passed in the 1970's makes it a crime, with few exceptions, to disclose information about patients in drug and alcohol treatment programs without the patients' narrowly defined written consent. That consent does not allow re-disclosure for any other purposes. Experts on privacy law call the measure unique and exemplary, and contrast it to the blanket consent forms allowed in the gathering of other types of health care information."); Hafner, *supra* note 14, at G1.

invite Congress to formally treat all personal data on par with the most sensitive categories.

Why would websites expose themselves to potential liability and increased prospective regulation? In other words, what economic forces have fostered a situation where websites are the dominant suppliers of more respectful Internet privacy norms? What benefits do they receive as suppliers of these norms that have caused them to assume the costs associated with their supply? This Article addresses these questions and examines the role of privacy norm proselytizers in changing the social meaning of data collection. These changes in social meaning have increased consumer demand for privacy and, correspondingly, website supply.

This Article will first examine the original data-collection practices that emerged at the World Wide Web's inception in the early 1990s. The social meaning of these practices was non-moral. Websites benefited through the largely unrestricted collection of personal data while consumers absorbed a third-party externality in the degradation of their personal privacy.[28] These practices emerged as the first norms of online data collection. This Article will analyze the strategic relationship structures among actors that allowed these permissive norms to flourish. The persistence of these norms created a norm gap between the actual practices and the practices norm proselytizers judge to be preferable.[29]

This Article will further examine methods by which norm proselytizers endeavored to moralize the social meaning of online data collection to close this norm gap. These privacy proselytizers precipitated a norm cascade toward more respectful privacy norms.[30] Following in their wake, other norm entrepreneurs promoted the emerging moralized data norms. This Article will conclude by examining the activities of two of these new entrepreneurs—the FTC and creators of new software privacy solutions.

---

28. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998).

29. Stephen Labaton, *U.S. Is Said to Seek New Law to Bolster Privacy on Internet*, N.Y. TIMES, May 20, 2000, at A1. ("'The bottom line is that the privacy gap between the safeguards in place and the intrusions seems to be growing not narrowing . . .' said Marc Rotenberg, director of the Electronic Privacy Information Center, a research organization that studies privacy issues and technology.").

30. Sunstein, *supra* note 4, at 909 (stating that a norm cascade is a rapid shift in norms, perhaps as a result of fragile social conditions); *see also* Randal C. Picker, *Simple Games in a Complex World: A Generative Approach to the Adoption of Norms*, 64 U. CHI. L. REV. 1225, 1227-28 (describing the function of the law in "norm seeding," which is the idea that norms adopted by a small group of people may produce a norm cascade, such that the norm spreads throughout society and replaces old norms).

The current situation is far from ideal, as many websites have failed to adopt more respectful privacy practices. Other firms have endorsed such practices in word but not deed, either by posting deceptive privacy policies, or regularly violating the terms of their posted policies.[31] On the whole, improvements in consumer/website interactions have been realized. Through the efforts of norm proselytizers, a grundnorm of respect for consumer data privacy has generally emerged in American culture.[32] American society is only at the beginning of the difficult task of incorporating this grundnorm into its social and business practices.

II. THE NON-MORAL SOCIAL MEANING OF EARLY WEBSITE DATA COLLECTION

The social meaning of the initial website data-collection practices was morally neutral. The mainstream participants, the websites and their visitors, did not perceive moral claims as generated by the data-collection activities of websites. The original data-collection practices that emerged in the early, unrestrained Internet environment are described in section A. Section B discusses how these practices evolved into the permissive norms that characterized the early website industry. These norms strongly favored the interests of the website industry over the interests of consumers. As a result, a norm gap existed between the actual practices and those practices that leading norm proselytizers viewed as justified. Section C considers the normative characteristics of these permissive practices. Finally, section D utilizes informal game theory methods to model the strategic structures of early website practices. This analysis will demonstrate why the early norms were resistant to change through industry self-regulation, and hence why the norm gap persisted.

A. Initial Data-Collection Practices of the Nascent Website Industry

The Internet was initially developed in the 1960s by government-funded engineers working in American universities. This effort was one small part of the U.S. government's Cold War strategy.[33] In this early period, Internet use was mainly by academic researchers working in com-

---

31. For example, in bankruptcy proceedings, Toysmart.com recently moved to sell personal data it had collected pursuant to a specific privacy guarantee. *See infra* note 169.

32. A grundnorm is a basic norm. *See* John R. Carnes, *Why Should I Obey the Law*, 71 ETHICS 14, 19 (1960).

33. STEPHEN SEGALLER, NERDS 2.0.1: A BRIEF HISTORY OF THE INTERNET 92 (1998).

mon disciplines.[34] In Robert Ellickson's terms, these were "close-knit" groups, as the members were relatively small in number and engaged in overlapping, multiplex interactions.[35] As members in such "close knit" communities are typically able to sanction perceived inappropriate behavior, there are internal incentives to deter opportunistic behavior.[36]

This situation changed due to two developments: the invention of the World Wide Web[37] and the commercialization of cyberspace. Once the core features of the Web were in place, the Internet became easier to use

---

34. *Id.* at 99-117.

35. *See generally* ELLICKSON, *supra* note 16. These researchers might see each other at conferences; they might be former classmates, or share advisors or mentors; or they might wish to seek future employment at one another's institutions. Accordingly, there would often exist ample opportunities to sanction non-cooperative behavior, or reward cooperative behavior. Listservs such as *The Well* are of interest in this regard. *The Well* was pre-Web and non-commercial. In addition, many of its members were part of a relatively close-knit community, the Bay Area Internet *cognoscenti*. *The Well* nevertheless allowed members to interact anonymously if they wished. Predictably, serious problems arose with the community under conditions of anonymity. *See* ESTER DYSON, RELEASE 2.0 46, 217 (1998).

36. *See* ELLICKSON, *supra* note 16, at 177-79. Based on empirical studies of ranching and farming communities in Northern California, Ellickson developed the hypothesis that efficient norms will emerge in "close-knit communities." *Id.* These norms will serve as solutions to the iterated "collective-action problems" faced by the group. *Id.* at 177. The apparent implication is that website privacy norms are inefficient if they are the product of communities that are not close-knit. Thus, while these norms are indeed rapidly emerging, there is reason to fear that they may not be moving toward greater efficiency because the Internet would appear not to be close-knit. *See* Reno v. ACLU, 521 U.S. 844, 851 (1997) ("Taken together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."); Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997) ("Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet."); Dan L. Burk, *Trademark Doctrines for Global Electronic Commerce*, 49 S.C. L. REV. 695, 716 (1998) ("Notwithstanding that the Internet is and will be segmented by economic, social, and technological divisions, those divisions will not necessarily map onto the geographic, political, and economic divisions already existing offline . . . . the current technological structure of the Internet . . . ignores customary political and geographical boundaries on which much of our legal system is based."); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1276-77 (1998) (expressing skepticism that Internet norms are efficient).

37. The Web is that portion of the Internet that runs Hyper Text Transfer Protocol ("HTTP"), Transmission Control Protocol/Internet Protocol ("TCP/IP") and utilizes Uniform Resource Locators ("URLs"). *See generally* TIM BERNERS-LEE, WEAVING THE WEB (1999).

and websites proliferated.[38] As commercial websites have been the main actors in the collection and use of personal data, the commercialization of cyberspace precipitated the current concerns regarding online privacy.[39]

Early commercial websites gathered consumers' personal data either by explicitly requesting it or simply taking it. Many websites conditioned access to their websites on the provision of personal data from visitors. In other instances, consumers received discounts, coupons, or free contest entries as an inducement to provide personal information.[40] Significantly, websites deployed new technologies that vastly improved their ability to collect data from visitors. Most significant has been the development of cookies, which allow a website's server to place information about previous visits on the consumer's computer in a text file that only the server can read.[41] From the website's perspective, cookies had the distinct advantage that typical consumers were unaware that their personal data was being gathered.[42]

When using cookies, a website assigns each consumer a unique identifier,[43] so that the consumer may be recognized in subsequent visits to the

---

38. Early websites were not commercial in nature, as the National Science Foundation did not allow such activity. *See* SEGALLER, *supra* note 33, at 224-25. The Web was not available to private enterprise until the Bush Administration zoned cyberspace for commercial use. *See id.* at 297.

39. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 40.

> While American businesses have always collected some information from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of a vast amount of information. It is the prevalence, ease, and relative low cost of such information collection that distinguishes the online environment from more traditional means of commerce and information collection and thus raises consumer concerns.

Id. Increasingly, however, privacy concerns have arisen regarding data collection by nonprofit sites as well. *See* Ellen Almer*, Online Therapy: An 'Arms Length Approach,* N.Y. TIMES, Apr 22, 2000, at A1.

40. Matthew L. Wald, *Pay-As-You-Go Plan For Car Insurance*, N.Y. TIMES, Dec. 22, 2000, at F1 ("'Privacy has increasingly become sort of a premium,' Mr. Rotenberg said. 'Increasingly people will be required to give up information to obtain a good deal.'").

41. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 45 n.4; Stacee Barcelata, *How Cookies Work* (Aug. 31, 2001) *at* http://www.zdnet.com/zdhelp/stories/main/0,5594,916619,00.html.

42. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 34-42 (1999).

43. Generally, a unique identifier is connected to the machine and not to a named individual. The problem is that this is a small gap to bridge. Consequently, privacy advocates have been concerned about unique identifiers even when connected to machines and not individuals. *See, e.g.*, *Oversight Hearing on Electronic Communications Privacy Policy Disclosures Before the House Committee on the Judiciary*, *Subcomm. on Courts and*

website.[44] This allows the website to obtain consumer-specific information on each subsequent return visit to its website. Websites are most interested in gathering consumer preference or interest information, as indicated by previously accessed web pages, downloaded information, or items the user previously clicked on.[45] Once firms collect personal data, they may then aggregate it or sell it to aggregating firms that maintain databases containing profiles of named individuals.[46] With this data, online companies can individually target products and services that are tailored to consumer preferences.[47] Cookie use is rising and firms are developing more sophisticated means of data gathering.[48] Personal data is quickly becoming an important commodity.[49]

Intellectual Property, 106th Cong. 78 (1999) (testimony and statement of Marc Rotenberg, Director Electronic Privacy Information Center). Recently, both Intel and Microsoft have made efforts to tie numbers to names. *See* Edward C. Baig, *Privacy: The Internet Wants Your Personal Info. What's In It for You?*, BUS. WK., Apr. 5, 1999, at 84; Don Clark & Kara Swisher, *Microsoft to Alter Windows 98 so Data About Users Won't Be Sent to Company*, WALL ST. J., Mar. 8, 1999, at B16; Robert Lemos, *The Biggest Computer Bugs of 1999!*, ZD INTERNET MAGAZINE, Dec. 23, 1999, *available at* 1999 WL 14538475 (discussing Intel's Pentium III serial number, global unique identifiers, and two Microsoft products, Office 97 and Windows 98, that attempted to match various numbers to personal information and names).

44. An industry has emerged to market a variety of software products designed to assist websites in collecting and analyzing visitor data and in providing targeted advertising. *See, e.g.*, Thomas E. Weber*, Software Lets Marketers Target Web Ads*, WALL ST. J., Apr. 21, 1997, at B1.

45. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 45-46.

46. *See* Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, 16 COMPUTER LAW 7 (May 1999) (noting that commercial activity involving personal data is growing at rapid pace).

47. *See* Froomkin, *supra* note 2, at 1469. For example, a firm named Acxiom currently holds personal and financial information about nearly all U.S., U.K., and Australian consumers. *Id.* at 1473-74.

48. *Id.* at 1487 ("Cookies, however, are only the tip of the iceberg. Far more intrusive features can be integrated into browsers, into software downloaded from the Internet, and into viruses or Trojan horses. In the worst case, the software could be configured to record every keystroke." (citations omitted)); Free On-Line Dictionary Of Computing, *at* http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=trojan+horse (last visited Sept. 2, 2001) (defining a trojan horse as a "malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game, or . . . a program . . .").

49. The term "commodification" is not inherently pejorative. Whether, and to what extent, the commodification of personal data is a negative development depends on one's normative theory. For instrumentalist theories generally, and economic analysis in particular, "commodification," *per se*, has no *sui generis* moral meaning. The core idea of this type of normative framework is that all things of value may be put on a single scale. Thus, to commodify data, or anything else, is not to change its moral status. In fact, eco-

B. Normative Features of Unregulated Data-Collection Practices

The previous section provided a description of the initial data-collection practices of the website industry. This section begins the examination of identity theft, medical data exploitation, and data collection from children from a normative perspective.[50]

As a descriptive matter, people are normative beings. Not surprisingly, human practices and institutions have normative features. This is true of the emerging practices regarding the collection and use of personal data by websites. The unregulated website practices described in the previous section may be characterized in terms of the following normative propositions.[51]

Permissive Data-Collection Norms

1) Websites felt free to gather as much personal data as desirable from consumers.

2) Websites did not feel obligated to ask permission to gather personal data.

3) Websites did not feel obligated to inform consumers when their personal data was gathered.

---

nomic theorists may view commodification as an instrumental good, as commodifying data may promote efficiency by allowing this data to more easily reach the hands of those who will value it most. For some versions of deontological theory, on the other hand, personal data may not morally be made the subject of market exchanges. *See* Samuelson, *supra* note 26, at 1143 ("If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights."). *See generally* Pamela S. Karlan, *Not By Money But By Virtue Won? Vote Trafficking and the Voting Rights System*, 80 VA. L. REV. 1455 (1994) (explaining rationale for public policies against vote trafficking). This type of deontological theory is not the type that is implicit in most discussions of online privacy, however. Most deontologically-oriented discussions of privacy implicitly accept the notion that under proper conditions, such as when there is informed consent, a data subject may morally alienate personal data in a market exchange. *See generally* Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace,* 73 CHI.-KENT L. REV. 1295 (1998).

50. This does not mean a critical normative perspective, however. I will not seek to provide arguments regarding what I take to constitute the correct or true moral analysis of norms of Internet privacy. Instead, I will engage in what I take to be a form of social science. Similarly, H.L.A. Hart took himself to be engaging in "descriptive sociology" in THE CONCEPT OF LAW. *See generally* H. L. A. HART, THE CONCEPT OF LAW (2d ed. 1994).

51. Websites might plausibly have thought their behavior was acceptable for a couple of reasons. First, personal data is in the public domain and so available for all to use, and second, consumers benefited from the personalized marketing possibilities available as a result of the increased commercial flow of data.

4) Websites felt free to place cookies on consumers' hard drives.

5) Websites felt free to use personal data in any manner they preferred, including selling or licensing this data to third-parties.

6) Websites did not feel obligated to monitor or regulate how these third-parties used consumer data they supplied.

7) Websites did not feel obligated to allow consumers access to their data.

8) Websites did not feel obligated to provide security for personal data in their possession.

The website industry did not highlight the fact that these norms characterized its relationship with consumers and their personal data. Websites acted in ways that established these norms because it was legal and profitable to do so.[52] These practices did not reflect the websites' desire to establish socially justified patterns of obligatory behavior.[53] Accordingly,

---

52. ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? 3-4 (1994).

> A great deal of information we consider to be highly personal, and of interest to ourselves and the town gossip—our names, telephone numbers, marital status, educational accomplishments, job and credit histories, even medical, dental, and psychiatric records—is now being sold on the open market to anyone who believes he or she might be able to use such information to turn a profit. These transactions usually take place without our knowledge or consent.

Id. Commercial websites behave in this morally dubious, but commercially reasonable manner for two reasons. First, personal data is not owned and hence it is not unlawful to collect it without consent, and second, in the emerging digital economy, personal data is becoming increasingly valuable. *See* Kathryn Kranhold & Michael Moss, *Companies Are Refusing to Share Their Cookies Tracking Devices, Consumer Data Is Too Precious*, CHI. TRIB., Apr. 10, 2000, at 11 (discussing how large Fortune 500 companies are protecting online tracking devices from Internet advertising companies because consumer data is a veritable "gold mine"); *Online Privacy*, BUS. WK., Mar. 20, 2000, at 82 (comparing the stockpiles of information to an Internet gold rush). *But see* Melissa Preddy, *Metro Teenagers Take Bait, Hook Prize on the Net—They Yield on Privacy in Bid for College Cash,* DETROIT NEWS, June 15, 2000, at 1 (profiling websites that entice Internet users to give up personal information, which on the Internet is regarded as "gold dust," for money and rewards).

53. Because social justification was not a factor, it served the website industry's interests that these norms in general remained unarticulated. This highlights the fact that norms, at their core, are patterns of behavior, not rules, statements, or other linguistic entities. A norm need not be expressed in linguistic terms in order to have content, whereas a rule is by definition linguistic. A norm's content is defined in terms of its strategic structure. A norm, then, is behavior of a certain sort, which may or may not have an

the above may be characterized as constituting the permissive norms of the early website industry which created freedom and did not impose obligations or constraints on the individual website conformers.[54]

The result of the previous data-collection norms was that consumers were adversely affected in many ways. One of the most concerning activities, data collection from children, has already prompted the enactment of the Childrens' Online Privacy Protection Act ("COPPA").[55] While COPPA has reduced the amount of data collected from children, there is evidence that these activities still persist. For example, the ToySmart.com plan to sell its database containing children's personal information, contrary to its previous explicit promises, brought it under FTC scrutiny.[56] Once the FTC was involved, it discovered that this data was collected without explicit parental consent in violation of COPPA.[57] Other websites have also been recently found in violation of COPPA.[58]

Prior to COPPA, children were especially vulnerable to questionable website practices. A wide variety of detailed personal information was collected from children online through various stratagems, notably en-

---

attached linguistic component. *See* Steven Hetcher, *Norms*, *in* ENCYCLOPEDIA OF ETHICS, 909, 909-12, (Lawrence C. Becker ed., 1992) [hereinafter Hetcher, *Norms*]. When characterizing a group's norms, it is necessary to keep in mind the difference between norms and rules, as it is important to be able to look at the actual practices of groups, rather than merely going by what they express linguistically. Talk is cheap; it is conforming behavior that creates benefits for conforming groups and externalities for third parties. *See* Steven Hetcher, *Creating Safe Social Norms in a Dangerous World*, 73 S. CAL. L. REV. 1, 43 (1999) [hereinafter Hetcher, *Creating Safe Social Norms*]. Elsewhere, I adopt the term, "norm statement" or "rule" for the linguistic component of a full norm. *See* Hetcher, *supra* note 5.

54. This is noteworthy as norms theorists often write as if norms by definition express obligatory behavior *See, e.g.,* Robert Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585, 587 (1998) ("Since this article focuses on obligations, my use of "norm" conforms to philosophical usage [that a norm is an obligation.]"); Eric Posner, *Law, Economics, and Inefficient Norms,* 144 U. PA. L. REV. 1697, 1699 (1996) ("A norm can be understood as a rule that distinguishes desirable and undesirable behavior and gives a third party the authority to punish a person who engages in the undesirable behavior.").

55. 15 U.S.C. §§ 6501, 6505 (Supp. 2000).

56. *See Toysmart.com's Plan To Sell Customer Data Is Challenged by FTC*, WALL ST. J., July 11, 2000, at C8.

57. *FTC Announces Settlement With Bankrupt Website, Toysmart.com Regarding Alleged Privacy Policy Violations*, FTC Release (July 21, 2000), *at* http://www.ftc.gov/opa/2000/07/toysmart2.htm.

58. *See FTC Announces Settlements with Web Sites That Collected Children's Personal Data Without Parental Permission*, FTC Release (Apr. 19, 2001) *at* http://www.ftc.gov/opa/2001/04/girlslife.htm.

couraging children to register for contests, enroll in electronic "pen pal" programs, complete a survey, sign up for informational updates, or play a game.[59] Other websites used "imaginary" characters to request information from children, or had them sign a "guest book."[60] The FBI and Justice Department's "Innocent Images" investigation revealed that online services and bulletin boards were rapidly becoming the most effective resources used by child predators to identify and contact their victims.[61]

Another publicized harm was "identity theft."[62] Identity theft occurs when one person intentionally assumes another person's online identity. Websites themselves did not typically engage in identity theft. Rather, identity thieves availed themselves of crucial personal information conveniently available online, including an individual's social security number and mother's maiden name, as the starting point for their activities. Typically, identity thieves go on shopping sprees at the expense of their

---

59. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 4-5.

60. *Id.*

61. *See* FEDERAL TRADE COMMISSION, PUBLIC WORKSHOP ON CONSUMER INFORMATION PRIVACY: CONSUMER ONLINE PRIVACY at 192-93, 229 (June 12, 1997) (testimony of Charlotte Baecher, Director of Education Services, Consumers Union and Linda Hooper, FBI Agent) [hereinafter 1997 FTC WORKSHOP]; *see also Child Pornography on the Internet and the Sexual Exploitation of Children, Before the Senate Appropriation Subcommittee for the Department of Commerce, Justice, and State, the Judiciary, and Related Agencies*, 105th Cong. (Mar. 10, 1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress98/sac310.htm; *Crimes Against Children Facilitated by the Internet: Hearing Before the House Judiciary Committee, Subcommittee on Crime* (testimony of Stephen R. Wiley, Chief, FBI Violent Crime and Major Offenders Section), 105th Cong. (Nov. 7, 1997) *available at* http://www.fbi.gov/congress/children/children.htm. Further, anecdotal evidence indicates that many children surfing the Web claim to have experienced problems such as attempted password theft and inappropriate advances by adults in children's chat rooms.

62. *See, e.g.,* Sandberg, *supra* note 3, at 56. Indicating the seriousness of the problem, the FTC has recently appointed a person to handle the issue. *See Prepared Statement of the Federal Trade Commission on "Identity Theft" Before the Subcomm. on Technology, Terrorism and Gov't Info. of the Senate Committee on the Judiciary*, 105th Cong. (May 20, 1998) (statement of David Medine, Assoc. Dir. for Credit Practices, Bureau of Consumer Prot., Federal Trade Commission). A recently passed Act imposes a penalty of up to twenty-five years of imprisonment and fines for theft of personal identification with intent to commit an unlawful act. Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(b) (1994); *see* Laracuente v. Laracuente, 599 A. 2d 968 (N.J. Law Div. 1991) (showing typical social security number identity theft); Kurt M. Saunders and Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act,* 8 CORNELL J.L. & PUB. POL'Y 661, 671 (1999); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 470-474 (giving examples).

victims, but the possibilities for abuse will only grow as the functionality of the Internet expands. As a means of combating identity theft, privacy norm entrepreneurs advocate greater data security measures by websites.[63]

The use of private employee medical information in making employment-related decisions is an egregious, and rapidly expanding, data-collection practice. One-third of Fortune 500 companies reportedly use personal medical information in hiring, promotion, or termination decisions.[64] As a result, many individuals are declining to seek medical diagnosis and treatment in order to avoid creating a paper trail that their employers can then use against them (or their children or grandchildren in diagnosis of genetic disease).[65] It remains to be seen whether the medical privacy regulations proposed by the Clinton administration and recently endorsed by the Bush administration will remedy the current situation.

The vast majority of commercial websites are engaged in the unregulated, ubiquitous gathering and use of nonspecialized personal data.[66] Studies indicate that most people feel uncomfortable with commercial entities gathering their personal data, especially when this data can be sold to

---

63. *See, e.g.*, FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY, May 1, 2000, *at* http://www.ftc.gov/acoas/papers/finalreport.htm [hereinafter ONLINE ACCESS AND SECURITY].

64. *See* Jane Birnbaum, *Look Into It; Here's How to Protect Your Medical Records*, CHICAGO TRIB., Nov. 23, 1999, at C1; David F. Linowles & Ray C. Spencer, *How Employers Handle Employees' Personal Information Report of a Recent Survey*, 1 EMPLOYEE RTS. & EMPLOYMENT POL'Y J. 153, 156 (1997).

65. *See Testimony Before the Subcomm. on Health of the House Committee on Ways and Means on the Subject of "Patient Confidentiality"*, 105th Cong. (Mar. 24, 1998) (testimony of Janlori Goldman, Health Privacy Project Inst. for Health Care Research and Policy, Georgetown Univ.) ("In the absence of such trust, patients will be reticent to accurately and honestly disclose personal information, or they may avoid seeking care altogether for fear of suffering negative consequences, such as embarrassment, stigma, and discrimination. Along the continuum, if doctors and other health care providers are receiving incomplete, inaccurate information from patients, the data they disclose for payment, research, public health reporting, outcomes analysis, and other purposes, will carry the same vulnerabilities."); Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 22 (1997) ("[W]ide disclosure of certain kinds of information may distort individual behavior in an inefficient fashion. Fearing loss of employment and social discrimination, people will either lie to their physicians or avoid seeking care that might lead to the creation of sensitive health care or genetic information.").

66. *See Testimony Before the Senate Comm. on Commerce, Science and Transp.*, 106th Cong. (May 25, 2000) (testimony of Sheila Anthony, FTC Comm'r) *available at* http://www.ftc.gov/os/2000/05/privacyanthony.htm (last visited Aug. 7, 2001) ("The vast majority of web sites collect personal data but do not provide privacy protections.")

third parties for unrelated purposes.[67] Among the most egregious activities, the public disclosure of highly private facts, may be legally sanctioned under the common law tort of disclosure.[68] The high standards required by this doctrine will not protect against the vast majority of website data collection activities.

Julie Cohen has advocated a right to read anonymously. She provided a powerful argument that freedom of conscience implies a right to anonymously browse the Internet.[69] No such right currently exists. When a website visitor reads online and links between various websites, it is lawful for anonymous third parties to monitor and record the visitor's activities. How may individuals freely explore their sexuality or political interests with concerns about creating a perpetual electronic record that might make it difficult to enter certain professions or run for public office?

C. The Emergence of a Privacy Norm Gap

From a policy perspective, the most striking feature of the early website norms is that they were completely biased toward serving the interests of the website industry. This reflects the reality that most websites felt neither legal nor social pressure to respect the data privacy of website visitors. This indicated a gap between the existing website data collection practices and informed, alternative practices more consonant with conventional community standards.

Gaps between actual versus desirable social practices may emerge for a variety of reasons, including small group migrations or the discovery of new scientific information. Sometimes when a smaller group migrates into a larger group, some minority practices are deemed to be out of step with the morality of the majority group, and a norm gap exists between actual and desirable practice from the majority perspective.[70] In the case of ciga-

---

67. Studies indicate that consumers are particularly afraid of transfers of their personal data to unknown third parties. *See* FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 2 (July 1999) [hereinafter 1999 FTC REPORT TO CONGRESS].

68. *See, e.g.*, Eugene Volokh, *Freedom of Speech and Informational Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1055 (2000).

69. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 982-83 (1996) (arguing that digital copyright management technologies violate First Amendment Rights protecting speech and freedom of thought); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1611 (1999) (claiming that the absence of privacy norms threatens democracy).

70. The much debated topic of female genital mutilation or modification is such an instance. As members of groups that engage in this practice have migrated into popula-

rette smoking, the disclosure of new scientific information about the health impacts of smoking has opened a gap between actual and desirable practices.[71]

In the past, traditional social theory casually assumed that diffuse social forces would push groups toward closing norm gaps.[72] Rational choice theorists have subsequently demonstrated that diffuse social gap-filling will not automatically occur.[73] Whether norm gaps close depends on the strategic structures of existing practices that create and maintain the gaps and new practices that might fill the gap. Norm gaps can close automatically or, more rarely, through intentional actions. Thus, norm gaps present opportunities for norm entrepreneurs. Part II will examine the privacy norm proselytizer, a special type of norm entrepreneur that has been instrumental in closing the norm gap between actual versus desirable website data-collection practices. To fully appreciate the techniques of these norm proselytizers, it is first necessary to examine the strategic structures that perpetuated the privacy norm gap.

D. Structural Impediments to Filling the Norm Gap

Several factors converged to maintain the privacy norm gap. The first is the normative quality of interactions between websites and their visitors. Significantly, typical consumers were morally insensitive to the privacy-invasive practices of websites. Consumers did not perceive themselves as being in a strategic relationship with websites. The second factor was the relationship structure among various websites. The website industry maintained a coordination game in which negative externalities could be absorbed by third-party consumers. Examining each of these factors will

---

tions that morally criticize the practice, a gap has emerged between actual practices and practices deemed justified by the mores of the broader community. *See, e.g.*, Edward Hegstrom, *Gynecologists Report Female Circumcisions; Some Immigrants Had Operation, Study Finds*, HOUSTON CHRONICLE, Dec. 27, 2000, at A19.

71. Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 404-05 (1997).

72. *See* Ellickson, *supra* note 4, at 2.

73. Sociologists sometimes refer to diffuse social forces as bringing about changes in norms. Law and norms theorists seek instead to find rational choice explanations for the emergence of new norms:

> I suggest that a new social norm arises through a process much like the market for widgets. A norm is not the product of 'diffuse social forces,' as a sociologists [*sic*] might put it, but rather of the purposive actions of discrete individuals, especially those who are particularly suited to providing the new rule and those who are particularly eager to have it adopted.

Id. at 2.

clarify why the initial privacy norm gap was unlikely to close spontaneously.

1. Unrealized Potential for Consumer/Website Strategic Interaction

In theory, consumer/website interactions may have been capable of closing the privacy norm gap. If visitors want to be treated better and websites want more customers, a market equilibrium should emerge through Coasean bargaining in which consumers receive the level of respect for which they are willing and able to bargain. Despite favorable prospects, there are two reasons why Coasean bargaining did not produce greater privacy protection for consumers. First, consumers were not typically aware of the practices of websites or the causal connections between data collection and potential resulting harms.[74] Additionally, consumers were morally insensitive to data privacy issues: they did not perceive a moral entitlement to control over their personal data.

A Coasean bargain produces welfare-maximizing outcomes only when the parties have adequate information such that their preferences are properly connected to welfare-enhancing outcomes.[75] These connections were lacking for early website users. As discussed in section A above, methods of data gathering, including cookies, often work invisibly such that visitors are unaware that the website is collecting individualized data.[76] Even when consumers' explicit provision of personal information made them aware of website data collection, they typically remained unaware that this data could then be sold or licensed to third parties for potentially objectionable uses. Among the most fundamental dangers posed by a loss of informational privacy is the danger resulting from the aggregation of separate pieces of data into consumer profiles.[77] That a consumer's data may flow downstream and be combined with data from other sources to form comprehensive profiles would not be apparent to a typical consumer.

---

74. People's preferences do not always reflect their true interests. For example, before the dangers of smoking cigarettes became widely known, an individual might have preferred to live a healthy lifestyle and preferred to smoke, due to a lack of information that created a tension in practical reason between the two preferences. So too, an individual might desire privacy and desire to travel cyberspace, without appreciating the practical tension thereby created.

75. *See generally* Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

76. *See supra* text accompanying notes 42-43.

77. *See generally* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS (May 2000).

Thus, a Coasean bargain would not produce an efficient outcome simply because there was no bargain in the first place. Websites took advantage of their close proximity to consumers to quietly lift personal data in the absence of any agreement.

Note that the prospect of repeat play would not place a consumer in a better position to receive more respectful treatment from websites. Cooperation may typically become a preferred strategy in repeat games. Even in the context of repeat play, cooperation did not emerge, as websites were able to hide their privacy-degrading activities from their visitors.[78] For example, an individual may not receive a job promotion due to disclosure of health information purchased by his employer through a data broker. He may fail to realize the particular circumstances that diminished his chances for promotion. Alternatively, he might be unaware of the particular causal route from his data provision to subsequent privacy invasion. For example, he may begin to receive targeting emails, and still not know whether this is the result of a visit to his doctor, the filling of a prescription online, or the fact that he browsed a medical website such as WebMD.[79] Repeat play would not affect the likelihood that consumers would benefit from cooperative behavior in either situation.[80]

---

78. Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS 311, 314 (1995); *see also The Domain Name System: A Case Study of the Significance of Norms to Internet Governance*, 112 HARV. L. REV. 1657, 1676-80 (1999).

79. The failure of repeat play to produce cooperative outcomes may occur in non-cyber contexts as well. For example, a rancher and a farmer may be involved in repeat play because they are neighbors and yet one party may be able to repeatedly cause injury to the other due to the secrecy of the injurious activities. Suppose, for example, that the farmer is using chemicals on her crops that are bleaching through the soil and slowly degrading the quality of the rancher's well water. Depending on the particular chemicals, the rancher may remain ignorant of the damage for some time. Even when the rancher becomes aware of the damage, she may not be in a position to know who caused it, perhaps because the farmer has changed practices, or because a number of farmers engage in similar practices and the rancher is unsure of whose chemicals caused the damage, due to the ambiguities of underground water flow. Ellickson notes that information is one of the conditions for efficient cooperative norms to emerge. *See* ELLICKSON, *supra* note 16, at 177-78.

80. Kathleen A. Linert, *Database Marketing and Personal Privacy in the Information Age*, 18 SUFFOLK TRANSNAT'L L. REV. 687*,* 697 n.43 (1995). ("Marc Rotenberg, director of Computer Professionals for Social Responsibility in Washington, D.C., cautions against believing contentions that privacy rights and access are inherently incompatible, since that controversy is created by those that stand to gain from less legislation and more freedom of information."); *Video Service is Compiling Data on Clients*, CHATTANOOGA TIMES/CHATTANOOGA FREE PRESS, Mar. 26, 2001, at A2 (Privacy Foundation technology officer Richard Smith said he is concerned that without privacy laws, personal TV service providers are "free to do whatever they choose" with information.).

Consumers generally did not have a moral understanding of the issue

		Website: Cooperate	Website: Not Cooperate
Visitor	Cooperate	4,2	1,4
	Not Cooperate	3,1	2,3

of data collection. Accordingly, they did not perceive their personal data as entitled to special treatment by websites. Consumers did not appreciate that certain behavior by websites disrespected their right to data privacy.[81] Because consumers failed to conceptualize this relationship as moral, they failed to appreciate the strategic nature of their relationship with websites.

A relationship is strategic when each party's utility is affected, not only by its choices, but also by the choices of the other parties. The utility of website visitors is affected both by their decision to visit a particular website *and* the website's choice to engage in harmful data-collection practices. Correspondingly, the website's utilities are affected both by its choice of data-collection practices *and* by the visitor's decision to engage in repeat visits. A website and a website visitor were potentially engaged in interactions that had the following strategic structure.

Figure 1: Consumer Failure to Appreciate Potential Strategic Relationships

The northeast cell characterizes the typical situation that existed between websites and unaware consumers. The visitor, not understanding actual website practices, instinctively cooperated. The website engaged in

81. It is worth repeating that the present account takes no position regarding the objective truth, or indeed whether there is objective truth, regarding the merits of data privacy and the rest of the circle of related moral terms under discussion. The goal here is normatively sophisticated social science. This project will be most objectively undertaken if the analysis is not seen as geared toward supporting any particular substantive normative position.

permissive data-collection activities and did not cooperate. As a result, the website benefited from its highest payoff of 4 while the visitor received its lowest payoff of 1.[82]

2. Proper Coordination Equilibrium Within Website Industry Actors

This section explores the strategic relationship structures among websites that perpetuated the privacy norm gap. According to the FTC, the website industry has an overriding interest in establishing more respectful privacy norms, if only the constituent websites could coordinate their efforts to bring about a cooperative result. The FTC claimed that if the website industry was more respectful of consumer privacy, then consumers would be less fearful of the Internet and consequently more likely to engage in electronic commerce, which would benefit the website industry.[83] Under this model, the website industry's adoption of respectful privacy norms would collectively benefit it. The barrier in initiating the collective good in this model is an example of the collective action problem.

It is, however, more plausible to suppose that the benefit of increased electronic commerce is not worth the high cost that respecting privacy might impose on websites. For many websites, the most significant cost will arise simply because consumer personal data will no longer be free for their use. For small websites, the cost of developing and implementing a privacy policy may itself be significant.[84] These development costs are of marginal importance for large websites. Large or well-funded companies, however, face a much greater cost: the increased exposure to litigation resulting from making explicit representations to consumers regarding

---

82. The numbers represent the ordinal preference rankings of the players, with 1 being a player's least preferred outcome and 4 being a player's most preferred outcome. Each pair of numbers represents the payoffs to each party for each of the four possible outcomes. The left-hand number in each pair is the payoff to the row-player and the right-hand number is the payoff to the column-player.

83. 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 43.

> By providing greater access rights, businesses could increase the reliability and accuracy of data, build consumer confidence and trust, experience a public relations benefit, make better decisions based on better data, expand markets by giving consumers greater confidence in online privacy, and experience greater efficiencies if they limit information collection to only what is necessary.

ONLINE ACCESS AND SECURITY, *supra* note 63, at §2.5.1.

84. Anecdotal evidence suggests, however, that some sites avoid this cost by simply, and illegally, cutting and pasting from the privacy policies of other sites that they find on the Web. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 36 n.148.

data-collection practices.[85] Given these costs, it is plausible that most firms would prefer not to make explicit privacy guarantees on their websites even if some lessening in the expansion of electronic commerce resulted. Thus, in seeking to foster respectful privacy norms by self-regulatory means, privacy norm entrepreneurs do not face the problem of helping a diffuse industry procure a collective good.

Instead, the strategic structure of the website industry's personal data practices is a coordination game.[86] This coordination game was solved through the pervasive data collection norms examined in Part One. These are coordination norms: a practice in which each conformer receives a coordination benefit for conforming to the norm. A coordination benefit is the added benefit an actor receives for conformity, given the conformity of other participants.[87] As a simple example, if the norm in the United States is to drive on the right side of the road, then an individual conformer receives a benefit when others also conform, as she is less likely to be involved in a collision.

A coordination norm may be an equilibrium, a coordination equilibrium or a proper coordination equilibrium.[88] Equilibrium is a combination of choices in which each actor, given the choices of the other actors, has maximally benefited. No actor will regret her choice given the choices of the others. A coordination equilibrium is a combination of choices such

---

85. For example, RealNetworks recently admitted that its RealJukebox assigned a personal ID number to users and uploaded information about their listening habits to its servers. Sara Robinson, *CD Software Is Said to Gather Data On Users' Listening Habits*, N.Y. TIMES, Nov. 1, 1999, at C1. The company was subsequently slapped with a $500 million class action lawsuit for violating California's unfair business practices law. A second class action suit was filed in the Eastern District of Pennsylvania one day later. *RealNetworks is Target of Suit in California Over Privacy Issue*, N.Y. TIMES, Nov. 9, 1999, at C1. After it was reported that its RealJukebox software continually transmits personal information about its users to the company, RealNetworks publicly acknowledged that the activity was improper and issued a fix for the software. *Id.*

86. Legal norms theorists are beginning to incorporate coordination games into their analyses. *See* Hetcher, *Creating Safe Social Norms*, *supra* note 53, at 43-45 & nn.161-68; Richard H. McAdams, *A Focal Point Theory of Expressive Law*, 86 VA. L. REV. 1649, 1654 (2001).

87. *See* Hetcher, *Creating Safe Social Norms*, *supra* note 53, at 43 n.161 (1999).

88. EDNA ULLMANN-MARGALIT, THE EMERGENCE OF NORMS 81 (1977); *see* Hetcher, *Creating Safe Social Norms*, *supra* note 53, at 44. *See generally* Margaret Gilbert, *Game Theory and Convention*, 46 SYNTHESE 41 (1981). The economics literature on "network externalities" encompasses a similar but broader rational structure as not all networks with significant externalities are norms. *See generally* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects,* 86 CAL. L. REV. 479 (1998); S.J. Liebowitz & Stephen E. Margolis, *Path Dependence, Lock-In, and History*, 11 J.L. ECON. & ORG. 205 (1995).

that no one would have been better off had any single actor behaved differently. A proper coordination equilibrium is a combination of choices such that no single actor would have been as well off had any single actor behaved differently.[89]

The crucial feature of coordination norms is that actors conform to them because it is in their direct interest. Thus, once established, coordination norms tend to stay in equilibrium. This is in contrast to collective action problems in which each actor's direct interest is not to conform, but to defect or free ride. With collective action problems, conformity occurs only if the participants can incentivize cooperation due to the possibility of repeat play, a by-product of the overlapping social relationships of close-knit communities.[90] If these conditions change, the equilibrium may falter and the norm deteriorate. With coordination norms, given the conformity of others, it is in the direct interest of actors to conform to the extant practice. Thus, coordination norms are often more stable. Efficient coordination norms may also emerge in communities that are not close-knit because these norms do not require overlapping interactions to provide incentives for conformity.[91]

---

89. DAVID K. LEWIS, CONVENTION: A PHILOSOPHICAL STUDY 22 (1969). With a proper coordination equilibrium, other conformers receive a benefit when a particular actor conforms. *Id.* It is this feature that causes David Lewis to claim that "conventions" are best modeled as proper coordination equilibria. *Id.* Conventions, on Lewis' well-known account, are maintained in part by sanctions. *Id*. at 44-49. Conformers sanction one another for non-conformity because it is in the interest of others that each conform. *Id.* The sanctions are meant to ensure the conformity of others. *Id*.

90. In addition to Ellickson, Robert Cooter, Richard McAdams and Eric Posner have each developed alternative accounts of how norms may serve as solutions to iterated collective action problems. Cooter focuses on the importance of the psychological phenomenon of "internalization," whereby conformers internalize the pro-conformist attitudes necessary to maintain productive norms. *See* Robert D. Cooter, *Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant,* 144 U. PA. L. REV. 1643, 1690-94 (1996). McAdams emphasizes the role of "esteem" sanctions, which, as he argues, solve the second-order collective action problem created by the need for group sanctions to incentivize conformity with desirable social norms. *See* McAdams, *supra* note 71, at 342 (stating that the "theory of origin and growth of norms" in which "the initial force behind norm creation is the desire individuals have for respect or prestige, that is, for the relative esteem of others"). Finally, Posner argues that cooperation in Prisoner's Dilemma games is due to the desire of putative cooperators to "signal" that they are good types rather than bad types, and thus players worthy of future cooperation from other players. *See* Eric A. Posner, S*ymbols, Signals, and Social Norms in Politics and the Law,* 27 J. LEGAL STUD. 765, 767-68 (1998). *See generally* ERIC A. POSNER, LAW AND SOCIAL NORMS (2000).

91. Hetcher, *Creating Safe Norms*, *supra* note 53, at 9.

The present concern is whether website practices are best modeled as coordination norms. The core feature of a coordination norm is that, given the conformity of others, an actor receives a coordination benefit from conforming. This condition is met in early website data-collection practices: given that most other websites are acting disrespectfully, a particular website has a direct interest in likewise disrespecting consumers. By conforming, websites obtain use of valuable personal data at less expense and effort, and avoid the worry of exposing themselves to legal liability by making explicit representations to consumers.

In addition, it is plausible that websites also prefer that the website industry generally disrespects consumer privacy. First, websites can more easily collect personal data when consumers are ignorant of website practices. Thus, all websites will be hurt when individual websites explicitly disclose their data gathering activities. The greater the public awareness, the more likely that consumers will be wary of particular websites' activities and pressure websites to alter their practices toward greater respect. Second, should litigation arise, this will facilitate dismissal of consumer claims to a reasonable expectation.[92] If most websites are collecting data at will, with no privacy safeguards in place, then the website-defendant will have a colorable defense to plaintiffs' central claims of a reasonable expectation of privacy.[93]

From this dynamic, industry insiders might be expected to discretely promote disrespectful norms through industry leader meetings, as doing so will strengthen the norm and likewise their safe harbor. This will strengthen these disrespectful website coordination norms. The original website data collection norms appear then to be proper coordination equilibria: each particular website is not as well off had either it or another website not conformed to the disrespectful privacy practices. This situation is represented in the following payoff matrix.

Figure 2: Website Industry Coordination Game

---

92. *See, e.g.*, Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 364-65 (2000) (noting that "[a]ssurances of privacy protection by e-commerce vendors and Internet service providers demonstrate that the commercial side of the Internet recognizes that respect for privacy is a significant expectation of Internet users" (footnotes omitted)).

93. *See also* Andrew B. Buxbaum and Louis A. Curcio, *When You Can't Sell to Your Customers, Try Selling Your Customers (But Not Under the Bankruptcy Code)*, 8 AM. BANKR. INST. L. REV. 395, 411-12 (2000) (arguing that the appearance of privacy policies would create an expectation of privacy).

		Other Websites: Respect Privacy	Other Websites: Disrespect Privacy
Website A	Respect Privacy	2,2	1,3
	Disrespect Privacy	3,1	4,4

The matrix in Figure 2 depicts the website payoffs depending on whether websites individually, as well as the industry as a whole, participate in personal data collection practices that either respect or disrespect the privacy of consumers. Note that whether websites respect or disrespect privacy affects the payoff to a typical website, Website A. The dominating preference is to disrespect privacy: Website A prefers to disrespect privacy regardless of the activities of other websites. Thus, A's payoffs are higher in the southern, as opposed to the northern, cells. Website A receives an additional coordination benefit when other websites also disrespect privacy. Thus, the payoff for A is higher in the southeast cell as compared to the southwest cell. Website A least prefers the northeastern cell scenario where it respects privacy and other websites disrespect privacy. In this situation, there will be no noticeable increase in electronic commerce because A's activities alone will not affect consumer confidence, and yet A has lost all the benefits from the free receipt of user data.

Like A, other websites prefer to disrespect privacy, so their highest payouts come in the eastern cells. They also prefer that A likewise disrespects privacy, due to the coordination benefit of keeping consumers in the dark. Thus, the other websites receive higher payoffs in the southeast, as compared to the northeast, cell. If the other websites are respecting privacy, however, they will likely prefer that A do the same so A is not at a competitive advantage. Thus, their payoff is higher in the northwest, as compared to the southwest, cell.

The southeastern cell outcome—where all websites disrespect privacy—is a stable equilibrium. No website has an incentive to change its behavior nor get another website to change its behavior. Just the opposite, each website has an incentive to encourage other websites not to change their behavior. The implication is that the norm gap will not close under

these conditions. The harm resulting from these practices—the degradation of personal privacy—is successfully externalized onto Web-surfing consumers.[94] Some commentators conclude that the failure of informal forces to adequately handle these externalities mandates direct governmental intervention.[95]

In the discussion in Part III below, however, it will be seen that omnibus government regulation of website practices has not been required to bring about more respectful privacy norms. The FTC has been actively involved, but its role is that of a norm entrepreneur rather than a norm imperialist. The FTC has been among a number of norm entrepreneurs, each contributing to a more respectful online privacy environment. As Part III explains, the lead role was played by public-interest privacy activists functioning as norm proselytizers.

III. PRIVACY ACTIVISTS MORALIZE THE SOCIAL MEANING OF DATA COLLECTION

The following discussion explores the actors working to close the privacy norm gap. These privacy norm proselytizers have partly overcome the factors maintaining this gap that were explored in Part I. The emergence of the grundnorm of industry respect for consumer privacy by websites is the story of how privacy activists working in their capacity as norm proselytizers have successfully changed the social meaning of data collection from a predominantly non-moral to a morally-charged activity. Consumers increasingly feel entitled to respectful treatment from those who handle their precious personal data. This dramatic change in the consumer/website relationship did not emerge spontaneously but was due to the conscious efforts of privacy activists.

The section A below examines the concept of social meaning generally. Sections B and C explore methods through which privacy activists have moralized the social meaning of data collection and the dimensions of this new morality. Finally, section D examines the impact of this change in social meaning on the strategic relationship between consumers and websites.

---

94. Similarly, the possibility of externalization of the costs of an industry custom is one reason why the established "rule of custom" in tort law is that conformity to industry custom may serve as evidence of due care, but is not dispositive. *See* Hetcher, *Creating Safe Norms*, *supra* note 53, at 73.

95. *See generally* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L. J. 771 (1999).

A. Social Meaning and Social Norms

Among the key insights of recent law and norms literature is the connection between norms and their social meanings. The best approach to changing a social norm may be to change its social meaning. To illustrate this, Larry Lessig discusses dueling by the aristocratic class in the Old South.[96] The dueling norm was resistant to legal prohibition, as making dueling illegal left intact its social meaning: participation was perceived as honorable, refusal as cowardly. A more promising approach was to change dueling's associated social meaning by making it illegal for duelers to hold the honorable position of public office.[97] This changed the social meaning such that potential participants were able to decline duels without losing honor due to the credible claim that the refusal was motivated by the esteemed prospect of holding public office.[98]

With other social norms, however, the affiliated social meaning may be very difficult to change. With gun possession by juvenile members of street gangs, the challenge is to shift the social meaning from one in which gang members enhance their relative status by challenging authority through handgun possession.[99] The perverse logic of the illicit handgun possession norm and its affiliated social meaning is that the greater the legal sanction against the activity, the greater the peer status for continued participation.[100]

With personal data collection, the goal of norm entrepreneurs has been to shift the social meaning from a morally neutral to a morally-loaded significance. Two differences exist between data-collection norms and norms such as gun possession and dueling, both of which uniquely complicate the privacy activists' task. In the previous examples, the norm conformers are also the primary intended beneficiaries of the proposed new norm. With data collection, however, it is website visitors who are the main group of intended beneficiaries, not the websites themselves.

A second difference is that the goal in the above examples was to reduce or eliminate behavior. With personal data collection practices, however, the goal is more complex. The purpose is not to completely eliminate

---

96. Lessig, *supra* note 5, at 968-73.

97. *Id*. at 971-72.

98. *Id*.

99. *See generally* Dan M. Kahan, *Social Influence, Social Meaning, and Deterrence*, 83 VA. L. REV. 349 (1997).

100. Likewise, with cigarette smoking, the challenge is to shift the social meaning away from the current situation whereby teen smoking is considered cool. The more that authorities try to control smoking, the cooler it may seem. *See* Lessig, *supra* note 5, at 1025-34.

the collection and use of personal data by websites, but rather to put this practice on firmer moral ground. Balancing websites' benefits from disrespectful collection practices and the desire not to eradicate data collection entirely, it seems especially difficult for privacy norm entrepreneurs to bring about a more respectful and nuanced result.

The next section addresses the manner by which privacy proselytizers have approached the difficult task of changing the meaning of personal data collection in cyberspace. As this section demonstrates, the logical first step was to fit the relevant practices into a broader normative framework. Privacy proselytizers were then in a position to evaluate potential demands placed on websites that respect privacy. Finally, the activists proselytized to convince the public to accept their moral position.

B. Internet Privacy Activists' Proselytizing Efforts

Privacy regulation in the United States has consisted of applying the concept of privacy to new situations that resulted from emerging technologies. Brandeis and Warren's famous article, for example, was a response to the new privacy threat posed by the invention of the camera and its subsequent use by the media.[101] The seminal Supreme Court cases, *Olmstead v. United States*[102] and *Katz v. United States*,[103] resulted from the development and use of telephone wiretapping technology by law enforcement officials.

A generation ago, the pre-Internet electronic privacy advocates highlighted the threat that government computers posed to privacy.[104] The threat arose from U.S. Government plans to use computers to construct a comprehensive personal information database on its citizens. While privacy activists continue to perceive government as a threat to personal privacy, the focus of attention has changed in recent years to the private domain. The single most significant impetus for this change has been the emergence of the Internet and the associated website industry.

When government was the perceived threat, privacy activists invoked the Fourth Amendment of the U.S. Constitution with some degree of success. When the main threat to privacy came from private entities such as

---

101. *See* Brandeis and Warren, *supra* note 9.

102. Olmstead v. United States, 277 U.S. 438 (1928).

103. Katz v. United States, 389 U.S. 347 (1967).

104. The privacy advocacy community formed in the 1960s to fight against wide-scale personal data collection and aggregation by agencies of the U.S. government, newly armed with mainframe computers. *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306-08 (1989); PRISCILLA M. REGAN, LEGISLATING PRIVACY-TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 70-71 (1995).

websites and Internet companies like DoubleClick, legal claims in favor of data privacy have had little success. It has been argued that these websites violated one or more privacy torts,[105] or engaged in unfair trade practices.[106] Attorneys have proposed that when websites plant cookies on the hard drives of consumers they commit trespass to chattels.[107] On the whole, however, none of these legal arguments has provided much protection against the majority of website data practices. Privacy activists instead place great reliance on claims that website practices are immoral.

In recent years, a number of public-interest organizations have identified online privacy as an important public-policy concern. These groups include the Electronic Privacy Information Center ("EPIC"), the Electronic Frontier Foundation ("EFF"), and the Center for Democracy and Technology ("CDT"). Particular individuals, notably Marc Rotenberg and Richard Smith, have become highly visible advocates for online privacy. Rotenberg, the Director of EPIC, is the best known "inside-the-beltway" proponent of electronic privacy. Smith is a so-called "ethical hacker," who works to expose new forms of privacy invasion.[108] As online privacy has become a highly publicized topic, shapers of public opinion, such as New York Times columnist William Safire, have also recently begun to proselytize.[109]

The privacy activist community has employed several strategies to further its goals: activists have functioned as industry watchdogs, legislative proponents, and worked closely with the media. Through these activities, privacy activists have pursued the related aims of education and effecting a change in moral perspective. They have sought to educate the public, politicians, and the media regarding factual issues relating to data collection *and* have striven to change these groups' moral perspective regarding their personal data.

Activists have sought to inform the public of the causal connection between privacy and website data-collection activities because the potential harms resulting from an inability to control personal data are not readily

---

105. *See In re* Doubleclick Inc. Privacy Litigation, No. 00CIV 0641 NRB, 2001 WL 303744 (S.D.N.Y. Mar. 28, 2001).

106. *See infra* text accompanying notes 184-185.

107. *See* Seth R. Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, 632A PRACTICING LAW INSTITUTE 187, 217-18 (June 2001).

108. *See, e.g.*, *Privacy champion defeating Net threats one by one*, SAN DIEGO UNION-TRIBUNE, Apr. 18, 2000, at 10. Richard M. Smith is a software expert who does not fully trust his own kind. *Id.* As a result, he has launched a personal crusade to expose technology practices that threaten the privacy of millions of Internet users. *Id.*

109. Ellickson refers to "opinion leaders." *See* Ellickson, *supra* note 4, at 12-13.

apparent.[110] It is widely believed that consumers are not significantly harmed by identity theft, as fraudulent credit card billing is insured beyond a $50 deductible.[111] In fact, the real danger from identity theft is the potential for serious harm to consumer credit records.[112] The lack of education also frustrates public appreciation of the connection between private medical data and potential damage to public health. The media presented stories connecting the flow of medical information with harms that include failure to seek medical treatment for fear of an electronic trail that could later affect employment opportunities.[113]

The bare knowledge of potential consumer harm does not inherently carry any moral implication. No moral implication follows, for example, from dental-hygiene advocates informing the public of the harmful results of plaque. Thus, establishing a moral connection between website activities and consumer harms was a core goal of the privacy norm proselytiz-

---

110. *See* Lemley, *supra* note 36, at 1276. Non-consensual website interactions are:

> particularly likely when incentives are asymmetrically distributed in the community, as when buyers and sellers have their own conflicting norms. The norm that results from this conflict may represent a variety of things besides consensus: superior bargaining power on the prevailing side, collective action problems on the other side, or the use of strategic behavior.

Id. As the discussion in the main text indicates, there is an additional reason for non-consensual website interactions besides the one Lemley lists, namely ignorance on the part of visitors of the data-collection practices of websites.

111. Susan Wells, *When It's Nobody's Business But Your Own*, N.Y. TIMES, Feb. 13, 2000, at C11.

112. Hal Berghel, *Identity Theft, Social Security Numbers, and the We*b, 43 COMMUNICATIONS OF THE ACM 17, 19 (2000), *available at* http://www.acm.org/pubs/citations/journals/cacm/2000-43-2/p17-berghel ("As any victim can attest, identity theft can destroy personal credit and potentially lead to very expensive litigation that may take years, or perhaps decades, to fully correct."); Kevin G. DeMarrais, *Beware Thieves Who Steal Christmas*, THE REC., Dec. 8, 1996, at B3 ("[I]dentity thieves can establish new accounts in your name and run up big bills and debt. By the time you realize what has happened, your credit record can be in ruins and it can take months to unravel the mess."); Michael A. Gips, *Victims Describe Identity Theft*, SECURITY MANAGEMENT ONLINE, *at* http://www.securitymanagement.com/library/000901.html (last visited Aug. 3, 2001).

113. Dan Stimson, *Internet security an issue for telemedicine success*, ALBEQUERQUE TRIB., Aug. 16, 1999, at A6 ("Exposure of private medical information can affect a person's ability to acquire employment . . . ."); *President to toughen medical privacy rules*, THE SUNDAY GAZETTE MAIL (Charleston), Aug. 20, 2000, at 6B ("Public opinion polls show that Americans are increasingly concerned about privacy in general and want greater protection for medical records, in particular. Some people say they shun testing for cancer, HIV infection and other conditions because they fear discrimination in . . . employment.").

ers. Norm entrepreneurs have advocated a moral relationship of responsibility between the data practices of websites and consumers' loss of privacy and have not dismissed consumer privacy loss as a necessary casualty of the emergence of electronic commerce. This is a moral criticism that has a distinct deontological or Kantian flavor: websites are effectively charged with treating people as mere means to an end. First, consider briefly a broad survey of the steps that privacy proselytizers have taken to promote their goals.

Ethical hackers and corporate watchdogs have been highly successful in discovering dubious website practices. Among the best examples of privacy activism targeting private companies surrounded DoubleClick's acquisition of Abacus Direct. Its intention was, contrary to earlier representations, to combine the online and offline personal data from both enterprises. The advocacy community brought the plan to the attention of the media, which gave generous attention to the story. The price of DoubleClick's stock dropped precipitously as the story unfolded in the press, destroying billions of dollars of the company's market capitalization.[114] The company has subsequently been embroiled in lawsuits and subjected to a heightened level of scrutiny from privacy activists and the FTC.[115]

Another example of successful privacy activism occurred when ethical hackers discovered that Microsoft was building a tracking utility into its software and RealNetworks was tracking the online activities of its customers.[116] The media coverage of these stores typically included a quote

---

114. *See The Internet's Chastened Child*, *supra* note 17, at 80.

115. *See* Jeri Clausing, *Privacy Advocates Fault New DoubleClick Service*, N.Y. TIMES, Feb. 15, 2000, at C2; *Privacy on the Internet*, N.Y. TIMES, Feb. 22, 2000, at A22; *Marketing the DoubleClick Way*, INDUSTRY STANDARD, Mar. 13, 2000; Will Rodger, *Activists charge DoubleClick double cross*, USA TODAY.COM (June 7, 2000), *at* http://www.usatoday.com/life/cyber/tech/cth211.htm.

116. *See* David Hamilton, *The Gadfly: Privacy Cop Richard Smith is Out to Keep Companies Honest Whether Or Not They Like It*, WALL ST. J., Jul. 16, 2001 (advocacy against RealNetworks and Microsoft); *Music software 'listens in'/ Realjukebox secretly reported listeners' tastes*, NEWSDAY (New York, NY), Nov. 2, 1999, at A47 ("One of the most popular software programs for listening to music on computers is secretly sending details back to a Seattle company about customers' music preferences, including the CDs they listen to and how many songs they copy, a security expert found. The company, RealNetworks Inc., acknowledged that information from its free 'RealJukebox' software, used by more than 12 million people, is sent via the Internet to its headquarters."); *RealNetworks is target of suit*, *supra* note 85, at C1. There were also other examples involving plans to sell data to third parties by Toysmart.com and AOL. *See infra* note 169 (Toysmart.com); Marcelo Halpern and Ajay K. Mehrotra, *From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age*, 21 U. PA. J. INT'L. ECON. L. 523, 536-37 (2000) (noting the reaction of AOL users to a

from a privacy advocate regarding the threat to personal privacy posed by the technology.[117] Once under the media spotlight, these companies quickly backed away from their planned activities.[118]

In an effort to promote laws that will create greater compatibility between positive law and the personal data norms that they promote, privacy activists have engaged in legislative activities. Marc Rotenberg, for example, has repeatedly testified before Congress in support of privacy legislation.[119] Rotenberg is credited with the Digital Millennium Copyright Act provision that could serve as a loophole if the Act fosters a regime of content licensing that requires unduly invasive monitoring.[120] Privacy activists

---

potential change in AOL's privacy policy permitting personal data sales to third parties. AOL users protested strongly and AOL decided not to alter the privacy policy).

117. *See, e.g.*, Steve Pain, *Big Brother in Disguise to Play Internet-Spy*, BIRMINGHAM POST, Mar. 13, 2001, at 24 (quoting Richard Smith).

118. *Online Ad Agency Gives Up Plan To Sell Data; DoubleClick Bows To Privacy Advocates*, ST. LOUIS POST-DISPATCH, Mar. 3, 2000, at C6.

> Bowing to intense pressure from government authorities, investors and privacy advocates, Web advertising firm DoubleClick on Thursday backed off plans to amass a giant online database of people's names and Internet habits. DoubleClick's reversal was applauded immediately by several leaders of the broad backlash against Web-privacy intrusions. Weeks of legal actions and government probes into DoubleClick Inc. have placed the online company at the center of a growing clash between businesses seeking to exploit the Internet's pervasiveness and those fearful of the consequences. "This is a great step forward for Internet privacy," said Ari Schwartz of the Center for Democracy and Technology, a Washington-based group that tracks civil liberties on the Internet.

Id.

119. *See, e.g., Relaxing Limits on Export and Encryption Software: Hearing on the Security and Freedom Through Encryption Act (SAFE), H.R. 695, Before the House Judiciary Comm., Subcomm. On Courts and Intellectual Property*, 105th Cong. (Mar. 20, 1997) (testimony of Marc Rotenberg, Director, Electronic Privacy Information Center); *Computer Technology Security: Hearing on CyberAttack: The National Protection Plan and its Privacy Implications, Before the Senate Judiciary Comm., Subcomm. On Technology, Terrorism, and Government Information*, 106th Cong. (Feb. 1, 2000) (testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center); *Electronic Privacy: Hearing on HR 5018 "Electronic Communications Privacy Act of 2000," HR 4987, "Digital Privacy Act of 2000," and HR 4908, "Notice of Electronic Monitoring Act"*, 106th Cong. (Sept. 6, 2000) (testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center).

120. *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need To Be Revised,* 14 BERKELEY TECH. L.J. 519, 544 n.138 (1999).

were also instrumental in lobbying for the enactment of COPPA.[121] More recently, they have pushed for an extension of this regulatory framework to adults.[122]

As with their watchdog activities, privacy activists have effectively utilized their media contacts to draw public attention and support for their legislative initiatives. The activists' efforts have generally been geared toward bringing media attention to online data issues and then converting the media to their normative positions. Both these efforts appear highly successful. In the recent past, the *New York Times* has contained at least one story per week touching on issues of electronic privacy. More conservative publications such as *The Economist* and *Forbes* have also given sympathetic treatment to the activists' views.[123] Because electronic privacy is currently a leading policy concern, the media's hunger for news stories is steadily growing, making it increasingly receptive to the story tips and press releases provided by the public interest advocacy groups.

The success of first generation privacy norm proselytizers is reflected by the attention of a second generation of privacy entrepreneurs, public

---

121. *See Privacy Advocate Calls for Strict Rules from Regulator, Encourages "Just Say No" Attitude from Parents Against Web Sites That Solicit Personal Data from Kids*, BUSINESS WIRE, Apr. 20, 1999 ("Junkbusters Corp. President Jason Catlett today urged Federal regulators and parents to stand firm against marketers who want to use the Internet to extract information from the nation's children. 'From Microsoft to the 'young investor' site that asked kids to report on their parents' financial assets, Internet companies have demonstrated they cannot be trusted to respect anyone's privacy. Parents and regulators must vigorously defend our children against the electronic molestation of their identities,' Catlett said."); *Privacy, For the Sake of Children*, CAPITAL TIMES, (Madison, WI) June 30, 2000, at 1D ("The Children's Online Privacy Protection Act—or COPPA, as its usually called—went into effect on April 21, 2000. Its 'enactment marked a triumph for children's advocates, who have agitated since the mid-1990s for basic protections for the Internet's youngest users.'"); *White House Starts Privacy Push*, CHICAGO SUN-TIMES, July 31, 1998, at 31 ("'On the main privacy issues, the ones that confront the country today, the administration is still reluctant to make the hard decisions,' said Marc Rotenberg, executive director of the Electronic Privacy Information Center.").

122. *See New Serious Side to Child's Play on Web*, N.Y. TIMES, Nov. 27, 1998, at A4 ("Privacy advocates have raised different concerns about the law. Marc Rotenberg, executive director of the Electronic Privacy Information Center, a privacy advocacy group in Washington, favors online privacy protections for adults, too, and would have preferred legislation based not on parental consent, but on the idea of privacy for all."); *Protecting Kids' Privacy Online*, NEWSBYTES, Mar. 11, 1999 ("'It's a parental notification law, which has some pluses and some minuses,' says Marc Rotenberg of the Electronic Privacy Information Center. 'What we really need is a base-line privacy bill for all users of the Internet. If this bill helps us move beyond industry self-regulation, we're moving in the right direction.'").

123. *See, e.g.*, THE ECONOMIST, *supra* note 3, at 21; Penenberg, *supra* note 3, at 182.

"opinion leaders," to online privacy.[124] William Safire, columnist for the New York Times, recently authored an editorial strongly endorsing the need for online privacy.[125] Remarkably, no particular privacy-related news event motivated the editorial—the topic itself has become newsworthy. Unlike many privacy activists, Safire did not either call for a legislative solution or explicitly promote a self-regulatory approach. Rather, he addressed the issue at a deeper, more philosophical level, arguing that Internet privacy is an issue of growing concern to all "lovers of freedom."[126] As this example suggests, a second success of the first generation of norm proselytizers is that online privacy is perceived as so urgent and morally cogent that it currently transcends ideological faction.

C. The Moral Meaning of Internet Privacy: Reasonable Control Over One's Personal Data

Norm proselytizers, including those advocating privacy norms, promote norms because they morally support them. The bare fact that privacy proselytizers accept similar moral principles does not mean they agree on the application of abstract moral principles to actual circumstances. Unless they take the untenable position that privacy trumps all other concerns, even strong believers in data privacy must balance this value against other values. Thus, the privacy proselytizer who has realistic hopes of winning converts among ordinary people must develop a position supporting increased online privacy that coheres with ordinary morality.

Two factors were present in the early online environment that should have deterred privacy proselytizers from quick conclusions about greater online privacy: the suspect website behavior was legal and consumers were indifferent toward online data privacy issues.[127] Typically, seriously immoral behavior is illegal. As website data collection practices were not illegal, one implication was that websites were behaving in a morally acceptable fashion. This is not dispositive, however, because when new types of behavior arise, often there is some delay before the law reacts.

---

124. Ellickson, *supra* note 4, at 12-13. Especially influential early on were the norms developed by the Organization for Economic Cooperation and Development ("OECD"), which endorsed eight "privacy guidelines." *Id*. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, has stated that OECD's eight principles for data protection are still the "benchmark for assessing privacy policy and legislation." *Oversight Hearing on Electronic Communications Privacy Policy Disclosures, supra* note 43; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980), *at* http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

125. William Safire, *Stalking the Internet*, N.Y. TIMES, May 29, 2000, at A15.

126. *Id*.

127. *See supra* text accompanying notes 73-76.

The second factor of consumer indifference is more troublesome for the privacy proselytizer. As discussed in Part I, consumers did not appear concerned about website data collection practices when they first emerged. If the consumers themselves were indifferent, could norm proselytizers intervene without appearing as norm paternalists?[128]

Paternalism is a suspect form of activity that morally coherent norm entrepreneurs avoid, as it conflicts with the widely accepted principle of autonomy.[129] To act paternalistically is to fail to respect individuals' ability to make decisions that they believe will best serve their interests. The privacy activist must sometimes recognize that many people may not care what websites do with their personal data.[130] In fact, many individuals may favor free use of their personal data because they prefer the resulting personally-tailored marketing over privacy.[131]

The paternalist seeks to assert parental authority against the inclinations of the subjects, while the proselytizer seeks to change the moral consciousness of autonomous subjects. Impressionistic evidence indicates that norm entrepreneurs have functioned in both capacities.

It is the mark of a savvy norm entrepreneur to spot a situation that is ripe for the emergence of a new norm. A norm may sometimes receive

---

128. A norm paternalist is one who seeks to enforce norms of behavior out of paternalistic motivations despite the fact that the subjects of the potential norm would not themselves prefer the change. It is typical to discuss paternalism in a legal context. The norm proselytizer has a wider scope of interest, however, one that includes both the formal legal domain and the informal social domain. Thus, the norm paternalist would seek to exert paternalistic authority against the inclinations of the norm subjects in both the formal and informal domains.

129. *See* JOHN STUART MILL, ON LIBERTY (1859), *reprinted in* ON LIBERTY AND OTHER ESSAYS, at 14 (John Gray ed., Oxford Univ. Press 1991); Richard J. Arneson, *Mill Versus Paternalism*, 90 ETHICS 470 (1980); Jean Braucher, *Defining Unfairness: Empathy and Economic Analysis at the Federal Trade Commission*, 68 B.U. L. REV. 349, 384-87 (1988); Joel Feinberg, *Legal Paternalism*, 1 CAN. J. PHIL. 105 (1971); *cf.* Danny Scoccia, *Paternalism and Respect for Autonomy*, 100 ETHICS 318 (1990).

130. *Laws Should Define Who Owns 'Our' Data*, NEWSDAY (New York, NY), Apr. 25, 2000, at A37 ("Who cares if once-intimate details of people's lives circulate from one databank to another? What important interest or principle is threatened by that?").

131. A majority of Internet users (61%) say they would be positive toward receiving banner ads tailored to their personal interests rather than receiving random ads. This represents about 56 million adult users interested in such personalization. More than two-thirds of Internet users (68%) say they would provide personal information in order to receive tailored banner ads, if notice and opt out are provided. This represents about 63 million adult users.

Excerpt from Dr. Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want*, (Nov. 1999), *at* http://www.pandab.org/doubleclicksummary.html.

widespread yet weak social support, while the latent support for a potential replacement norm is strong. Cass Sunstein discusses the attack on apartheid in South Africa, the use of the term "liberal" as a term of opprobrium, and the current assault on affirmative action, as examples of this phenomenon.[132] Eric Posner provides a similar analysis of the norms that bolstered regimes of the former Soviet republics.[133] In Poland, the population was ripe for a new regime incorporating more democratic norms because the support for the old norms was more apparent than real.[134] Similarly, contemporary online privacy activists intuitively sensed that widely-held moral concepts would assist them in quickly shifting public views from a position of indifference to moral concern.

The task of the privacy norm proselytizer varies depending on the community. In countries with generally weak commitments to privacy values, it is more difficult to proselytize for data privacy. In the United States, however, the privacy norm activists have an easier task because there is already a strong commitment to privacy.

The goal is to extend the scope of the concept of privacy to cyberspace. This is analogous to the task of animal rights proselytizers seeking to extend moral principles applicable to humans across species to other sentient creatures. Electronic privacy advocates do not extend moral principles to new species but rather to new types of situations involving the online collection of personal data. In either case, the goal is the same: to make people see a commonality where before they saw a distinction. The privacy proselytizer's core normative assertion is that individuals have a right to data privacy—though privacy activists rarely discuss why this right should exist. Indeed, it is not the task of privacy proselytizers to establish the right as an objective moral truth. Their task is to convince others to adopt their position; effective proselytizing need not involve reasoning from first principles.

The website industry accepts the proposition that consumers have some right to data privacy.[135] This is a striking admission. One might have expected the industry to take the more aggressive position that since personal data is in the public domain, websites are as entitled to use it as are the data subjects. Instead, the typical posture of industry is to acknowledge that data subjects have some special entitlement to their personal data, de-

---

132. Sunstein, *supra* note 4, at 912.

133. *See* ERIC A. POSNER, LAW AND SOCIAL NORMS Ch. 8 (2000).

134. *Id*.

135. *See, e.g.,* Walmart.com Privacy Policy, *at* http://www.walmart.com/cservice/ca_sp_privacypolicy.gsp?NavMode=3 (last visited Aug. 13, 2001) (stating that "[y]ou have the right to control your personal information as you see fit.").

spite a dearth of legal protection. The website industry's conflict with public-interest privacy advocates is over the proper conception of privacy, how much privacy is appropriate, and which thick behavioral practices should invoke the grundnorm of privacy respect. In other words, the disagreement is not over the grundnorm, per se, but which second-order norms and which thick behavioral norms should be established to promote privacy. The website industry has predictably proffered a fairly minimalist framework of practices to promote the grundnorm.

There is no monolithic view as to what the right to data privacy encompasses.[136] On one extreme, the less personal data collected and used, the better.[137] This position may have trouble winning widespread support, however, as this appears to go against consumer preferences.[138] Many consumers seem willing to trade away personal data as long as they receive valuable consideration in return.[139] Most privacy proselytizers do not seek to minimize data collection and use, but rather to change the nature of the relationship between websites and consumers from a morally problematic to a morally acceptable situation.

Norm proselytizers espouse a number of concrete norms to support the second-order norms of data privacy respect: notice, consent, access, security, and enforcement. Least controversial is the notion that data privacy rights include a right to receive notification of the uses to which websites will put personal data. At least in its public discourse, the website industry widely accepts the requirement of notice.[140] Some notion of consent or agreement is the second most often mentioned component of data privacy rights. There is, however, deep division regarding the definition and implication of consent in the context of website data gathering.[141]

---

136. Robert MacMillan, *Congress to Air Public Concerns Over Privacy*, NEWSBYTES, Sept. 5, 2000 (privacy advocates are split with some advocating very strong privacy protections).

137. *See, e.g.,* Litman, *supra* note 2, at 1287.

138. *See* Fred O. Williams, *Area Man Wins Cybercash,* BUFFALO NEWS, Oct. 28, 2000, at C1 (noting that "consumers appear willing to exchange personal data for free prizes and cash").

139. *Websites with a personal touch*, FINANCIAL TIMES (London), Mar. 15, 1999, at 6 ("Do consumers mind being asked to part with information in order to receive personalised goods and services? Most early research would suggest that they do not, so long as they perceive a benefit, such as reading a newspaper for free or saving time.").

140. *See, e.g., Harold McGraw III Says Internet Has Sparked a Revolution on Multichannel Publishing*, BUSINESS WIRE, June 18, 2001; *see also* Schwartz, *supra* note 69, at 1688-91 (noting the concept of notice being equivalent to privacy protection seems to be capturing much of the policy debate).

141. *See* Glancy, *supra* note 92, at 370.

The concept of consent is ambiguous in distinguishing between opt-in and opt-out regimes. In an opt-out regime, personal data will automatically be collected unless a consumer specifically indicates otherwise. Industry groups such as the Online Privacy Alliance have also promoted an opt-out policy.[142] The Alliance is a coalition of more than eighty companies and trade associations and was formed in early 1998 to encourage self-regulation of data privacy.[143] In an opt-in regime, the default is that personal data will not be collected unless the consumer explicitly agrees. Privacy advocates are typically advocates of opt-in.[144]

Privacy is often defined as the right to be left alone.[145] Website respect for consumer privacy cannot mean that websites should literally leave

---

> Whether Internet users in the United States must be asked to consent to each appropriation of information about their on-line activities (opt-in) or, rather, whether Internet users have implicitly consented to general use of digitized profiles of their Internet activities so that each Internet user must expressly withdraw consent to sale of such information (opt-out), remains a very contentious privacy issue.

See generally Jeff Sovern, *Opting In, Opting Out, or no Options at All: The Fight For Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

142. *See, e.g.,* http://www.privacyalliance.org/resources/ppguidelines.shtml.

> Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use.

Id.

143. *See* 1999 FTC REPORT TO CONGRESS, *supra* note 67, at 8-9.

144. Amy Borrus, *The Stage Seems Set For Net Privacy Rules This Year*, BUSINESS WK., Mar. 5, 2001.

> Instead, privacy hawks will push for so-called "opt-in" rules that require companies to get users' prior consent before collecting or sharing personal info. Opt-in is a far higher hurdle than opt-out, which allows a company to gather data until a consumer orders it to stop. Privacy gurus hope President Bush will be their strongest ally. As a candidate, Bush said customers "should be allowed to opt in to information sharing." Says Rotenberg: "This is one campaign promise we're not going to forget."

Id.

145. THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1888). With respect to privacy, the specific right articulated by Cooley was the "right to one's person." *Id.* Cooley suggested that the personal right was that of "complete immunity" from attacks and injuries." *Id.* This he characterized as the right "to be let alone." *Id.*; *see also Legislative Hearing on H.R. 3365 Drivers Privacy Protection Act of 1993 Before the United States House of Representatives Committee on the Judiciary, Subcommittee on Civil and Constitutional*

consumers alone, as consumers are the ones who visit websites. Instead, the core meaning of privacy in the context of website personal data practices is that the website should leave the visitor's data alone, except to the extent the visitor consents to her personal data being collected and used. When a consumer allows her data to be collected and used, she will have less informational privacy as a result. Note that while this collection and use would reduce privacy, it would not be an instance of the website disrespecting the visitor, because the collection and use occurred with the visitor's consent. The central moral imperative is not to minimize collection and use of personal data, but rather to gather and use a visitor's personal data in a manner that does not violate her ability to control the flow of her personal data. When a website surreptitiously collects personal data from a consumer, this bypasses her rational capacities and treats the consumer as incapable of choosing to supply her data.

In addition to notice and consent, norm proselytizers have promoted a right of access to personal data residing on the databases of websites or related entities like DoubleClick.[146] Generally, the claim is for access and the additional ability to contest or correct incorrect data.[147] The industry has generally opposed these measures, claiming that they would be unduly expensive to implement.[148] Some websites, however, have begun to make explicit offers of consumer access to data.[149]

Rights, 103rd Cong. (Feb. 3, 1994) (statement of Mary J. Culnan, Associate Professor, School of Business, Georgetown University).

146. Drew Clark, *Activists Unite To Push For Stronger Privacy Laws*, NAT'L J'S TECH. DAILY, Jan. 30, 2001.

> For the privacy advocates, the proliferation of privacy-invading technological means that Congress should pass privacy legislation rather than forcing consumers to confront privacy questions each time a new technology is introduced. "Every new service offering raises new privacy issues because Congress and the administration are reluctant to apply a new privacy standard," said Rotenberg. He praised the Edwards bill, which would require companies that make online tracking software to inform users and give them the right to access their personal data, as "probably higher up the curve in terms of good privacy legislation" than most.

Id.

147. Seventy-nine percent of American consumers rate as "absolutely essential" that customers should be afforded the opportunity of seeing their transaction records so that their accuracy can be checked and any mistakes can be corrected. Excerpt from Dr. Alan F. Westin, *The Era of Consensual Marketing is Coming*, (Dec. 1998), *at* http://www.pandab.org/1298essary/html.

148. *See* ONLINE ACCESS AND SECURITY, *supra* note 63, §2.5.1 ("For businesses this approach would lead to a substantial increase in costs, including, among others, the costs of required modifications or new design requirements placed on existing systems, new

A fourth element of the general right to data privacy is security for personal data residing in databases of commercial firms.[150] If personal data is easily accessible by hackers, the website may be causally implicated in injuring the consumer whose data is stored by the website, even if the website is not guilty of any active wrongdoing.

Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of an enforcement principle, which requires that governmental and/or self-regulatory mechanisms impose sanctions for non-compliance with fair information practices.[151] These five aspects of the general right to data privacy are accurately grouped under the notion that people have a right of reasonable control over their personal data.[152] Note that a right to reasonable control does not entail a consumer right to ownership of individual personal data.[153] If consumers own their personal

---

storage costs, new personnel costs, new legal costs and losses due to disclosure of internal practices and proprietary information . . . .").

149. *See, e.g.,* Citigroup Privacy Promise, *supra* note 19 ("We will tell our customers how and where to conveniently access their account information at http://www.citibank.com/privacy/, except when we're prohibited by law, and how to notify us about errors which we will promptly correct.").

150. Stewart Baker, *Cyberterrorism, Industrial Espionage and Crime on the Internet, Regulating Technology for Law Enforcement*, 4 TEX. REV. LAW & POL. 51, 53 (1999).

> If you are going to protect communications from cyberterrorism, if you are going to prevent people from breaking into computers and stealing valuable information, and if you are going to trust your life and your personal data to a computer, you want guarantees that the information will be kept secure. Cryptography and encryption—the ability to scramble data—are some of the building blocks of security.

Id.

151. The European Union ("EU") has recognized that self-regulation may in certain circumstances constitute "adequate" privacy protection for purposes of the EU Directive's ban on data transfer to countries lacking "adequate" safeguards. The EU has noted, however, that non-legal rules such as industry association guidelines are relevant to the "adequacy" determination only to the extent they are complied with and that compliance levels, in turn, are directly related to the availability of sanctions and/or external verification of compliance. *See* European Commission, Directorate General XV, Working Document: Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country?, (Jan. 14. 1998), *available at* http://www.europa.eu.int/comm/internal_market/en/media/data-prot/wpdocs/wp7en.htm.

152. The website industry views the norms proposed by the privacy proselytizers as unworkable and overly expensive to implement. Todd R. Weiss, *Bush Faces His First Privacy Challenge: Proposals from Industry, Advocates Differ*, COMPUTERWORLD, Jan. 22, 2001, at 7. The industry's response has been to promote less demanding norms.

153. Some proselytizers have advocated for ownership of one's personal data as the best means to secure the set of rights entailed by the second order right to data privacy. *See* Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-

data, they presumably can sell it. Once alienated, the consumer has no more claim to it than a piece of real property. The right to access personal data and secure data storage discussed above may be rights that are preferably inalienable.[154]

There is a logic of ordinary morality that applies by extension to the normative language of data privacy. For example, there are important differences between preferences and entitlements. Websites that mistreat personal data are not merely subverting consumer preferences but are violating consumers' perceived rights. This is morally offensive. Many consumers prefer that Amazon charge less for shipping and handling, but they do not feel morally outraged when Amazon fails to oblige because they are not entitled to this treatment. Consumers do increasingly feel entitled to the specific respectful treatment of their data.[155] One Internet entrepreneur summarized Internet firms' growing recognition of consumer feelings: "Companies used to think of customer data as theirs. They're starting to realize they're really custodians, and the customer controls the information."[156]

Consumers currently have little legal recourse, but they may nevertheless possess a moral response that is, from the website's perspective, functionally equivalent. Morally speaking, consumers will disdain disrespectful websites. They will view such websites as less reputable, trustworthy, and worthy of continued business relationships. More aggressive consumers may feel that disrespectful websites deserve to be sanctioned or otherwise reciprocally ill-treated.[157]

We are now in a better position to understand the distinct and interrelated functions of privacy proselytizers. First, proselytizers sought to educate the public about the causal connection between website data-collection activities and individual privacy. Advocates then sought to

---

65 (1999). Such a right would be in tension with the First Amendment, however. *See generally* Volokh, *supra* note 68.

154. *See, e.g.* Samuelson, *supra* note 26, at 1143 ("If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights.").

155. Opinion polls show increasing public concern with respect to online privacy. *See* Glenn R. Simpson, *E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise,* WALL ST. J., Jan. 6, 2000, at A24. A recent poll found that 92% of Internet users were uncomfortable about websites sharing personal information with other sites. *Business Week/Harris Poll: A growing threat*, BUS. WK. ONLINE, Mar. 20, 2000, *at* http://www.businessweek.com:/2000/00_12/63673010.htm?scriptframed.

156. *Sellers Try to Soothe Fears About Personal Data Safety*, USA TODAY, Apr. 27, 2001, at 2B (quoting Hans Peter Brondmo).

157. *See* sources cited *supra* note 15.

highlight that websites were morally harming the public through their activities. Activists further taught that consumers have a moral entitlement to a reasonable degree of control over their personal data. The following section will discuss a consequence of this moral connection: consumers utilize their strategic leverage over websites to further their moral rights and entitlements to privacy.

D. Data Privacy Rights Create a Strategic Interaction of Respect and Trust

An important strategic implication follows from the activities of privacy activists in creating a sense of consumer entitlement to personal data. As previously discussed, consumers did not view their relationship with websites as strategic until they perceived it as a moral relationship. But once consumers perceive websites as either respecting or disrespecting them, they will respectively trust or distrust websites. The more strongly consumers feel a data privacy entitlement, the more they will be morally affronted by instances where websites disrespect their privacy. Accordingly, they will be slower to trust websites and more inclined to punish those that fail to show respect. Retaliation may take the form of negative gossip or providing false or misleading information to the website.[158]

The notion of website visitors choosing to trust is similar to Richard McAdams's idea that actors can choose whether to esteem another party with whom they are interacting.[159] Note, however, that whereas McAdams plausibly contends that the desire for esteem is a brute preference that a rational actor might prefer for its own sake, I am not asserting that trust is something that websites would independently desire. Rather, a website would prefer to gain the trust of its visitors because this trust will be posi-

---

158. *See* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and Practice*, 7 J. INTELL. PROP. L. 57, 62 (1999).

> The obvious product of this distrust is that people avoid disclosing personal information by opting against online transactions and website registration. Less obvious but equally troubling for online marketers is the 'garbage in' syndrome: in two recent surveys, over forty percent of Americans who registered at websites admitted to providing false information some of the time, mainly because of privacy concerns; the figure for European registrants was over fifty-eight percent . . . . The message to marketers is clear: if you want useful and accurate data, earn it by assuring consumers that you will use it appropriately.

Id.

159. *See* McAdams, *supra* note 71, at 355-72. Similarly, Cooter's internalization account appears not to play a role as websites are commercial enterprises that are not readily susceptible to the psychological phenomenon of internalization. *See* Cooter, *supra* note 90, at 1690-94.

tively correlated with these visitors choosing to interact with the website in the future. In other words, websites hope to signal to consumers that they are desirable partners with whom to cooperate.[160] The situation becomes strategic because the website is then in the position to choose whether to respect the consumer and engender consumer trust.[161] Part of the website's choice to show respect, or not, will depend in part on its calculation of how much its choice will cause the consumer to trust the website, and how much the resultant cooperative opportunities are worth to the website.[162] The strategic structure of the situation is represented in Figures 3 and 4.

Figure 3: Large Website/Consumer Strategic Interaction

		Large Website: Privacy Policy	Large Website: No Privacy Policy
Visitor	Trust	3, 3	1, 4
	No Trust	3, 1	1, 2

Figure 4: Small Website/Consumer Strategic Interaction

Small Website: Privacy Policy	Small Website: No Privacy Policy

160. On signaling theory, see *supra* note 92. *See generally* POSNER, LAW AND SOCIAL NORMS, *supra* note 133.

161. *Gallup Poll Uncovers Opportunities to Build Consumer Confidence in 2001 by Implementing Best Practices for Online Privacy*, PR NEWSWIRE, Jan. 16, 2001.

162. Prior to the burst of the Internet bubble, the mere eventuality of future visits to the site in itself was money in the bank, as Internet companies were valued in the market in important part based on the number of "hits" the site received.

Visitor	Trust	2, 2	1, 4
	No Trust	2, 1	1, 3

Each party has two choices, each affecting the utility of the other party. Thus, each party needs to think about how its choice and the choice of the other party will affect its payoff. This means that each party considers whether they can affect the other's choice to improve his own outcome. Specifically, the website will consider whether it should attempt to foster consumer trust, and the consumer will consider whether it can influence the website's choice to provide a privacy policy.[163] Once the consumer appreciates that the website's actions will affect her outcomes, she will either withhold or bestow trust to incentivize the website to show respect.

Because of these mutually affecting choices, a greater number of websites may find it in their interest to respect privacy in order to maintain the trust of the increasingly educated, and demanding, consumer.[164] Indeed, the number of websites that show respect for privacy has continued to grow as public consciousness of the issue of online privacy has grown.[165] Note that as recently as a few years ago, only a minority of websites—the larger and better-known websites—offered privacy policies.[166] This makes sense because these websites are most likely to have overlapping, multifaceted interactions with consumers; thus making it crucial for these websites to have respectful and trustworthy reputations.

---

163. As the above discussion has indicated, there are different ways to respect privacy. A privacy policy will be used in the example as it is the most basic means.

164. *See supra* note 18 (discussing how some companies are hiring Chief Privacy Officers).

165. *See generally* 1999 FTC REPORT TO CONGRESS, *supra* note 67.

166. In the Federal Trade Commissions's 1998 study, only 14% of websites were addressing consumer privacy issues. 1998 FTC REPORT TO CONGRESS, *supra* note 2. As the consumer sense of entitlement grows, the chances of plaintiffs' lawyers prevailing in lawsuits grows. *See* Matt Fleischer, *Lawyers Eye Privacy Cases Against Many DoubleClick Rivals*, 22 NAT'L LAW J. no. 27, at A1 (Feb. 28, 2000) (noting many lawyers are now searching for the next privacy lawsuit against DoubleClick competitors, such as Engage, 24/7 Media, MatchLogic, Flycast, and L90, each collecting over 100 megabytes of clickstream data-information per day).

That websites place a premium on consumer confidence is readily indicated by the extent to which they attempt to acquire it deceptively. Many firms have deceptive privacy policies. In other words, the firm wraps itself in a cloak of respect by means of the privacy policy, and yet the actual terms of the policy are "lawyered" such that the firm does whatever it pleases with personal data.[167] The most egregious, publicly-known case occurred recently. Toysmart.com explicitly promised not to sell data: "[p]ersonal information voluntarily submitted by visitors . . . is never shared with a third party."[168] In bankruptcy, Toysmart then attempted to sell this data.[169] Despite the sense of consumer entitlement, many small websites may still prefer to avoid the expense of providing privacy policies. As illustrated in Figure 4, many small websites may still prefer the outcome of mutual non-cooperation (southeast cell) to that of mutual cooperation (northwest cell).

As a result of privacy proselytizers, a situation has emerged in which there are two types of norms. Previously, there were simply permissive norms whereby websites did whatever they wanted with personal data without regard for consumers. Now new, more respectful, norms are emerging. For simplicity's sake, the previous discussion focused solely on

---

167. *See* Schwartz, *supra* note 20, at 824.

> In light of these flaws, the true argument in favor of the Privacy Policy can only be as follows: when a Web site says something about its data processing practices—even if this statement is vague or reveals poor practice—the visitor to the site is deemed to be in agreement with these practices so long as she sticks around . . . . Thus, a site that said 'we reserve the right to do whatever we want with the information we collect' [is] deemed to have provided notice of information practices.

Id.

168. Toysmart Privacy Statement, *at* http://www.ftc.gov/os/2000/07/toyexh1.pdf.

169. *See FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, (July 21, 2000) *at* http://www.ftc.gov/opa/2000/07/toysmart2.htm; *Judge Is Urged to Reject Toysmart.com Settlement*, WALL ST. J., Jul. 26, 2000, at B2; *Toysmart.com's Plan To Sell Customer Data Is Challenged by FTC*, *supra* note 56, at C8. In addition, Toysmart faced a lawsuit filed by TRUSTe, which contended that Toysmart was in violation of its online agreement not to sell consumer data to third parties. *See* Elinor Abreu, *TRUSTe to File Antiprivacy Brief Against Toysmart*, INDUSTRY STANDARD, June 30, 2000, *available at* http://www.thestandard.com/article/display/0,1151,16577,00.html. *See generally* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1180 (1997). This example demonstrates how non-internalized the norm is for a website. This is a difference between humans and firms. Once internalized, a human conforms to a norm in a manner that cannot be readily changed. A firm's commitments can completely change with the installation of new management.

the provision of privacy policies. But as already mentioned, there are many actions websites may undertake in order to demonstrate their respect. Although this represents significant moral progress from a privacy activist perspective, a major problem remains. New, more respectful norms are now in play, but so, too, are the old nonrespectful norms.

Part IV will demonstrate that while the privacy activists may not themselves have the resources to push for universal conformity to respectful norms, these norms have taken on a life of their own. The result is that other norm entrepreneurs find it is their interest to get involved in promoting these norms. Part IV describes how both the FTC and various private companies have come to have an interest in further promoting those more respectful data norms first proselytized by the privacy activists. Before examining these norm entrepreneurial activities, however, consider briefly one additional force that may cause websites at the margin to switch to more respectful norms as a consequence of the initial efforts of the privacy activists.

E. Causal Feedback Loop Leading Toward Pooling Equilibrium

There is an apparent causal feedback loop operating: as more respectful practices emerged, consumers have become informed about online privacy, and consequentially increasingly demanding of their privacy.[170] In a criminal law context, Dan Kahan observes a parallel phenomenon whereby a rise in crime makes social sanctions less powerful, which leads to more crime.[171] In the situation described by Kahan, the causal feedback loop leads to normative breakdown. Richard McAdams describes a similar dynamic involving social norms pertaining to wearing fur and smoking cigarettes.[172] McAdams plausibly observes that these are activities in which the more people shun the behavior, the more negative the impact felt by remaining participants in the activity. This puts greater pressure on these remaining participants to abandon the activity. Depending on the utility functions of the remaining participants, the greater pressure may induce some to abandon the activity. Through continued iterations of this causal loop, all participants may, over time, defect from the activity. Alternatively, some stalwarts may have strong preferences that continuously outweigh all pressures to defect. After a time, a new equilibrium may re-

---

170. *See* Buxbaum and Curcio, *supra* note 93, at 411-12 (arguing that the appearance of privacy policies would create an expectation of privacy).

171. *See* Dan Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem,* 67 U. CHI. L. REV. 607, 611-18 (2000).

172. *See* McAdams, *supra* note 71, at 366.

sult such that these are stable populations of conformers and nonconformers.

A parallel dynamic in website privacy practices seems to be under way. As the number of websites providing privacy policies increases, the more intense will be the perception that the remaining websites are disrespectful of consumer interests. Increasingly, websites without a policy will be outliers in their disregard for consumer privacy interests. This will likely cause an increasing number to alter their behavior, possibly leading to a tipping point where most websites begin to take privacy more seriously.[173]

Whether such a feedback loop is in operation is an important question. The previously described process is self-regulating in the sense that the impetus toward the new norms comes from informal social forces rather than formal legal methods. One criticism occasionally made of self-regulation is that while it may work to motivate many, or even most, players to act in a cooperative fashion, there will still be some players—the "bad actors,"—who fail to conform. Due to the causal feedback mechanism, there may be the potential for the "bad actors" to become cooperators. For example, this may already be occurring among the participants in the Network Advertising Initiative, an industry group formed to agree on acceptable forms of privacy protection. A commentator suggested that the 10% of advertisers who did not initially comply with the industry guidelines might be led by "centrifugal force" to go along, or risk losing both respect and business.[174]

IV. STRENGTHENING THE PRIVACY ENTITLEMENT FOR NON-MORAL REASONS

A. The FTC's Threat Model of Privacy Entrepreneurship

The FTC has recently acted to reinforce the privacy promoting efforts of the privacy activists. Privacy activists are motivated because they care

---

173. This is modeled by the critical mass phenomenon of "tipping." *See* THOMAS C. SCHELLING, MICROMOTIVES AND MACROBEHAVIOR 102-04 (1978). Tipping occurs when the success of a social practice depends on the formation of a critical mass, and enough actors sign on or sign off such that the practice succeeds or fails. If enough actors sign on, the activity is tipped in. If enough actors sign off, the practice is tipped out. Because a relatively small number of crossover actors may cause a norm to tip, social norms may shift relatively suddenly. *Id.*

174. David Stout, *Government and Internet Ad Group Reach Agreement on Data Gleaned from Web Surfers*, N.Y. TIMES, July 28, 2000, at C6.

deeply about privacy. What could motivate a federal government agency to promote more respectful online personal-data practices? Elsewhere, I have argued that public choice theory provides a plausible answer: the FTC has sought to become the leading federal agency regulating online activities as a means of extending its regulatory grasp to the fertile new domain of the Internet.[175] The FTC's role in helping to moralize the social meaning of data collection can also be understood in public choice terms as an effort to extend the agency's purview over the burgeoning website industry.

As an indirect result of privacy advocacy, Congress asked the FTC to examine online privacy issues.[176] Voters are increasingly contacting their congressional representatives and voicing concerns about online privacy.[177] These concerns have translated into increased agitation on Capitol Hill regarding online privacy. This agitation has resulted in proposed legislation and calls for FTC involvement. The FTC acts pursuant to its authority under the Federal Trade Commission Act, which mandates that the agency address "unfair" and "deceptive" trade practices.[178] Generally speaking, the FTC's hook into the privacy debate comes by means of casting website data-gathering practices as potentially unfair and deceptive.[179] In particular, the agency has borrowed the various specific privacy protection measures supported by the privacy activists and shrouded them in the

---

175. *See* Hetcher, *supra* note 25, at 2053.

176. In a series of hearings in October and November of 1995 the FTC reported to Congress on consumer protection issues, including privacy concerns. *See Prepared Statement of FTC on "Internet Privacy" Before the House Comm. on Judiciary* (Mar. 26, 1998) *at* http://www.ftc.gov/os/1998/9803/privacy.htm. Brian Krebbs, *IT Industry Council Signals Privacy-Law Advocacy,* NEWSBYTES, Feb. 2, 2001 (due to public outcry lawmakers are suggesting federal electronic privacy protections); *see also PrivacyRight, Inc. Forms Strategic Equity Partnership with Venture Factory*, PR NEWSWIRE, June 6, 2000; Rosalind C. Tritt, *Privacy: A Threat to Free Speech?*, PRESSTIME, Jan. 2001, at 27.

177. Rep. Billy Tanzan, CATO Online Privacy Workshop, Washington, D.C. (May 1999).

178. 15 U.S.C. § 45(a) (1994). The FTC prosecutes "[u]nfair methods of competition . . . and unfair or deceptive acts or practices in or affecting commerce" under Section 45 of the Federal Trade Commission Act ("FTCA"). *Id.* Section 57(b) authorizes the prosecution of actions to enforce Section 45. *Id*. § 57(b). Section 57(a) permits the FTC to create rules to prohibit deceptive or unfair practice prevalent in certain industries. *Id*. § 57(a).

179. Note that the FTC's framework for regulating unfair practices does not require ownership of personal data. The fact that data subjects may have de facto control over their data is enough to generate an instance of an unfair or deceptive trade practice. This means that the agency may gain jurisdiction over website activities without a change in the intellectual property status of personal data.

rhetoric of fairness.[180] The FTC refers to standard proposed privacy measures as the fair information practice principles ("FIPPs").[181]

The FTC contends that these fair practices are best promoted through website privacy policies. In other words, websites should address the elements of notice, consent, access, security, and enforcement in the representations that they make to consumers in their privacy policy. A privacy policy that accurately and completely states the website's personal data practices would be in accordance with the principle of notice/awareness because once the consumer has notice of the website's practices, she can consent to the data exchange or exit the website. In addition, stipulations concerning access/participation to the user's personal data on file with the website can be set out in the privacy policy, as can stipulations concerning integrity/security and enforcement/redress.

Note that whereas the privacy activists promoted respect for privacy as the core moral concern, the FTC has shifted the moral focus from respect for privacy to a concern for fair practices. When websites take up the FTC's suggestion and seek to implement the FIPPs via privacy policies, the FTC's regulatory grasp is enhanced. Once websites make representations to consumers regarding their practices, the FTC has a claim to jurisdiction if the websites behave differently. From the FTC's perspective, the website has engaged in unfair and deceptive trade practices, which is directly within the FTC's jurisdiction.[182]

As a norm entrepreneur, the FTC faced a problem not confronted by the privacy activists: an unreceptive audience. As discussed in Part TwoII, privacy activists' audience is consumers. Consumers were[TENSE] naturally disposed to accepting the extension of the general right to privacy to the domain of data privacy in cyberspace and were thus generally receptive to such ideas. By contrast, the audience for the entrepreneurial efforts of the FTC were websites. Different websites had differ-

---

180. The FTC explicitly states that it takes its normative framework from the privacy policy community. *See* 1998 FTC REPORT TO CONGRESS, *supra* note 2.

181. 1999 FTC REPORT TO CONGRESS, *supra* note 67, at 3.

182. Lawsuits filed so far have involved more than simple unconsented data collection and use. *See In re* DoubleClick, Inc., Federal Trade Commission (filed Feb. 10, 2000), *at* http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Judnick v. DoubleClick, No. CV-421 (Marin Cty. Sup. Ct., filed Jan. 27, 2000), *at* http://www.perkinscoie.com/resource/ecomm/netcase/complaint1.pdf; Pamela Parker, *Doubleclick's Legal Troubles Deepen*, INTERNETNEWS.COM, *at* http://www.internetnews.com/bus-news/article/0,,3_299771,00.html (discussing four different cases against Doubleclick, Inc.); The Perkins Coie LLP Internet Case Digest, *at* http://www.perkinscoie.com/resource/ecomm/netcase/Cases-18.htm (summarizing other cases against Doubleclick, Inc.).

ing interests when it came to the provision of privacy protection for the online consumer. Generally, larger and more established websites had an incentive to provide privacy protections while smaller websites did not.[183] Importantly, the FTC's preference for websites to incorporate the FIPPs into online privacy policies provided no additional incentive to the smaller websites to provide such protections. The FTC addressed this impediment by creatively utilizing the unique resources available to it as a federal agency: it issued a threat to the website industry.[184]

In 1998, the FTC threatened to recommend to Congress that it enact privacy legislation if more respectful industry customs were not forthcoming through industry self-regulation. The threat was highly credible and particularly salient due to the Commission's recent success in shaping legislation to protect children's online privacy.[185] This threat was a shock to the normative equilibrium of the website industry, causing many firms to alter their behavior. Generally, the impact of the FTC's threat correlated with website size and structure. The larger and more multi-faceted a website's activities, the more likely it was that the website reacted to the FTC's threat by providing more respectful privacy practices.

Some large websites felt so threatened that they personally attempted to incentivize smaller websites into compliance with more respectful

---

183. Large sites are prominent and they would run the risk of coming under FTC scrutiny for questionable, albeit legal, trade practices, were they to fail to make a respectable effort to show respect for user privacy, as newly spelled out by the FTC, in its fair information practice principles. In contrast, small websites would plausibly having a dominating preference to not provide privacy policies. Because they are small, they will be able to fly under the FTC's radar. With the FIPPs, the FTC had merely outlined the principles that it contends are fair. It did not mandate them.

184. *See* Hetcher, *supra* note 25.

185. In 1998, after finding self-regulation of children's online privacy to be inadequate, the FTC recommended to Congress that it create legislation, which Congress quickly did, enacting the Children's Online Protection Act ("COPPA"). On October 21, 1998, the President signed COPPA into law. Children's Online Privacy Protection Act of 1998 Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L. 105-277, 112 Stat. 2681, 2681-728 (codified at 15 U.S.C. §§ 6501-6506) (Oct. 21, 1998).

> The stated goals of the Act are: (1) to enhance the parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to help protect the safety of children online fora such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of children's personal information collected online; and (4) to limit the collection of personal information from children without parental consent.

144 Cong. Rec. S12741-04 (Oct. 21, 1998) (statement of Sen. Bryan).

norms. Under this threat, the major websites are no longer indifferent to the actions of the smaller websites. The failure of these smaller websites to adopt privacy-respecting practices might lead to privacy legislation, which would adversely affect *all* websites. The large websites in particular would have the most to lose from onerous legislative requirements. Faced with this situation, large websites devised methods to bring small websites into conformity with more respectful data collection practices. Large websites threatened to withhold advertising from websites that did not demonstrate adequate respect for privacy.[186] As represented in Figure 5, this action changed the strategic structure of the relationship between large websites and small websites.

186. *See* Hetcher, *supra* note 25, at 2047.

Figure 5: Intra-Industry Strategic Threats

		Large Websites: Privacy Policy	Large Websites: No Privacy Policy
Small Website	Privacy Policy	4, 4	3, 2
	No Privacy Policy	2, 3	1, 1

The threats issued by some key large websites likely contributed toward the desired outcome, as an increasing number of small websites are now offering privacy policies. As indicated by the FTC's 1999 Report to Congress, the number of websites providing privacy policies has increased significantly. Regarding the issuance of threats by large websites, the FTC stated that "Companies like IBM, Microsoft and Disney, which have recently announced, among other things, that they will forego advertising on websites that do not adhere to fair information practices are to be commended for their efforts, which we hope will be emulated by their colleagues."[187]

Note that when large websites threaten to withhold advertising from small websites, the effectiveness of the threat does not depend on repeated interaction between the parties. Even if the small websites only interact once with Microsoft or IBM, they will typically prefer that this interaction permit advertising. In the terminology of informal game-theory, the instrumental allocation of advertising is functioning like a "selective incentive" that rewards cooperative behavior on an individual basis.[188] Selective incentives allow the party seeking to incentivize conformity to provide incentives to individuals in order to elicit their conformity. This is in contrast to the collective good itself, which by definition is a public good: when provided for one, it is provided for all, and thus is open to free riders.

---

187. *Id*.

188. *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1965); Lessig, *supra* note 5, at 996.

This type of selective incentive cannot be expected to work for all small websites. Some small websites will have little prospect of receiving advertising revenue from large websites and benefit extensively from the unfettered use of personal data. These websites may continue to have a dominating preference to free ride on the growing practice of providing privacy policies. Thus, the net result of the FTC threats was still a bi-normative world in which many large websites and some small websites are respectful of privacy while other small websites are not. More recently, however, a growing number of the recalcitrant websites do appear to be conforming to more respectful privacy norms.[189] The final section will explore another important process that appears to be contributing toward this development.

B. Software Makers Promote Privacy for Profit

A new type of privacy norm entrepreneur has recently emerged. These are software vendors marketing so-called "privacy solutions."[190] Privacy solutions are software that users or websites can install to create a more privacy-respecting online environment. The following discussion provides an examination of the advertisements placed by some of these software vendors for their products in tech-oriented magazines. Looking at the text of these advertisements serves two purposes: it provides strong evidence of privacy proselytizers' success in moralizing data privacy and suggests new methods by which these moralized norms may be further entrenched.

The ultimate audience for this growing type of advertisements is often websites, as they are the direct purchasers of these products. Due to the viral nature of norms, it is also integral that these advertisements impact consumers. The more the advertisements are successful in fostering moral concern among consumers, the greater the social pressure toward increased privacy protection that will be exerted on the website industry. As the price of not providing privacy increases, the number of websites that

---

189. 1998 FTC REPORT TO CONGRESS, *supra* note 2, at 17.

190. John Graubert & Jill Coleman, *Consumer Protection and Antitrust Enforcement at the Speed of Light: The FTC Meets the Internet*, 25 CAN.-U.S. L.J. 275, 290 (1999) ("In the case of Internet privacy, several technologies potentially capable of protecting the online privacy of consumers are evidently already on the market or under development. Technology-based privacy solutions may eventually provide consumers with the confidence and security that they need to conduct business on the Internet on a global scale."); *see P3P: Just a Start*, ZDWIRE, Jul. 17, 2000 ("There's no disputing that privacy has emerged as a leading issue of the Internet age. A whole industry is springing up around it, with software and service providers rushing to offer the latest and greatest solution for protecting an individual's personal information and identity online.").

will have the balance favoring of respectful over nonrespectful norms will increase.

Particularly striking is the overt normative language used in the advertisements that dramatically inform consumers that they are being disrespected by many websites. For example, consider the representative advertisement by the firm, ZeroKnowledge.[191] It depicts an average Internet user, unremarkable except for the bar code emblazoned on her neck. The text consists of a small number of rhetorical statements made by a representative online consumer to the website industry: "I am not a pair of eyeballs to be captured or a consumer profile to be sold . . . . I am not a piece of your inventory . . . . I will not be bartered, traded or sold."[192] These phrases play on current website industry jargon, in which customer visits are referred to as "capturing eyeballs," and personal data is amassed into "consumer profiles."

The theme of these statements is aptly viewed in everyday Kantian terms. The consumer is demanding more respectful treatment. As portrayed, these firms equate her with her data in contravention of the Kantian maxim that actors should not treat persons merely as a means to their own ends.[193] The import of the advertisement is that typical websites currently treat people not as individuals, but instead as "inventory" that can be bar-coded and bartered, or as "eyeballs" that can be "captured."

The advertisement then contrasts these industry attitudes with the normatively acceptable position as portrayed by a representative consumer speaking rhetorically to the website industry. "I am an individual and you will respect my privacy."[194] This brief statement contains three normatively loaded words: "individuals," "respect" and "privacy."[195] The final claim is that "On the Net, I am in control."[196] This statement is, of course, aspirational, as the whole force of the advertisement is that the woman is not presently in control of her personal data. By demanding her moral

---

191. ZeroKnowledge, Inc., Advertisement, WIRED, Aug. 2000, at 5-6. ZeroKnowledge Systems lets Internet users surf the net anonymously. *See* http://www.zeroknowledge.com (last visited Sept. 4, 2001). Zero-Knowledge Systems' Freedom software uses the encryption and several different computers to mask its users' identities even from itself. *Id.* The Freedom IP overlay network opens up an anonymous route, with encryption, from server to server. *Id.*

192. *Id.*

193. IMMANUAL KANT, THE METAPHYSICS OF MORALS 187-89 (Mary Gregor trans., Cambridge University Press 1991) (1797).

194. ZeroKnowledge, Inc., Advertisement, WIRED, Aug. 2000, at 5-6.

195. *Id.*

196. *Id.*

rights when it comes to online privacy, she in effect admonishes the reader of the advertisement to do the same.

The advertisement by the company Netcreations, a provider of a permission-based email marketing system, similarly invokes an everyday Kantian theme.[197] Netcreations promotes itself as providing consumers with only the information they have asked for. As contained in this article's epigram, the advertisement features a picture frame with the following tenets set out as its "Code": "This is not Cattle. This is a human being. We do not spam human beings. We respect human beings. Respecting human beings is good business. This is the code."[198] The advertisement strives to convince the website industry that privacy-respecting practices are also good for business. As the advertisement says, "[w]hat is right is also effective."[199]

A similar effort is made by a firm named PrivaSeek.[200] In a series of advertisements, PrivaSeek promotes technology that will give consumers control over their online profiles.[201] The advertisement notes that, "[c]onsumers are becoming more savvy about protecting their personal information online."[202] PrivaSeek's product is geared toward this changing privacy environment because it promises to increase the "confidence" of customers.[203] "Confidence" is a term that is often used in the business-to-business software market that supports secure online transactions. PrivaSeek plays on websites' desire for consumers to have confidence in them, so that consumers will readily interact with websites on a repeated basis.

In conclusion, each software privacy solutions provider will likely influence privacy norms by further stoking consumer privacy concerns and the corresponding entitlement to personal data. In other words, the advertisements will further advance the shift in the social meaning of personal data collection toward a more normatively-charged interpretation.[204] Although there is no hard data, these advertisements will likely have an effect in further galvanizing public opinion in the direction of greater de-

197. Netcreations, Inc., *supra* note 1.
198. *Id.*
199. *Id.*
200. PrivaSeek, Inc., Advertisement (on file with the author).
201. *Id.*
202. *Id.*
203. *Id.*
204. The strong moral tone of these advertisements is seen by contrasting them with ads meant to alert users to security issues. Here the threatening activities are illegal and the need is to protect oneself from theft. There is no attempt to create moral outrage on the part of consumers in the text of these advertisements.

mand for more respectful website privacy practices. For websites at the margin, it may now make sense to switch to more respectful norms. Thus, while companies selling privacy solutions may lack the lobbying savvy of organizations like EPIC or the coercive power possessed by the FTC, they may nevertheless be powerful shapers of public norms regarding online privacy due to their ability to directly reach millions through their print media campaigns.

V. CONCLUSION

There have been important changes in informal online privacy regulation over the past few years; primarily the recognition of a moral entitlement to privacy in cyberspace. This Article has argued that privacy norm proselytizers are the leading contributors to this development. These activists have taken an interest in online privacy because they believe Internet users are morally entitled to, and desperately in need of, increased protection. Other norm entrepreneurs have subsequently supported an entitlement to privacy for reasons less moral, but no less efficacious in stimulating demand for increased privacy protections.

As a result of these efforts, Internet users are increasingly conscious of moral entitlements to respectful treatment by websites. The general social demand for privacy respect in cyberspace is half of a broader supply and demand model documenting the emergence of Internet privacy norms. While this Article has begun to address the response on the part of websites to the growing demand for privacy, a more detailed analysis of the supply side is necessary in order to address a puzzle that has been created by the foregoing account.

Privacy activists have not been impressed with the response by websites to the increasing demand. They allege that websites have only made reluctant and ineffectual efforts to respect users' privacy interests. The puzzle is why the substantial increase in demand for online privacy has not resulted in a corresponding increase in the supply of online privacy, as a market model would naturally suggest. This important issue should be addressed in future research on the emergence of online privacy norms.

ARE XENOTRANSPLANTATION SAFEGUARDS LEGALLY VIABLE?

By Patrik S. Florencio[†] and Erik D. Ramanathan[‡]

ABSTRACT

Scientists agree on the need for robust public health safeguards to accompany the imminent introduction of xenotransplantation—clinical transplantation of animal tissues into humans. To protect society in the event of emerging infectious diseases, governments must devise a legally effective means of ensuring compliance with such safeguards.

Neither consent law, the law of contracts, nor existing public health legislation can adequately enforce such compliance. Consent law serves as a mechanism of communicating the momentary waiver of legal rights, not as a durable enforcement doctrine. Because it would be essential for recipients personally to comply with public safety measures, the law of contracts would also be unable to compel compliance. Existing public health legislation would also likely be ineffective because it would need to be substantially amended to incorporate the heightened powers necessary for the periodic examination of asymptomatic xenotransplant recipients.

Xenotransplantation-specific legislation would be a legally effective means of enforcing public health safeguards since it could require conforming behaviors and could impose monetary fines on those recipients who, having benefited from life-saving intervention, fail to comply. This Article argues that legislation implementing a post-xenotransplantation surveillance system should withstand constitutional scrutiny because it would not be discriminatory and because, although it would violate fundamental rights of recipients, such violations would be justified under existing constitutional doctrines.

---

† Associate, Proskauer Rose LLP, New York; LL.B., B.C.L., McGill Law School; B.Sc., McGill University. Contact (212) 969-3000 or pflorencio@proskauer.com.

‡ Director, Legal Department, ImClone Systems Inc., New York; J.D., Harvard Law School; B.A., The Johns Hopkins University. Contact (212) 645-1405 or erikr@imclone.com.

I. INTRODUCTION

Xenotransplantation is an innovative medical procedure in which materials such as cells, tissues, or organs are procured from animal sources and subsequently transplanted into humans. Scientists have already managed successfully to transplant animal cells and tissues into humans;[1] all attempts at animal-to-human whole organ transplantation, however, have failed because of immunological rejection.[2] Nonetheless, scientists have recently achieved significant experimental progress in overcoming the immunological and physiological barriers to whole organ xenotransplantations, and expect this biotechnology to become a clinical reality in the near future.[3]

By offering a potentially limitless source of animal materials for transplantation,[4] xenotransplantation biotechnology—or xenobiotechnology for short—promises substantial future medical benefits, and may put an end to the current worldwide shortage of replacement organs.[5] Yet xenobiotechnology also carries with it a serious risk of introducing and spreading new infectious diseases into the world's human population.[6] Specifically, infec-

---

1. Terrence Deacon et al., *Histological Evidence of Fetal Pig Neural Cell Survival After Transplantation into a Patient with Parkinson's Disease*, 3 NATURE MED. 350 (1997); C.G. Groth et al., *Transplantation of Porcine Fetal Pancreas to Diabetic Patients,* 344 LANCET 1402 (1994); Ole Isacson & Xandra O. Breakefield*, Benefits and Risks of Hosting Animal Cells in the Human Brain*, 3 NATURE MED. 964 (1997); Rachel Nowak, *Xenotransplants Set to Resume*, 266 SCI. 1148 (1994); Joseph Palca, *Animal Organs for Human Patients?*, 25 HASTINGS CENT. REP. 4 (1995).

2. Leonard L. Bailey et al., *Baboon-to-Human Cardiac Xenotransplantation in a Neonate*, 254 JAMA 3321 (1985); Keith Reemtsma, *Renal Heterotransplantation from Non-Human Primate to Man*, 162 ANNALS. N.Y. ACAD. SCI. 412 (1969); T.E. Starzl et al., *Baboon-to-Human Liver Transplantation*, 341 LANCET 65 (1993); T.E. Starzl et al., *Renal Heterotransplantation from Baboon to Man: Experience with Six Cases*, 2 TRANSPLANTATION 752 (1964).

3. Jeffrey L. Platt, *New Directions for Organ Transplantation*, 392 NATURE 11 (1998); Thomas E. Starzl et al., *Will Xenotransplantation Ever Be Feasible?*, 186 J. AM. C. SURGEONS 383 (1998).

4. Robert P. Lanza et al., *Xenotransplantation*, 277 SCI. AM. 54 (1997).

5. According to recent Canadian statistics, the shortage of human donor organs is such that each year only 16% of Canadians waiting to receive a heart transplant and 2.7% of Canadians waiting for a kidney transplant actually obtain one. Comparable statistics apply to potential liver and lung transplant patients. *See The Canadian Organ Replacement Register Annual Report: Organ Donation and Transplantation*, 2 CANADIAN INST. FOR HEALTH INFO. (1997).

6. Jonathan S. Allan, *Xenotransplantation at a Crossroads: Prevention Versus Progress*, 2 NATURE MED. 18 (1996); Louisa E. Chapman et al., *Xenotransplantation and Xenogeneic Infections*, 333 NEW ENG. J. MED. 1498 (1995); Jay A. Fishman, *The Risk of*

tious animal agents residing in the source material could infect the xenotransplant recipient who could then pass this infection on to the community, causing morbidity and mortality if pathogenic. There is, consequently, a foreseeable yet unquantifiable possibility that xenobiotechnology might give rise to a human epidemic with effects comparable to those of HIV/AIDS or worse.[7]

In light of these foreseeable risks of harm, some commentators have advocated a precautionary approach to clinical xenotransplantation on the basis that a number of scientific, ethical, legal, and public health issues need to be addressed before proceeding with xenobiotechnology.[8] In contrast, other commentators have stressed that progress should not be impeded, as the potential benefits to patients could be great and the associated risk to the community remains unquantifiable.[9] Given the recent international flurry of activity preparing for the arrival of xenotransplantation, the latter view seems to be prevailing.[10]

The critical question no longer revolves around whether we have the scientific knowledge and ability to introduce clinical xenotransplantation, but is instead directed at the circumstances under which it would be acceptable to proceed. Importantly, despite the divergence of opinion as to whether further scientific, ethical, and legal analyses are required prior to introducing clinical xenotransplantation, everyone has agreed that should

---

Infection in Xenotransplantation, 862 ANNALS N.Y. ACAD. SCI. 45 (1998); Clive Patience et al., *Zoonosis in Xenotransplantation*, 10 CURRENT OPINION IMMUNOLOGY 539 (1998); Robin A. Weiss, *Transgenic Pigs and Virus Adaptation*, 391 NATURE 327 (1998).

7. *Id*. For a good summary of the risks and benefits associated with xenotransplantation, see Declan Butler et al., *Last Chance to Stop and Think on Risks of Xenotransplantation*, 391 NATURE 320 (1998).

8. *See*, *e.g.*, Jonathan S. Allan, *Nonhuman Primates as Organ Donors?*, 77 BULL. WORLD HEALTH ORG. 62 (1999); F.H. Bach et al., *Uncertainty in Xenotransplantation: Individual Benefit Versus Collective Risk*, 4 NATURE MED. 141 (1998); Patrik S. Florencio & Timothy Caulfield, *Xenotransplantation and Public Health: Identifying the Legal Issues*, 90 CAN. J. PUB. HEALTH 282 (1999); Jonathan Hughes, *Xenografting: Ethical Issues*, 24 J. MED. ETHICS 18 (1998).

9. *See*, *e.g.*, David H. Sachs et al., *Xenotransplantation—Caution, But No Moratorium*, 4 NATURE MED. 372 (1998); Daniel R. Salomon et al., *Xenotransplants: Proceed with Caution*, 392 NATURE 11 (1998); Thomas E. Starzl et al., *Will Xenotransplantation Ever Be Feasible?*, 186 J. AM. C. SURGEONS 383 (1998).

10. *See*, *e.g.*, Xavier Bosch, *Spanish Researchers Reject Xeno Moratorium While Canada Faces the Issue Head-On*, 5 NATURE MED. 361 (1999); Declan Butler, *US Decides Close Tabs Must Be Kept on Xenotransplants and Sets Up a Body To Oversee Trials*, 405 NATURE 606 (2000); Rebecca Currie, *UK Moves Ahead on the Xenotransplantation Issue*, 4 NATURE MED. 988 (1998); Gretchen Vogel, *No Moratorium on Clinical Trials*, 279 SCI. 648 (1998). *But see* Declan Butler, *Europe is Urged to Hold Back on Xenotransplant Clinical Trials*, 397 NATURE 281 (1999).

xenotransplantation proceed in the near future, the government must also implement robust public safety measures.[11] The debate now encompasses an important legal component: to what extent, if at all, will the law be capable of enforcing those public health safeguards that the scientific community deems necessary?

This Article will argue that the legal authority to enforce the most important public health safeguard associated with post-xenotransplantation surveillance—the periodic collection of bodily specimens such as serum samples from xenotransplant recipients—could exist, but that its subsistence would ultimately depend on its ability to withstand constitutional challenges. Although the medical community could not physically compel recipients to provide serum samples, the government could enact legislation to fine recipients who, having benefited from the life saving intervention, refused to accept responsibility for conforming to the public safety measures.

This Article begins by explaining why the scientific community agrees that xenotransplantation requires robust public safety measures. The Article will demonstrate that the importance of the safeguards lies not in their ability to prevent the emergence of infectious diseases—because they are incapable of doing so—but in their ability to provide the foundation for a rapid response to emerging infectious diseases. The Article then summarizes the nature and scope of the public safety measures proposed by the health authorities in the various countries now contemplating the introduction of clinical xenotransplantation.

The Article goes on to examine the various sources of legal authority that authorities might use to enforce compliance with the safeguards. In this discussion, the Article focuses on the laws of both the United States and Canada for two reasons. First, a comparative review of their laws allows one to draw upon the best practices of two legal traditions in analyzing existing and proposed legal safeguards. Second, the public health systems of these neighboring nations are inextricably intertwined and, although they cannot insulate themselves from the world's public health crises in an age of global travel and migration, coordination of multinational public health efforts would be an excellent start to addressing the problem globally. The final section of the Article comments on the constitutional

---

11. *See generally supra* notes 6, 8 and 9. *See also* L.E. Chapman et al., *Xenotransplantation: The Potential for Xenogeneic Infections*, 31 TRANSPLANTATION PROC. 909 (1999); Jay A. Fishman, *Infection and Xenotransplantation: Developing Strategies to Minimize Risk*, 862 ANNALS N.Y. ACAD. SCI. 52 (1998); Frederick A. Murphy, *The Public Health Risk of Animal Organ and Tissue Transplantation into Humans*, 273 SCI. 746 (1996); Robin A. Weiss, *Xenografts and Retroviruses*, 285 SCI. 1221 (1999).

dimension of the problem in both countries. The Article concludes that restrictions on the rights of recipients that would necessarily result from the enactment of xenotransplantation legislation would be in accordance with the principles of fundamental justice and would thus be demonstrably justified in a free and democratic society.

II. LEGAL REGULATION OF XENOTRANSPLANTATION

A. Public Safety Measures

1. The Need for Public Safety Measures

It is probably fair to state that we are not yet, nor are we likely to become in the near future, masters of the microbial world.[12] Even though infectious diseases have always plagued humans, our science is still young and has not yet matured to a level where it might be acceptable to ignore the potential harms that infectious diseases can cause. One need only to look at the devastation wrought by the periodic emergence of yellow fever in European and American cities during the eighteenth and nineteenth centuries to see the damage that infectious disease can cause.[13] Recent examples, such as the 1995 epidemic of Ebola hemorrhagic fever in the Democratic Republic of Congo, demonstrate that our vulnerability to infectious diseases is not a historical relic.[14] The resurgence of diseases such as tu-

---

12. The microbial world is thought by many to pose one of the biggest threats to the future existence of humankind:

> Ingenuity, knowledge, and organization alter but cannot cancel humanity's vulnerability to invasion by parasitic forms of life. Infectious disease which antedated the emergence of humankind and will last as long as humanity itself, and will surely remain, as it has been hitherto, one of the fundamental parameters and determinants of human history.

WILLIAM H. MCNEILL, PLAGUES AND PEOPLES 291 (1976). *See also* Joshua Lederberg, *Medical Science, Infectious Diseases, and the Unity of Humankind*, 260 JAMA 684 (1988).

13. For instance, the yellow fever epidemic that hit Memphis in 1878 is recorded to have led to the death of a quarter of its population. J.M. KEATING, HISTORY OF THE YELLOW FEVER EPIDEMIC OF 1878 IN MEMPHIS, TENNESSEE 116 (Cincinnati, Wrightson & Co. 1879).

14. Barbara Kerstiëns & Francine Matthys, *Interventions to Control Virus Transmission during an Outbreak of Ebola Hemorrhagic Fever: Experience from Kikwit, Democratic Republic of the Congo, 1995,* 179 J. INFECTIOUS DISEASES 263 (Supp. 1999). *See also* MICHAEL B.A. OLDSTONE, VIRUSES, PLAGUES, AND HISTORY 130-35 (1998).

berculosis[15] and the spread of HIV[16] remind us that infectious illnesses can also have a dramatic impact on the modern western world. Today, infectious diseases are the third leading cause of death in the United States, and the leading cause worldwide.[17]

It is because of our physiological vulnerability to infectious microbes that we must proceed prudently and conscientiously when engaging in activities that raise the specter of emerging infectious illnesses, especially when the etiology of disease is our own behavior. Indeed, human behavior is the leading cause of emerging infectious diseases.[18] For example, the immense volume of global travel has made us more vulnerable to the effects of infectious diseases today than we have ever been in the past.[19] If

---

15. Christopher Dye et al., *Global Burden of Tuberculosis: Estimated Incidence, Prevalence, and Mortality by Country*, 282 JAMA 677 (1999); Thomas R. Frieden et al., *The Emergence of Drug-Resistant Tuberculosis in New York City*, 328 NEW ENG. J. MED. 52 (1993).

16. Jonathan M. Mann & Daniel J.M. Tarantola, *HIV 1998: The Global Picture*, 279 SCI. AM. 82, 82 (1998) ("Since the early 1980s more than 40 million individuals have contracted HIV, and almost 12 million have died . . . . In 1997 alone, nearly six million people—close to 16,000 a day—acquired HIV, and some 2.3 million perished from it, including 460,000 children.").

17. Gregory L. Armstrong et al., *Trends in Infectious Disease Mortality in the United States During the 20th Century*, 281 JAMA 61 (1999); Sue Binder et al., *Emerging Infectious Diseases: Public Health Issues for the 21st Century*, 284 SCI. 1311 (1999); Robert W. Pinner et al., *Trends in Infectious Diseases Mortality in the United States*, 275 JAMA 189 (1996).

18. David M. Forrest, *Control of Imported Communicable Diseases: Preparation and Response*, 87 CAN. J. PUB. HEALTH 368, 368-69 (1996):

> A number of factors, both singly and interactively, facilitate the emergence of new diseases. These include environmental and geoclimatic conditions, fluctuating reservoir and vector characteristics, microbial conditions, and especially, human factors. Human factors include anthropogenic ecological change, alterations in demographics and behaviours, international travel and commerce, and deficiencies in public health structure.

See also Stephen S. Morse & Ann Schluederberg, *Emerging Viruses: The Evolution of Viruses and Viral Diseases*, 162 J. INFECTIOUS DISEASES 7 (1990).

19. Stephen S. Morse, *Factors in the Emergence of Infectious Diseases*, 1 EMERGING INFECTIOUS DISEASES 1, 10 (1995).

> The history of infectious diseases has been a history of microbes on the march, often in our wake, and of microbes that have taken advantage of the rich opportunities offered them to thrive, prosper, and spread. And yet the historical processes that have given rise to the emergence of new infections throughout history continue today with unabated force; in fact, they are accelerating, because the conditions of modern life ensure that the factors responsible for disease emergence are more prevalent than ever before.

we are not careful, xenotransplantation could become the next example of human behavior that results in the introduction of new infectious microbes into the human population.[20]

The foregoing commentary means to provide the reader with an awareness of why the scientific community agrees that robust public safety measures must accompany the introduction of xenotransplantation. The following passage embodies the quintessence of this commentary: "[h]istory has shown us repeatedly, in terms of both human suffering and economic loss, that the costs of preparedness through vigilance are far lower than those needed to respond to unanticipated public health crises."[21] In the context of xenotransplantation, preparedness means public health safeguards.

Public safety measures would establish a surveillance system[22] that should permit the early detection of—and a rapid response to—any emerging epidemics.[23] Commentators have often described surveillance as the cornerstone of infectious disease control,[24] and as "essential to minimize illness, disability, death, and economic losses."[25] However, it must be made absolutely clear that any surveillance system would be incapable of preventing the emergence of infectious illnesses. As one group of commentators stated: "surveillance is not the same as prevention. New infectious agents may spread and cause disease among human populations before surveillance techniques have permitted their detection and isolation.

See generally MARY E. WILSON, A WORLD GUIDE TO INFECTIONS: DISEASES, DISTRIBUTION, DIAGNOSIS (1991).

20. Patrik S. Florencio & Nathalie Weizmann, *Xenotransplantation and the Role of Human Behaviour in the Emergence of Infectious Disease*, 7 HEALTH L. REV. 20 (1998).

21. Ruth L. Berkelman et al., *Infectious Disease Surveillance: A Crumbling Foundation*, 264 SCI. 368, 370 (1994).

22. The United Kingdom Xenotransplantation Interim Regulatory Authority (UKXIRA), the regulatory authority in charge of overseeing xenobiotechnology in England, defines surveillance as the "on-going systematic collection, analysis, and interpretation of relevant data, closely integrated with the timely dissemination of these data to those responsible for control and prevention" and state that surveillance is a "critical step in the pathway of identification and prevention of infectious diseases and xenogeneic infections." *See* U.K. XENOTRANSPLANTATION INTERIM REGULATORY AUTH., DRAFT REPORT OF THE INFECTION SURVEILLANCE STEERING GROUP OF THE UKXIRA 6, 17 (May 1999), *at* http://www.doh.gov.uk/pub/docs/doh/surveil.pdf [hereinafter UKXIRA].

23. James M. Hughes & John R. La Montagne, *Emerging Infectious Diseases* 170 J. INFECTIOUS DISEASES 263 (1994).

24. Donald A. Henderson, *Surveillance Systems and Intergovernmental Cooperation*, *in* EMERGING VIRUSES 283 (Stephen S. Morse ed., 1993). *See also* Ruth L. Berkelman & James M. Hughes, *The Conquest of Infectious Diseases: Who Are We Kidding?* 119 ANNALS INTERNAL MED. 426 (1993).

25. Binder et al., *supra* note 17, at 1311.

Further, detection and isolation of infectious agents does not equate to the containment of their propagation at the human level."[26]

The importance of surveillance is problematic, because, in general, our public health infrastructure is "geared to crisis response, but seems inadequately prepared for proaction, crisis anticipation, and prevention."[27] Prevention means avoiding a public health crisis through instrumentalities such as vaccines and, in the case of xenotransplantation, the imposition of a moratorium until we know more about the associated infectious disease risks. As noted above, however, the current international trend has been to reject the precautionary approach and to prepare for the arrival of clinical xenotransplantation. Further, even if governments implement preventative measures, infectious microbes could still emerge from xenotransplantation and could result in severe morbidity and mortality if pathogenic in human populations. Appropriate safeguards would nevertheless represent an essential precaution to such consequences, as they would ideally enable officials to respond quickly to emerging infectious diseases through the rapid detection and isolation of the microbes responsible for causing sickness and the subsequent development of treatments.

2. Proposed Public Safety Measures in the Case of Xenotransplantation

Recognizing the need for public safety measures to accompany the clinical introduction of xenotransplantation, the health departments of various governments—including those of the United States,[28] the United Kingdom,[29] and Canada[30]—have drafted guidelines proposing public health safeguards that are intended to form the foundation of infectious disease surveillance. Although each country's guidelines differ in many respects, each imposes similar requirements on xenotransplant recipients. In light of this similarity, and to avoid repetition, this Article will use the

---

26. Florencio & Caulfield, *supra* note 8, at 283-84.

27. Forrest, *supra* note 18, at 368.

28. *See* U.S. DEP'T OF HEALTH AND HUMAN SERVS., PHS GUIDELINE ON INFECTIOUS DISEASE ISSUES IN XENOTRANSPLANTATION, *at* http://www.fda.gov/cber/gdlns/xenophs0101.pdf (January 19, 2001) [hereinafter U.S. DEP'T OF HEALTH AND HUMAN SERVS.].

29. *See* UKXIRA, *supra* note 22.

30. *See* HEALTH CANADA, PROPOSED CANADIAN STANDARD FOR XENOTRANSPLANTATION, *at* http://www.hc-sc.gc.ca/hpb-dgps/therapeut/zfiles/english/btox/standards/xeno_std_e.html (July 1999) [hereinafter HEALTH CANADA].

recently drafted guidelines from the United Kingdom to exemplify the nature of the safeguards proposed in all three jurisdictions.[31]

According to the United Kingdom's guidelines, its surveillance system intends to enable the prompt recognition, investigation and management of infectious illnesses that might emerge as a result of xenobiotechnology.[32] In order to have access to clinical xenotransplantation, recipients would need to agree to: 1) the periodic provision of bodily samples that would then be archived for epidemiological purposes;[33] 2) post-mortem analysis in case of death, the storage of samples post-mortem, and the disclosure of this agreement to their family; 3) refrain from donating blood, tissue or organs; 4) the use of barrier contraception when engaging in sexual intercourse; 5) keep both name and current address on register and to notify the relevant health authorities when moving abroad; and 6) divulge confidential information, including one's status as a xenotransplant recipient, to researchers, all health care professionals from whom one seeks professional services, and close contacts such as current and future sexual partners.[34] The recipient would have to adhere to these obligations consistently for the recipient's lifetime, or until the government determines that there is no longer a need for public health safeguards.[35]

By far the most important of these public health safeguards, and the only safeguard that will be receiving attention throughout this article, is the collection and archiving of bodily specimens that are needed for epidemiological purposes. Regarding this essential safeguard, the United Kingdom's guidelines state that:

> Surveillance of potential xenogeneic infections in humans *requires* access to human and animal data . . . . Effective public health response to an incident [of infectious disease] is *dependent* on both maintenance of records and of archived specimens both at the time of xenotransplantation and for the future. Animal and human specimens need to be held for public purposes. Access by the relevant authorities to appropriate information and

---

31. Although we have chosen to focus on American and Canadian law in this Article, we believe that the xenotransplantation guidelines issued by the United Kingdom are the most comprehensive to date, and are therefore the best model for the discussion of Western governments' preliminary thinking about xenotransplantation safeguards.

32. *See* UKXIRA, *supra* note 22, at 8.

33. *Id.* at 29. The guidelines, which are subject to review on the basis of emerging scientific information, call for baseline sampling pre-xenotransplantation and for sampling at 0-2 days; 2, 4 and 6 weeks; 3 and 6 months; 1 and 2 years post-xenotransplantation.

34. *Id*. at 29-30.

35. *Id*. at 11, 21.

> samples from locally held records and archives *must be a precondition to approval for a clinical trial*.[36]

Even outside of the context of xenobiotechnology, scientists have been calling for "well-controlled epidemiology, careful clinical and histologic observations, and increased attention to specimen collection and processing."[37] Without the enforcement of this safeguard in connection with xenotransplantation, scientists would be handicapped in detecting and isolating the infectious microbes causing any resulting illness. Such a handicap could prove to be fatal because until doctors identify the illness-causing microbes, treatment strategies may be no more sophisticated than a game of trial and error.

B. Enforcing Public Safety Measures

Although the scientific community almost universally agrees that public health safeguards must be a prerequisite to the introduction of clinical xenotransplantation, and although extensive work has gone into the development of comprehensive safeguards, little thought has been given to how to enforce these safeguards. The relevant scientific literature often appears to assume that the law will be able to accommodate and enforce whatever measures scientists deem necessary.[38] The reality is that there are limits to the enforcement measures that the law can currently accommodate.

The remaining sections of this Article discuss whether officials could use existing or novel legal frameworks to enforce the proposed public

---

36. *Id*. at 10-13 (emphasis added). Similarly, the Canadian guidelines stipulate that the "patient will *need* to comply with long term surveillance *necessitating* routine physical evaluations with archiving of tissues and/or serum specimens from the recipient" and that "[c]onsent should indicate that the patient is *obligated* to follow all of the requirements of the program." HEALTH CANADA, *supra* note 30 (emphasis added). Moreover, the United States guidelines state for example that "[p]ost-xenotransplantation clinical and laboratory surveillance of xenotransplantation recipients is *critical, as it provides the means of monitoring for any* introduction and propagation of xenogeneic infectious agents in the xenotransplantation product recipient." DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 28, at 35 (emphasis added).

37. David A. Relman, *The Search for Unrecognized Pathogens*, 284 SCI. 1308, 1310 (1999). *See also* K.F. Gensheimer et al., *Preparing for Pandemic Influenza: The Need for Enhanced Surveillance*, 5 EMERGING INFECTIOUS DISEASES 297, 297 (1999) ("Because it establishes the scientific foundation for a public health response, surveillance is the single most important tool for identifying new or re-emerging infectious diseases with potential to cause serious public health problems.").

38. *See, e.g.,* Michele L. Pearson, M.D. et al., *Xenotransplantation: Is the Future Upon Us?*, 19 INFECTION CONTROL AND HOSP. EPIDEMIOLOGY (1998). Other scientific articles recognize that enforcement may be an issue but defer discussion of enforcement to other commentators. *See, e.g.,* Bach et al., *supra* note 8, at 144.

safety measures. Possibilities among existing law include consent law, the law of contracts, and existing public health legislation. Because the law is not immutable, it can be adapted to reflect changing social and scientific realities. Thus, even if the public safety measures prove unenforceable under existing law, legislatures could enact new statutes or executive agencies could adopt new regulations that would render lawful the required enforcement mechanisms.

Regardless of the approved legal standards, the judiciary could declare these new enactments illegal if they transgress constitutionally protected rights and freedoms. If the courts strike down such legislation on constitutional grounds, xenotransplant recipients in the relevant jurisdiction would not be legally obligated to comply with the public health safeguards. As a result, the ability of scientists to gather epidemiological data in that jurisdiction, and hence the capacity of the public safety measures to perform their protective function, would depend entirely on the willingness of recipients to comply voluntarily with the invasive measures. In the absence of such willingness, the surveillance system would crumble, leaving society defenseless in the advent of an epidemic. Part III of this Article examines the constitutional limitations that courts might impose on public safety legislation.

1. From Informed Consent to Binding Contract?

a) Informed Consent is Not a Promise to Undertake Future Obligations

Mandatory compliance with public safety measures has rarely, if ever, served as a prerequisite to having access to innovative medical interventions. Indeed, the case of xenotransplantation would be exceptional in this regard; all that is normally required before doctors provide medical treatment is the patient's informed consent.[39] Lawmakers designed informed consent to correct the imbalance in knowledge, and hence power, between health care providers and patients.[40] It is premised on the patient's right to

---

39. ELLEN T. PICARD & GERALD B. ROBERTSON, LEGAL LIABILITY OF DOCTORS AND HOSPITALS IN CANADA 84-85 (3d ed. 1996).

40. Dow Corning Corp. v. Hollis, [1995] 4 S.C.R. 634, 656 ("The doctrine of 'informed consent' was developed as a judicial attempt to redress the inequality of information that characterizes a doctor-patient relationship.").

self-determination[41] and requires the physician to disclose "the nature of the proposed operation, its gravity, any material risks and any special or unusual risks attendant upon the performance of the operation."[42] The level of disclosure required varies depending on the nature of the intervention.[43] In the case of experimental procedures such as xenotransplantation, the degree of disclosure would be higher than that necessary for conventional medical treatments.[44]

In addition to the right to know, the patient's right to self-determination encompasses the right to accept or reject treatment.[45] It is ultimately the patient, and not the health care provider, who decides whether or not the intervention will be performed. Moreover, health care providers cannot interfere with the patient's decision to refuse treatment, no matter how foolish or medically unsound they believe it to be.[46]

Although the doctrine of informed consent protects the patient's right to know the risks of a medical procedure, it does not bind the patient to a contractual agreement. Importantly, consent speaks not to the patient's promise to undertake future obligations in consideration of having access to medical care, but to the patient's initial acquiescence to a particular intervention. In the case of xenotransplantation, the recipient's consent to the intervention, even with full understanding of the accompanying public health safeguards, would not legally bind the recipient to comply with the safeguards. This is because the recipient's right to self-determination con-

---

41. For an early source making reference to this right, see Schloendorff v. Soc'y of N.Y. Hosps., 105 N.E. 92, 93 (N.Y. Ct. App. 1914) ("Every human being of adult years and sound mind has a right to determine what shall be done with his own body."). *See generally* Tom L. Beauchamp, *Informed Consent*, *in* MEDICAL ETHICS 185-208 (Robert M. Veatch ed., 1997).

42. Hopp v. Lepp, [1980] 2 S.C.R. 192, 210. *See also* Canterbury v. Spence, 464 F.2d 772 (D.C. Cir. 1972); Salgo v. Leland Stanford Jr. Univ. Bd. of Trs., 317 P.2d 170 (1957); Reibl v. Hughes, [1980] 2 S.C.R. 880.

43. Margaret A. Somerville, *Structuring the Issues in Informed Consent*, 26 MCGILL L.J. 740 (1981).

44. Weiss v. Solomon, [1989] 48 C.C.L.T. 280, 282 (Que. S.C.); Halushka v. Univ. of Sask., [1965] 53 D.L.R. (2d) 436, 443-44 (Sask. C.A.).

45. Hopp, 2 S.C.R. at 192.

46. *See* Fleming v. Reid, [1991] 4 O.R. (3d) 74, 85 (C.A.):

> The fact that serious risks or consequences may result from a refusal of medical treatment does not vitiate the right of medical self-determination. The doctrine of informed consent ensures the freedom of individuals to make choices about their medical care. It is the patient, not the doctor, who ultimately must decide if treatment—any treatment—is to be administered.

See also Walker v. Region 2 Hospital Corp., [1994] 116 D.L.R. (4th) 477 (N.B.C.A.); Malette v. Shulman, [1990] 67 D.L.R. (4th) 321 (Ont. C.A.).

tinues after she gives her initial consent and begins treatment. Recipients could withdraw their consent, written or otherwise, at any time.[47]

Because the recipient's consent is insufficient to guarantee adherence to public safety measures, some other legal mechanism is required. This alternative mechanism will necessarily conflict with the now-entrenched patient autonomy model of medical decision making. As such, officials would need to find a distinct source of legal authority that might be used to trump or pre-empt the application of the right to self-determination. What we must therefore determine is the nature of the legal authority that might accomplish this task.

b) Contract Law Is Not a Viable Enforcement Mechanism

Medical commentators have emphasized that the law of contracts may provide a means of legally enforcing a patient's compliance with the safeguards. For instance, according to one commentator, "[t]he fact that the patient is going to be *required* to comply with postoperative monitoring alters the nature of 'consent' to something more binding and contractual."[48] According to another commentator, recipients and their close contacts:

> would not only have to agree to the risks attendant to a transplant procedure, but also to a contract binding the patient and others to carry out future obligations, including the patient's possible quarantine, as well as modification of the guarantees of confidentiality and surrender of the right to 'drop out' of the study.[49]

---

47. *See* Ciarlariello v. Schacter, [1993] 2 S.C.R. 119, 136 (holding that a "patient's right to bodily integrity provides the basis for the withdrawal of a consent to a medical procedure even while it is underway."). The right to withdraw consent exists even in the context of life sustaining interventions. *See* Cruzan v. Dir., Miss. Dept. of Health, 497 U.S. 261 (1990) (holding that vegetative patient's wishes to not have life sustaining interventions must be honored if they are proven with clear and convincing evidence); Nancy B v. Hotel-Dieu de Québec, [1992] 86 D.L.R. (4th) 385 (Que. S.C.).

48. A.S. Daar, *Ethics of Xenotransplantation: Animal Issues, Consent, and Likely Transformation of Transplant Ethics*, 21 WORLD J. SURGERY 975, 977 (1997). *See also* A.S. Daar, *Animal-to-Human Organ Transplantation—A Solution or a New Problem?*, 77 BULL. WORLD HEALTH ORG. 54, 58 (1999).

49. Bach et al., *supra* note 8, at 144. *See also* DAVID K.C. COOPER & ROBERT P. LANZA, XENO: THE PROMISE OF TRANSPLANTING ANIMAL ORGANS INTO HUMANS 218 (2000):

> What is being envisaged is no longer a simple matter of the patient's signing a consent form after being provided with the necessary information. In view of the perceived potential risk to the commu-

As currently formulated, the law of contracts would most likely be unable to ensure that recipients comply with the public health safeguards. At first blush, one might employ the common law theories of promise[50] or reliance[51] to validate the contract. The theory here would be that since the recipient promises to comply with the safeguards and society relies upon that promise, society should be able to enforce the promise. Indeed, one might view compliance with the safeguards as the consideration that is required in order to have access to the innovative biotechnology. Similarly, under the Civil Code of Quebec, all that is theoretically required for the existence of a valid contract is a meeting of the minds between persons having the capacity to contract.[52] Yet, there are a number of reasons for believing that the law of contracts would be incapable of serving as an effective source of legal enforcement.

There are two threshold challenges to using the law of contracts as a source of legal authority. One must first identify the legal entity with whom the recipients would be contracting and determine whether that entity would have the legal capacity to enter into and enforce such contractual undertakings. Stated differently, who would be the creditor of the recipient's obligation of complying with the safeguards? The surgical team or institution performing the operation? The federal or provincial/state government(s)? Society? Moreover, could any of these "creditors" enforce the obligation?

Assuming that one could answer these threshold queries, a court could nevertheless strike down the contract, or at least render it unenforceable, as being against public policy.[53] Compulsory compliance with the safeguards would require the relinquishment of certain civil liberties, and, as a matter of public policy or human rights, it is highly unlikely that these could be contracted away.[54] Recipients may initially agree to bind themselves to contracts calling for, among other things, the periodic provision

---

> nity from infection passed from the patient to his or her contacts, the patient will be expected to enter into what can be considered a 'contract' with the surgical team and transplant center. Some have suggested that this might have to be a binding legal contract. The patient—and possibly even members of the patient's family—will agree to lifelong monitoring in return for the potential benefits that might result from undergoing the xenotransplant.

50. *See generally* CHARLES FRIED, CONTRACTS AS PROMISE (1981).

51. *See generally* P.S. ATIYAH, THE RISE AND FALL OF FREEDOM OF CONTRACT (1979).

52. *See* Arts. 1378, 1385 C.C.Q. (Can.).

53. *See* RESTATEMENT (SECOND) OF CONTRACTS § 178 (1981).

54. *See*, *e.g.*, Arts. 3(2), 8 C.C.Q. (Can.).

of bodily samples. If they later withdraw their consent, however, the specific performance of these contracts would be incompatible with legislation upholding civil liberties such as the inviolability of the body.[55] To be lawful, an invasion of civil liberties would have to be expressly authorized by legislation and the legislation would itself be subject to constitutional scrutiny.

Even after surmounting these hurdles, courts could nonetheless consider the contracts to be illicit. This is true because, unlike most contracts, under which there is no requirement that the debtor personally perform the obligation(s),[56] the nature of the contractual undertaking in the case of xenotransplantation requires the recipient to comply with the safeguards himself or herself.

The civil law of Quebec refers to such contracts as *intuitu personae* and generally refuses to enforce them.[57] Simply put, enforcement of such contracts would lead to a conflict between two competing legal values—those of holding the debtor to her word, and respect for individual liberty.[58] In light of this conflict, the State may not use its power to force the debtor personally to execute the contract's obligations.[59]

In the common law, the remedy of specific performance best approximates the idea behind *intuitu personae* contracts. The traditional rule has been that equitable relief clauses, requiring the specific performance of

---

55. *See*, *e.g.*, Arts. 3(1), 10 C.C.Q. (Can.); *see also Quebec Charter of Human Rights and Freedoms*, R.S.Q., ch. C-12, § 1, pmbl. (1985) (Can.). The specific performance of these contracts would also engage constitutional protections such as the rights to liberty and security of the person. *See* CAN. CONST. (Constitution Act 1982), pt. I (Canadian Charter of Rights and Freedoms), cl. 11 § 7; s*ee also* U.S. CONST. amend. XIII (outlawing involuntary servitude).

56. In general, the debtor of the obligation(s) under a contract always has the option of delegating the performance of the obligations to a third party such as an agent or an employee.

57. Specific performance of the contract can be enforced so long as there is no requirement that the contract's prestation be carried out by the debtor in person. *See* Rosalie Jukier, *The Emergence of Specific Performance as a Major Remedy in Quebec Law,* 47 REVUE DU BARREAU 47 (1987).

58. JEAN-LOUIS BAUDOUIN, LES OBLIGATIONS 413 (4th ed. 1993):

> L'exécution en nature d'une obligation de faire, par le débiteur lui-même, pose clairement le conflit entre deux principes juridiques fondamentaux: le respect de la parole donnée, qui exige que la loi fasse tout pour obliger le débiteur à l'exécution, et le respect de la liberté individuelle, selon lequel la loi ne doit pas, dans des circonstances ordinaires, aller jusqu'à priver de sa liberté celui qui ne respecte pas son engagement.

59. *Id.*

contractual obligations, will only be awarded when monetary damages are inadequate.[60] Such is the case where the contractual obligation involves the transfer of a "unique" parcel of land.[61] Given that the viability of the public health safeguards depend on the execution of the contractual undertakings by the recipients personally, the circumstances of xenotransplantation arguably present another occasion where a court may consider monetary damages inadequate. Yet, similarly to Quebec civil law, Canadian[62] and American[63] common law seldom enforce the specific performance of personal service contracts.

It is also unlikely that the law of contracts could furnish an alternative remedy to specific performance, such as monetary damages that might be used indirectly to coerce the recipient into compliance. This is because the most logical creditor of the obligation (the surgical team or transplant center) would suffer no loss as a result of a breach of contract. The loss would instead be borne by the public, the third-party beneficiary to the contract. Yet, the public similarly would be incapable of obtaining an award in damages following a breach of contract. The common laws of the United States[64] and Canada,[65] as well as the civil law of Quebec,[66] require that one could identify third-party beneficiaries at the time the promise is to be performed. The 'public,' however, is not an identifiable beneficiary. As a result, the most vital safeguard—the collection and archiving of bodily

---

60. *See* Harnett v. Yielding, [1805] 2 Sch. & Lef. 549, 553; *see also* George T. Washington, *Damages in Contract at Common Law*, 47 L.Q. REV. 345 (1931).

61. Semelhago v. Paramadevan, [1996] 2 S.C.R. 415, 424-25.

62. *See* Warner Bros. Pictures Inc. v. Nelson, [1937] 1 K.B. 209; Emerald Resources Ltd. v. Sterling Oil Props. Mgmt. Ltd., [1969] 3 D.L.R. (3d) 630, 647 (Alta. C.A.) ("An example of a contract of which the Court will not compel specific performance is a contract of personal service . . . . [T]his seems to be based on the grounds of public policy; that it would be improper to make one man serve another against his will."), *aff'd*, [1970] 15 D.L.R. (3d) 256 (S.C.C.). *See generally*, ROBERT J. SHARPE, INJUNCTIONS AND SPECIFIC PERFORMANCE 7.540-7.630 (2000) (looseleaf ed.).

63. *See* Fitzpatrick v. Michael, 9A.2d 639 (Md. 1939); American Broadcasting Companies, Inc. v. Warner Wolf, 420 N.E.2d 363 (N.Y. Ct. App. 1981). Judicial compulsion of performance may even run afoul of the Thirteenth Amendment to the United States Constitution that prohibits involuntary servitude. *See* Arthur v. Oakes, 63 F. 310, 318 (7th Cir. 1894).

64. E. ALLAN FARNSWORTH, CONTRACTS § 10.3 (3rd ed. 1999).

65. In common law Canada, the doctrine of privity has not been relaxed to the extent that it has in other jurisdictions such as Quebec and the United States. As a result, third-party beneficiaries can only derive rights from a contract in very narrow circumstances. *See* Fraser River Pile & Dredge v. Can-Dive Servs. Ltd., [1999] 3 S.C.R. 108; London Drugs Ltd. v. Nagel Int'l Ltd., [1992] 3 S.C.R. 299. The public would not be recognized as a third-party beneficiary in common law Canada.

66. Arts. 1444-1445 C.C.Q. (Can.).

samples from recipients for epidemiological purposes—would remain unenforceable under contract law.[67]

2. Current Public Health Legislation

a) Current Public Health Legislation is Designed to Curb the Spread of Infectious Disease by Authorizing Examination of Individuals and Penalties for Non-compliance

The federal governments of both the United States and Canada have enacted legislation designed to curb the spread of communicable disease.[68] While the American federal government, acting primarily through the Centers for Disease Control and Prevention,[69] has been active in communicable disease control, the Canadian federal government's participation has largely been limited to the management of communicable disease in the context of people crossing the Canadian border.[70]

In addition to this central regulation through their federal governments, each U.S. state[71] as well as every Canadian province and territory[72] has

---

67. Even if this third party beneficiary problem were solved, the courts could construe any damages specified in a contract with a xenotransplant recipient as punitive penalties rather than liquidated damages. Such categorization would render such measures unenforceable, however, as it is a fundamental precept of contract law that damages for breach of contract must be an estimation of actual damages resulting from the breach, not a coercive mechanism to obtain performance. *See* RESTATEMENT (SECOND) OF CONTRACTS § 356 (1981). The same rule applies in Canada. *See* G.H.L. FRIDMAN, THE LAW OF CONTRACT IN CANADA 811-17(4th ed. 1999).

68. *See, e.g.,* 42 U.S.C. § 264 (1994) (U.S. Public Health Service Authority); 21 C.F.R. § 1240 (2001) (U.S. Food and Drug Administration Authority); Quarantine Act, R.S.C., ch. Q-1 (2000) (Can.).

69. The Centers for Disease Control and Prevention is an agency of the United States Department of Health and Human Services. For a description of the U.S. Centers for Disease Control's active role in public health matters, see Centers for Disease Control and Prevention, About CDC, *at* http://www.cdc.gov/aboutCDC.htm (last modified July 28, 2001).

70. *See* Immigration Act, R.S.C., ch. I-2, § 91 (2000) (Can.); Quarantine Act, R.S.C., ch. Q-1 (2000) (Can.).

71. *See, e.g.,* DEL. CODE ANN. tit. 16 §§ 501-508 (2001); D.C. CODE ANN. § 6-117 (1999); KAN. STAT. ANN. § 65-118 (2000); KAN. STAT. ANN. §§ 65-116(a)-(m), 119, 122, 123, 126-129 (1992).

enacted public health legislation specifically addressing communicable disease control. In Canada, although some provinces such as British Columbia and Saskatchewan have enacted specific venereal disease legislation,[73] most provinces deal with all communicable diseases by way of a single statute.[74] In the United States, the public health laws of most states are much more disease specific.[75] For instance, in addition to having a number of provisions that apply to communicable diseases generally, New York's public health law also has separate provisions dealing specifically with typhoid fever, poliomyelitis, tuberculosis, HIV, and others.[76]

In both the United States and Canada, public health legislation affords wide powers to public health officials. These include the powers to examine, detain, and isolate individuals, and to enter and close places.[77] Given that the collection and archiving of bodily samples is vital to effective post-xenotransplantation surveillance, the most significant power contained in public health legislation will be the authority to examine individuals. The nature and extent of the power to examine, however, varies from jurisdiction to jurisdiction. In the province of Ontario, for example, the medical officer of health can direct a person—under the authority of the Health Protection and Promotion Act—to submit "to an examination by a physician."[78] Unfortunately, because the Act does not define the term "examination," it is unclear whether this includes the power to collect bodily specimens.

---

72. Public Health Act, R.S.A. 1984, ch. P-27.1 (2001) (Can.); Public Health Act, R.S.M., ch. P210 (2001) (Can.); Health Protection and Promotion Act, R.S.O. 1990, ch. H-7 (2001) (Can.).

73. *See* Venereal Disease Act, R.S.B.C. 1996, ch. 475 (2001) (Can.); Venereal Disease Prevention Act, R.S.S. 1978, ch. V-4 (2000) (Can.).

74. *See* Public Health Act, R.S.A. 1984, ch. P-27.1 (2001) (Can.); Public Health Act, R.S.M., ch. P210 (2001) (Can.); Health Protection and Promotion Act, R.S.O. 1990, ch. H-7 (2001) (Can.).

75. *See, e.g.,* COLO. REV. STAT. § 25-4-1201 (2000) (streptococcus); DEL. CODE ANN. tit. 16 § 507 (2001) (diphtheria immunization); FLA. STAT. § 392.51 (2000) (tuberculosis); MD. CODE ANN. HEALTH-GEN. I § 18-324 (2001) (tuberculosis).

76. N.Y. PUB. HEALTH LAW § 2120 (McKinney 2001) (typhoid fever); N.Y. PUB. HEALTH LAW § 2164 (poliomyelitis, mumps, vaccinations); N.Y. PUB. HEALTH LAW § 2200 (McKinney 2001) (tuberculosis); N.Y. PUB. HEALTH LAW § 2781 (McKinney 2001) (HIV testing).

77. *See, e.g.,* DEL. CODE ANN. tit. 16 §§ 501-508 (2001); MD. CODE ANN. HEALTH-GEN. I § 18-324 (2001); Public Health Act, R.S.A. 1984, ch. P-27.1 §§ 30, 39, 40 (2001) (Can.); Health Protection and Promotion Act, R.S.O. 1990, ch. H-7 § 22(4) (2001) (Can.).

78. Health Protection and Promotion Act, R.S.O. 1990, ch. H.7, § 22(4)(f) (2001) (Can.).

The legislation in Quebec, although equally ambiguous, appears to grant relatively broad powers of examination.[79] The legislation specifies that the Minister of Health and Social Services has the duty to "establish and maintain a system for gathering . . . medical and epidemiological data . . . ."[80] Further, the provincial government, in consultation with the Bureau of Quebec Physicians, has the authority to "take the steps necessary" to examine persons coming under the jurisdiction of the relevant act.[81] Similarly, the California Health and Safety Code authorizes the State Department of Health, upon being informed by a health officer of any contagious, infectious, or communicable disease, to "take measures as are necessary to ascertain the nature of the disease and prevent its spread."[82] If the language of necessity in the Quebec and California statutes is meant to authorize a particular mode of examination so long as it can qualify as "necessary" to the determination of whether an individual is infected with a communicable disease, then these laws could be used to sanction the collection of bodily specimens.[83]

Some legislation, however, unambiguously provides for the collection of bodily samples. For instance, British Columbia's legislation specifically authorizes the collection of "blood, sputum or other excreta" and the performance of X-ray examinations.[84] Likewise, New York's public health law provides that the commissioner of health can set forth in the sanitary code of the state of New York "the diseases for which specimens shall be submitted for examination to a laboratory approved by the department."[85]

---

79. *See* Public Health Protection Act, R.S.Q. 1977, ch. P-35 (2001) (Can.).

80. *Id.* § 2(d).

81. *Id*. §§ 10, 11.

82. CAL. HEALTH & SAFETY CODE § 120,140 (West 2000). *See also id.* § 120,175.

83. Alberta's public health legislation also uses the language of necessity and, although equally as broad, is somewhat less vague than the legislation in Quebec and California. The Alberta legislation would almost certainly authorize the collection of bodily specimens since it provides that individuals coming under the purview of the Act must "submit to *any examinations necessary* to determine whether the person is infected with the disease." Public Health Act, R.S.A. 1984, ch. P-27.1, § 41 (2001) (Can.) (emphasis added).

84. Health Act, R.S.B.C. 1996, ch. 179, § 65(3) (2001) (Can.). Similarly, Saskatchewan public health legislation authorizes the taking of "specimens of blood or body discharge." Venereal Disease Prevention Act, R.S.S. 1978, ch. V-4, § 15(2) (2000) (Can.).

85. N.Y. PUB. HEALTH LAW § 225(5)(g) (McKinney 2001). *See also id.* § 201 (requiring the New York state department of health to "conduct laboratory examinations for the diagnosis and control of disease"); *id.* § 2100 (requiring local boards of health to exercise "proper and vigilant medical examination and control of all persons . . . infected with or exposed to [communicable diseases].").

In sum, the power to collect bodily samples for the purposes of examination probably exists in most jurisdictions. While the legislation in some jurisdictions expressly and unambiguously provides for the collection of bodily specimens, the legislation in other jurisdictions uses language that is sufficiently broad to infer the existence of the power to take samples.

On balance, public health law provides a more satisfactory legal mechanism to enforce xenotransplantation precautions than contract law. Unlike the law of contracts, public health law encompasses the authority to demand the performance of human conduct that officials deem necessary to protect society from the spread of infectious diseases.[86] Moreover, the enforcement provisions of public health legislation have greater coercive effect than those of contract law since courts can levy severe penalties for non-compliance with an order given pursuant to legislation. The nature and extent of these penalties vary greatly among jurisdictions. For instance, although every jurisdiction empowers officials to impose a monetary fine in the case of non-compliance, the maximum fine that they can issue varies greatly.[87] In addition, while the legislation in some jurisdictions provides only for the imposition of monetary fines,[88] the legislation in other jurisdictions also permits the temporary incarceration of non-compliant individuals.[89]

In short, current public health legislation may offer a source of legal authority from which to guarantee compliance with post-xenotransplantation public safety measures. Unlike contract law, existing public health legislation in some jurisdictions can require the performance of conduct such as the collection of bodily specimens. In addition, because of its strong enforcement provisions, public health law has coercive tools that contract law does not. What remains to be determined, however, is whether there are any impediments that might frustrate or disqualify the

---

86. *See supra* note 77 and accompanying text.

87. In Quebec, public health law authorizes the imposition of monetary fines up to a maximum of $1000 for each day that the offense continues. Public Health Protection Act, R.S.Q. 1977, ch. P-35, § 71 (2001) (Can.). In Ontario, the maximum is $5000 for each day or part day that the offense continues. Health Protection and Promotion Act, R.S.O. 1990, ch. H.7, § 101(1) (2001) (Can.). In contrast to these elevated penalties, Alberta's legislation provides for a fine of not more than $100 for each day that the offense continues. Public Health Act, R.S.A. 1984, ch. P-27.1, § 81(2) (2001) (Can.).

88. *See, e.g., id.*

89. In New York, violations of the sanitary code can result in both monetary penalties as well as imprisonment. A first offense is punishable by a fine not exceeding $250 or by imprisonment for a time not exceeding 15 days, or both. N.Y. PUB. HEALTH LAW § 229 (McKinney 2001). A subsequent offense is punishable by a fine not exceeding $500 or by imprisonment for a time not exceeding 15 days, or both. *Id.*

use of current public health legislation as a means of regulating xenotransplantation.

b) Current Public Health Legislation is Nevertheless Incapable of Adequately Regulating Xenotransplantation

One possible impediment to the use of current public health legislation is the common law right to self-determination. This right grants individuals the authority to accept, reject and/or withdraw their consent to medical treatments. The right to self-determination may not, however, hinder the application and enforcement of public health legislation, because statutes take precedence over such common law doctrines. Moreover, should a separate statute protect the right to self-determination, as it does in Ontario,[90] the public health legislation typically pre-empts the application of a conflicting statute.[91]

Nevertheless, there are a number of other reasons why current public health legislation cannot regulate xenotransplantation. One reason is that in the case of xenotransplantation, officials probably could not satisfy the legislation's conditions precedent. Typical conditions include the presence of a certain level of proof that the individual in question has in fact contracted an infectious disease and poses a risk to the public health. In Quebec, for example, officials have the power to examine only a "person who apparently has a disease" contemplated by the legislation.[92] In Ontario, officials must have "reasonable and probable" grounds for believing that a communicable disease "exists or may exist or that there is an immediate risk of an outbreak"; that the disease "presents a risk to the health of persons"; and that "the requirements specified in the order are necessary in order to decrease or eliminate the risk to health presented by the communicable disease."[93]

In general, satisfaction of the required level of proof will depend on the extent to which an individual *appears* to be sick. Thus, if an individual exhibits symptoms of infection officials may have grounds for invoking

---

90. *See* Health Care Consent Act, S.O. 1996, ch. 2 (2001) (Can.).

91. *See*, *e.g.*, Health Protection and Promotion Act, R.S.O. 1990, ch. H-7, §22(5.1) (2001) (Can.).

92. Public Health Protection Act, R.S.Q. 1977, ch. P-35 § 11 (2001) (Can.).

93. Health Protection and Promotion Act, R.S.O. 1990, ch. H.7, § 22(2) (2001) (Can.).

the legislation. In contrast, if an individual is asymptomatic officials will normally not have prima facie grounds justifying the application of the intrusive legislation. There are, however, exceptions to this general rule. Tuberculosis legislation in California provides one such exception. The legislation allows officials to examine those who are in close contact with individuals infected with active tuberculosis and anyone else officials have "reasonable grounds to determine are at heightened risk of tuberculosis exposure."[94] Such exceptions are present only in legislation that applies only to specific diseases and are therefore not generally applicable.

Because the infectious disease risks associated with xenotransplantation, even if foreseeable, are theoretical both in nature and in severity, there would probably be insufficient grounds for invoking and applying general public health law provisions to recipients for as long as they remained asymptomatic.[95] Yet, the viability of a post-xenotransplantation surveillance system depends upon its ability to collect epidemiological data whether the recipients appear to be symptomatic or not. Similarly, existing public health legislation would be inapplicable to xenotransplantation because it applies only to infectious diseases that legislators can list in the legislation or corresponding regulations. For instance, New York's officials can only enforce their public health legislation against individuals infected by or exposed to a communicable disease that the sanitary code expressly designates.[96]

The degree of specificity that the application of public health legislation currently requires is unattainable for xenotransplantation. Commentators have described xenotransplantation as presenting an unquantifiable yet undeniable risk to the public health.[97] The risk is undeniable because our science base enables us to appreciate the theoretical threats associated

---

94. CAL. HEALTH & SAFETY CODE § 120,142 (West 2000). *See also id*. §§ 121,363, 121,364.

95. As one group of commentators put it: "existing legislation would require modification in order to compel the continued surveillance of asymptomatic individuals. In general, Canadian public health laws are designed to allow a response when an individual has a known infectious disease. There are no 'monitoring' provisions." Florencio & Caulfield, *supra* note 8, at 283.

96. N.Y. PUB. HEALTH LAW § 2100 (McKinney 2001). Similarly, Ontario's public health legislation only applies to communicable and virulent diseases, the former being defined as "a disease specified as a communicable disease by regulation made by the Minister" and the later being defined as including those illnesses enumerated in the legislation such as ebola, plague, Lassa fever, leprosy, smallpox, syphilis, and tuberculosis as well as any diseases specified by regulation. *See* Health Protection and Promotion Act, R.S.O. 1990, ch. H.7, § 1(1) (2001) (Can.).

97. *See* Chapman et al., *supra* note 6. *See generally supra* notes 6-8 and accompanying text.

with xenotransplantation. More importantly, the risk remains unquantifiable because we have a limited ability to predict the nature and extent of the harms that might arise. Scientists have already discovered the identity of one potential disease threat that is capable of replicating in human cells in vitro[98] and in mice in vivo,[99] but does not appear to lead to illness in recipients.[100] There could exist countless other infectious agents residing in xenografts that have not yet been identified. These infectious agents could cause disease in their natural state or could recombine with innocuous human retroviruses to form new chimeric agents.[101] It is unclear which infectious agents present in xenografts would be communicable and pathogenic in human populations.[102]

In sum, current public health law provisions cannot be used to enforce post-xenotransplantation surveillance because the nature and communicability of the pathogen and severity of the resultant disease are not yet determined. Furthermore, most current public health legislation would fail because symptoms or other indices of disease are required before official intervention, even though adequate prevention of epidemics relies on the ability to identify infected but asymptomatic individuals. This is problematic given that public health law has the unique ability to enforce perform-

---

98. Paul Le Tissier et al., *Two Sets of Human-Tropic Pig Retrovirus,* 389 NATURE 681 (1997); Ulrich Martin et al., *Expression of Pig Endogenous Retrovirus by Primary Porcine Endothelial Cells and Infection of Human Cells,* 352 LANCET 692 (1998); Clive Patience et al., *Infection of Human Cells by an Endogenous Retrovirus of Pigs*, 3 NATURE MED. 282 (1997).

99. Luc J.W. van der Laan et al., *Infection by Porcine Endogenous Retrovirus After Islet Xenotransplantation in SCID Mice*, 407 NATURE 501 (2000).

100. Walid Heneine et al., *No Evidence of Infection with Porcine Endogenous Retrovirus in Recipients of Porcine Islet-Cell Xenografts*, 352 LANCET 695 (1998); Khazal Paradis et al., *Search for Cross-Species Transmission of Porcine Endogenous Retrovirus in Patients Treated with Living Pig Tissue*, 285 SCIENCE 1236 (1999).

101. Jon Allan, *Silk Purse or Sow's Ear*, 3 NATURE MED. 275 (1997); Douglas M. Smith, *Endogenous Retrovirus in Xenografts*, 328 NEW ENG. J. MED. 142 (1993). Such recombination is a course of events not uncommon in cells infected with retroviruses. M.A. McClure et al., *Sequence Comparisons of Retroviral Proteins: Relative Rates of Change and General Phylogeny,* 85 PROC. NAT'L ACAD. SCI. U.S.A. 2469 (1988). This latter mechanism is thought to account for the pandemics caused by the modified influenza viruses in 1957 (subtype H2N2) and 1968 (subtype H3N2). C. Scholtissek et al., *On the Origin of the Human Influenza Virus Subtypes H2N2 and H3N2*, 87 VIROLOGY 13 (1978).

102. Although some agents might not be pathogenic, others, like the deadly human influenza virus which in 1918 is estimated to have killed between 20 to 40 million people in less than a year, might result in considerable morbidity and mortality. *See* Elizabeth Pennisi*, Virology: First Genes Isolated From the Deadly 1918 Flu Virus*, 275 SCIENCE 1739 (1997).

ance of human conduct such as the collection of bodily specimens. It is this ability that renders public health law the most effective, if not the only, legal mechanism for ensuring compliance with the public safety measures.

There are, however, two solutions that may allow officials to apply public health legislation to xenotransplantation. Officials could either amend the general provisions in public health legislation so that they apply to xenotransplantation, or enact xenotransplantation-specific legislation. The latter represents the better solution because existing general public health provisions are ill-suited to cope with the exceptional difficulties posed by xenotransplantation, and because amendment to incorporate the necessary powers might overtax and confuse these provisions.

3. Proposal for New Xenotransplantation Legislation

The main function of xenotransplantation legislation would be to provide legal authority for the monitoring requirements of the public health safeguards—especially the periodic collection of bodily specimens from recipients regardless of whether or not they appear to be symptomatic, and the power to conduct post-mortem analyses. In this regard, the legislation would only apply to those individuals who undergo an animal-to-human organ, tissue, or cellxenotransplantation procedure. Pre-xenotransplanta tion baseline sampling would not fall under the aegis of the legislation but would instead be a prerequisite to undergoing the operation. In addition to authorizing monitoring of recipients, xenotransplantation legislation could provide a contingency plan in the event that recipients become infected with communicable agents as a result of the operation. If so, the legislation would need to grant public health officials the powers to treat and to detain and isolate the recipient if necessary. Alternatively, control of any emerging communicable illnesses, once detected through surveillance authorized by xenotransplantation-specific legislation, could be handled by existing public health legislation.

If enacted, the monitoring provisions of xenotransplantation legislation would grant health authorities greater power than that found in existing public health legislation. In existing legislation, the officials' power to examine functions only to assess whether an individual is infected with a specific and identifiable agent. Such an examination will normally lead to treatment or other intervention only if the examination results are positive. In the case of xenotransplantation monitoring provisions, however, the officials' power to examine must be expanded because monitoring will need to be an ongoing process as opposed to a single event. This is neces-

sary to monitor recipients for signs of infection and to collect epidemiological data because those carrying out the monitoring will be looking not for a specific agent but for any and all signs of infection that might arise over time. Ongoing monitoring will also be critical for the identification of novel infectious agents through epidemiological strategies that require large data bases, as well as data points collected at different moments in time.

In implementing xenotransplantation legislation, officials must also consider the appropriate penalties for violations of the monitoring provisions. In general, loss of liberty would be too onerous an enforcement mechanism to impose on recipients given the theoretical nature of the risks to the public health. As long as recipients remain asymptomatic and there is no evidence of further transmissibility, officials would not have sufficient grounds to justify imprisonment. If diligently enforced, monetary fines could be a sufficiently persuasive means of enforcement. Officials should, however, ultimately be empowered to isolate and detain individuals to prevent or quell the spread of disease should recipients become infected with a communicable agent posing a threat to the public health. Officials need to direct more thought toward devising the fairest enforcement model possible in light of the current social and scientific knowledge that has been gathered on xenotransplantation.

Another issue requiring further reflection is what level of government should have the power to enact and enforce the legislation. To be most effective, the public health safeguards would need to be uniformly applicable worldwide. Assuming that global implementation will not be feasible in the near future due to the novelty of the issue, uncertainty of the potential harm, and disparities in governmental and economic resources available to implement public health measures, legislation should at least extend to the largest areas with border controls—typically nations.[103] If it is not, then recipients receiving a xenotransplant in a jurisdiction with adequate safeguards could move to a jurisdiction having less onerous and possibly substandard safeguards. Such a state of affairs would erode the surveillance system and would therefore be unacceptable.

There are two ways of ensuring legislative uniformity within national borders. Legislators could prepare a single set of minimum safeguards that would be ratified at the local level by each of the provinces/states in every nation hosting clinical xenotransplantation. Another possibility would be to have the central governments of each nation enact the legislation. Al-

---

103. In areas such as the European Union with no national border controls, implementation across the included territory would be advisable.

though this latter option would pose little problem in countries where the federal government has played an active role in communicable disease control (for example, the United States),[104] it may pose problems in other countries where the involvement of the central government in public health matters has thus far been limited (for example, Canada).[105] Nevertheless, the problem is likely solvable given the national scope of the potential health problem.[106]

Although xenotransplantation legislation would impose onerous obligations on recipients, it nevertheless represents a fair compromise between outright prohibition of clinical xenotransplantation and unduly jeopardizing the public's health through non-existent, inadequate or ineffective regulation. In exchange for the opportunity to save and prolong their lives, xenotransplant recipients would provide society with the minimum level of epidemiological data that it requires to protect itself. When comparing the advantages of xenotransplantation with the disadvantages of the public health legislation, the advantage of saving one's life through xenotransplantation should greatly outweigh the drawback of having to provide periodic serum samples. Moreover, in light of the public health risks associated with xenotransplantation, the monitoring provisions would not represent an excessive safety measure. Rather, they would be a minimum precaution based on sound scientific principles. Thus, judicial review of

---

104. *See* Lawrence O. Gostin, *Public Health Law in a New Century—Part II: Public Health Powers and Limits*, 283 JAMA 2979, 2979-80 (2000). In addition to direct intervention through the U.S. Centers for Disease Control and other divisions of the U.S. Department of Health and Human Services, the federal government often uses its constitutional spending power to make crucial federal public health funds contingent on state conformance with uniform federal standards. *See id.* at 2980.

105. *See supra*, note 70 and accompanying text.

106. For example, given its dual jurisdiction over matters of health, the Canadian parliament likely possesses the authority to enact xenotransplantation legislation:

> Legislation dealing with health matters has been found within the provincial power where the approach in the legislation is to an aspect of health, local in nature . . . . On the other hand, federal legislation in relation to 'health' can be supported where the dimension of the problem is national rather than local in nature . . . . In sum 'health' is not a matter which is subject to specific constitutional assignment but instead is an amorphous topic which can be addressed by valid federal or provincial legislation, depending in the circumstances of each case on the nature or scope of the health problem in question.

Schneider v. The Queen, [1982] 2 S.C.R. 112, 141-142.

xenotransplantation legislation should be reluctant to dismiss the scientific underpinnings upon which it is founded.[107]

III. CONSTITUTIONAL DIMENSION: BALANCING THE RIGHTS OF THE COLLECTIVE AND THE DUTY OF THE STATE TO PROTECT THE PUBLIC HEALTH WITH THE RIGHTS OF THE INDIVIDUAL

The use of coercive measures such as monetary fines to attain public health goals raises difficult issues concerning an individual's responsibility to protect other members of society as well as society's obligation to respect the civil rights and liberties of its individual citizens.[108] Should

---

107. Lawrence O. Gostin, *Public Health Law in a New Century—Part III: Public Health Regulation: A Systematic Evaluation*, 283 JAMA 3118, 3120 (2000):

> [T]o the extent possible, risk assessments should be based on objective and reliable scientific evidence provided by the multiple disciplines of public health, including medicine, virology, bacteriology, and epidemiology. Science-based risk assessments provide a more secure ground for decision making and avoid reflexive actions based on irrational fears, speculation, stereotypes, or pernicious mythologies.

See also Lawrence O. Gostin, *The Future of Public Health Law*, 12 AM. J. LAW & MED. 461, 464 (1988) [hereinafter Gostin, *The Future of Public Health Law*]:

> Science has a more precise understanding of the etiological agents of infectious disease, the most likely harborers of the agent, the most efficient modes of its transmission, and the methods of modifying behaviors or environments in order to interrupt its spread. Accordingly, modern measures for reducing the spread of disease are predominantly based upon research, education, and counselling, specifically targeted to groups at risk of spreading or contracting the disease. Public health statutes and judicial review of public health action should reflect these new scientific understandings by requiring that the goals of public health measures be limited to the interruption of the most efficient modes of disease transmission.

108. As stated by one commentator:

> [T]here is a fundamental conflict of interest between providing medical care to individuals and providing public health services to a community. The patient-autonomy model that underlies personal health care is incompatible with the subrogation of individual interests that is necessary for effective public health . . . . Public health rejects the patient's right to have sole control of his/her treatment.

Edward P. Richards & Katharine C. Rathbun, *The Role of the Police Power in 21st Century Public Health*, 26 SEXUALLY TRANSMITTED DISEASES 350, 354-55 (1999).

xenotransplantation legislation be enacted and subsequently challenged,[109] courts will be seized with the delicate task of striking the right balance between individual and societal rights and responsibilities. The purpose of this section is not to provide an exhaustive discussion of the constitutional dimension of the problem but simply to offer some preliminary thoughts on some of the issues that are likely to be raised.

A. Individual Rights and Freedoms

1. Personal Rights and Liberties

Section 7 of the Canadian *Charter* guarantees an individual's right not to be deprived of life, liberty, or security of the person except in accordance with the principles of fundamental justice.[110] Xenotransplantation safeguards do not, however, involve literal intrusion upon the physical integrity of nonconsenting recipients since the monitoring provisions would provide for monetary sanctions, rather than physical force, as a means of enforcing the collection of bodily samples. This is important because physical intrusion would clearly violate the *Charter's* provisions.[111] Notwithstanding the non-physical nature of the coercion involved, xenotransplantation legislation could infringe a transplant recipient's constitutional rights. For instance, the legislation would infringe the recipient's right to personal autonomy and self-determination by removing the option of withdrawing his or her participation from public health safeguards[112] Ad-

---

109. Florencio & Caulfield, *supra* note 8, at 284 ("Although xenotransplant candidates would have to agree to participate in all public health measures to be eligible for the transplant procedure, once the procedure has taken place and their health has improved, patients may feel that the restrictions on their rights are too onerous.").

110. CAN. CONST. (Constitution Act 1982), pt. I (Canadian Charter of Rights and Freedoms), cl. 11 § 7.

111. CAN. CONST. (Constitution Act 1982), pt. I (Canadian Charter of Rights and Freedoms), cl. 11 § 7-8. If an individual is symptomatic, he will be isolated and detained in accordance with regular public health legislation and thus, there would be no violation of the Charter's provisions.

112. The right to autonomy derives from the common law but it is arguably also protected by the Charter. *See* Rodriguez v. B.C.(A.G.), [1993] 3 S.C.R. 519, 588:

> There is no question, then, that personal autonomy, at least with respect to the right to make choices concerning one's own body, control over one's physical and psychological integrity, and basic human dignity are encompassed within security of the person, at least to the extent of freedom from criminal prohibitions which interfere with these.

Given the quasi-criminal and penal nature of public health legislation, it is highly probable that the right to personal autonomy would enjoy as much protection in a public health context as it does in a criminal context. *See also* Fleming v. Reid, [1991] 4 O.R.

ditionally, by tying weighty penal consequences to non-compliant behavior, the legislation might also be contravening the recipient's interest in personal security by inflicting serious psychological stress upon him.[113] Determining the viability of xenotransplantation legislation under section 7 of the Charter would involve a two-step process. First, a court would decide if there had been a breach of the right to life, liberty or security of the person. If there was no breach, the legislation would be upheld as valid. If there was a breach, a court would next determine whether such a breach was in accordance with the principles of fundamental justice.

The Supreme Court of Canada has been using two different approaches to determine whether fundamental justice justifies a violation of personal rights and liberties. According to the first approach, the contravention of an individual's section 7 rights will be in accordance with the principles of fundamental justice so long as the societal or state interest outweighs the individual's right to life, liberty and/or security of the person.[114] The second approach is to perform an analysis under section 1 of

---

(3d) 74, 88 (C.A.) ("[T]he common law right to determine what shall be done with one's own body and the constitutional right to security of the person, both of which are founded on the belief in the dignity and autonomy of each individual, can be treated as co-extensive.").

113. *See* R. v. Morgentaler, [1988] 1 S.C.R. 30, 56 ("[S]tate interference with bodily integrity and serious state-imposed psychological stress, at least in the criminal law context, constitutes a breach of security of the person."). It is noteworthy that the minority in *Morgentaler* chose to set forth a more stringent test as to when state-imposed psychological stress would result in a violation of the security of the person interest:

> As to an asserted right to be free from any state interference with bodily integrity and serious state-imposed psychological stress, I would say that to be accepted, as a constitutional right, it would have to be based on something more than the mere imposition, by the State, of such stress and anxiety . . . . A breach of the right would have to be based upon an infringement of some interest which would be of such nature and such importance as to warrant constitutional protection. This, it would seem to me, would be limited to cases where the state-action complained of, in addition to imposing stress and strain, also infringed another right, freedom or interest which was deserving of protection under the concept of security of the person.

Id. at 146-147. Interestingly, because the monitoring provisions would both impinge upon the personal autonomy of recipients and impose psychological stress upon them, counsel for the recipients might contend that even the requirements of the minority's test would be satisfied in the circumstances.

114. *See, e.g.,* Thomson Newspapers v. Canada (Dir. of Investigation and Research, Restrictive Trade Practices Comm'n), [1990] 1 S.C.R. 425, 583 ("Fundamental justice in our Canadian legal tradition . . . is primarily designed to ensure that a fair balance be struck between the interests of society and those of its citizens"); s*ee also* R. v. Beare, [1988] 2 S.C.R. 387, 415 (holding that fingerprinting a person charged with but not con-

the Charter which states that the rights and freedoms guaranteed by the Charter are subject to "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[115] This Article argues that the second approach would be superior to the first in determining whether xenotransplantation legislation is justified by the principles of fundamental justice.

The first approach, or the 'balancing' approach, to fundamental justice is problematic in several regards. First, courts consider the societal interest under section 7, where the burden of proof lies with the *Charter* claimant, instead of under section 1, where the burden of proof lies with the state. Second, unlike section 1, section 7 does not provide an analytical framework capable of structuring judicial discretion during the performance of the balancing test. Third, the fact that courts consider the interests of the state along with those of the individual directly within section 7 of the *Charter* weakens the ability of the *Charter* to operate as a rights-based, counter-majoritarian instrument.[116]

The second approach defines the principles of fundamental justice as being located within the basic tenets of the Canadian legal system.[117] Under this approach, courts only consider the interests of the state under section 1 of the *Charter*.[118] This second approach does not suffer from the

---

victed of an indictable offense does not infringe upon rights guaranteed in section 7 of the Canadian Charter of Rights and Freedoms); R. v. Lyons, [1987] 2 S.C.R. 309 (examining whether the dangerous offenders provisions of the criminal code contravened the right to liberty guaranteed under the Charter); R v. Jones, [1986] 2 S.C.R. 284 (balancing the compelling state interest in compulsory education against right to liberty under Section 7 of the Charter).

115. CAN. CONST. (Constitution Act 1982), pt. I (Canadian Charter of Rights and Freedoms), cl. 11 § 1.

116. *See* Patrik S. Florencio & Robert H. Keller, *End-of-Life Decision Making: Rethinking the Principles of Fundamental Justice in the Context of Emerging Empirical Data*, 7 HEALTH L. J. 233, 247 (1999).

117. *See* Reference Re Section 94(2) of the *Motor Vehicle Act*, R.S.B.C. 1979, [1985] 2 S.C.R. 486, 503 ("The principles of fundamental justice are to be found in the basic tenets of our legal system. They do not lie in the realm of general public policy but in the inherent domain of the judiciary as guardian of the justice system.").

118. For example, legislation depriving individuals of life, liberty, and security of the person must not be substantively or procedurally arbitrary lest it violate the principles of fundamental justice. *See* B.(R.) v. Children's Aid Soc'y of Metro. Toronto, [1995] 1 S.C.R. 315, 374 ("The protection of a child's right to life and to health, when it becomes necessary to do so, is a basic tenet of our legal system, and legislation to that end accords with the principles of fundamental justice . . . ."); R. v. Swain, [1991] 1 S.C.R. 933, 977 (holding that the "common law rule which allows the Crown to raise evidence of insanity over and above the accused's wishes is a denial of liberty which is not in accordance with the principles of fundamental justice"); Singh v. Minister of Employment and Immigra-

infirmities enumerated above and is hence both analytically superior and more just in its result than its balancing counterpart.[119]

According to either the first or the second approach, however, the xenotransplantation legislation meets the requirements of fundamental justice, although the second approach requires that the legislation meet a stricter test. Indeed, given that the monitoring provisions would not be arbitrary—they would be based on *sound* scientific principles for the *legitimate* objective of protecting the public health and would apply *only* to individuals having received a xenotransplantation—officials could forcefully maintain that the legislation would not be in violation of the principles of fundamental justice. Thus, notwithstanding the breaches to the personal security interest of recipients, the monitoring legislation would not contravene section 7 of the *Charter* since the breaches would be in accordance with fundamental justice.

The U.S. Constitution also limits the extent to which public health legislation may impinge upon the fundamental rights of privacy and bodily integrity. The concept of privacy is most directly embodied in the Fourth Amendment to the Constitution, which provides that the government shall not violate "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[120] The Supreme Court has consistently held that state-compelled collection and testing of bodily fluids such as blood or urine, such as would be required of xenotransplant recipients, is a "search" subject to the Fourth Amendment.[121] Whether a search or seizure passes constitutional scrutiny under the Fourth Amendment would depend upon whether that search or seizure is reasonable in light of the balance between the intrusion on the

---

tion, [1985] 1 S.C.R. 177, 220 (holding that procedures under the 1976 Immigration Act did not meet the requirements of fundamental justice under section 7 of the Charter and that such procedures did not constitute a reasonable limit on the rights of persons claiming refugee status within the meaning of section 1 of the Charter).

119. *See* Florencio & Keller, *supra* note 116, at 247-248, for a more detailed discussion of why the second approach is superior to the first approach.

120. U.S. CONST. amend. IV.

121. *See*, *e.g.*, Vernonia School District 47J v. Acton, 515 U.S. 646, 652 (1995); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 617 (1989); Schmerber v. Cal., 384 U.S. 757, 767-68 (1966). Courts would consider a search that is authorized or required by xenotransplantation legislation to be state-compelled even if private transplant centers or physicians conduct it. *See Skinner*, 489 U.S. at 614-15. Courts may also view sampling of bodily fluids as a "seizure" because it interferes with a xenotransplant recipient's possessory interest in her bodily fluids. *See id.* at 617, n.4.

individual's legitimate privacy interests and the government's legitimate interest in protecting the public health.[122]

Courts are likely to find that the intrusion on a transplant recipient's privacy is minimal for several reasons. First, a reasonable expectation of the privacy of her bodily fluids is substantially reduced because ongoing surveillance of those bodily fluids would follow a recipient's voluntary and extensive experience with the high degree of intrusion involved in transplant surgery and the large number of related medical examinations that are conducted before and after surgery.[123] Second, several factors would make the character of the intrusion less compromising of privacy. Two such factors are that officials would likely take blood samples rather than excretory fluids[124] and that officials would draw these samples in a medical establishment rather than in a more public setting.[125] A final consideration which should inform the drafting of xenotransplantation legislation, is that courts will be more likely to consider a search or seizure reasonable if the results are disclosed only to those who need to know the results—i.e., the recipient's physicians and relevant public health authorities.[126]

Privacy and bodily integrity are also protected by the "substantive due process" conception of implied fundamental liberty rights embodied in the Due Process Clause of the Fourteenth Amendment.[127] Courts generally

---

122. *See Vernonia*, 515 U.S. at 652-53. Although we believe that the risks posed by xenotransplantation without surveillance make the government's interest in surveillance compelling, the U.S. Supreme Court requires only that the governmental interest be more important than the legitimate expectation of privacy that testing would intrude upon. *See id.* at 660-61. However, it is particularly important that the governmental interest in surveillance clearly outweighs the privacy interest because xenotransplant recipients would be tested without individual suspicion of infection. *See Skinner*, 489 U.S. at 624 (holding that a search may be reasonable despite the absence of individualized suspicion if the important governmental interest furthered by the search would be jeopardized by a requirement of individualized suspicion).

123. *See Vernonia*, 515 U.S. at 656-57 (holding that student athletes have a reduced expectation of privacy because they voluntarily "go out for the team" and because public school students already are subject to medical examination and vaccination).

124. *See Skinner*, 489 U.S. at 617, 626 (distinguishing blood tests from urinalysis and other tests taken in a manner that compromises traditional expectations of privacy).

125. *See Schmerber*, 384 U.S. at 771 (holding that blood tests are more reasonable when taken by a physician in a hospital environment according to accepted medical practices).

126. *See Vernonia*, 796 F. Supp. at 1364.

127. *See*, *e.g.*, Cruzan v. Dir., Miss. Dept. of Health, 497 U.S. 261, 262 (1990) (discussing the right to bodily integrity); Roe v. Wade, 410 U.S. 113, 153 (1973) (recognizing that the right to privacy encompasses the abortion decision); Eisenstadt v. Baird, 405 U.S. 438, 438 (1972) (recognizing a fundamental right to privacy including the decision

subject laws that burden a fundamental right to "strict scrutiny."[128] Under strict scrutiny, when an individual's liberty interest is balanced against the government's interest in enforcing a restriction on liberty, the restriction must be narrowly drawn to achieve a compelling state interest, rather than merely having a rational relation to a governmental interest.

Even if we assume that a court would apply strict scrutiny, xenotransplantation legislation is likely to pass constitutional muster. For decades the Supreme Court has been highly deferential to the government with respect to public health legislation, rarely questioning its compelling nature.[129] This is particularly true when legislation calls for intrusions of limited duration and severity,[130] and when it protects the health of the individual whose rights are being intruded upon, as well as the rights of the populace.[131] Although monitoring of a xenotransplant recipient could go on for an indefinite duration, perhaps for many years, the severity of the intrusions necessary for surveillance should be minimal and the health of the recipient is protected by such surveillance. Thus, carefully drawn xenotransplantation legislation should withstand a substantive due process challenge.

2. Finding the Right Balance

This section has argued that although the monitoring provisions in xenotransplantation legislation would constitute a violation of the rights of recipients to liberty and/or to the security of their persons, this violation would be in accordance with the principles of fundamental justice and therefore inherently justified. Lest this reasoning be amiss, it is also important to inquire whether the proposed legislation might be justified on

---

whether or not to use contraception). *But see*, Bowers v. Hardwick, 478 U.S. 186, 191 (1986) (failing to extend the right of privacy to acts of sodomy). The Fourteenth Amendment provides that no state shall "deprive any person of life, liberty, or property, without due process of law." U.S. CONST. amend. XIV.

128. *See*, *e.g.,* Planned Parenthood of Southeastern Pa. v. Casey, 505 U.S. 833, 871 (1992).

129. *See*, *e.g.,* Washington v. Harper, 494 U.S. 210, 222 (1990) (finding that forced treatment of a prisoner with antipsychotic medication was justified by potential harm to the prisoner and others); Whalen v. Roe, 429 U.S. 589, 603-604 (1977) (upholding prescription reporting legislation for controlled substances); Buck v. Bell, 274 U.S. 200, 207 (1927) (allowing sexual sterilization of a mentally retarded prisoner on public health grounds); Jacobson v. Mass., 197 U.S. 11, 31 (1905) (upholding compulsory vaccination of the general public).

130. *See*, *e.g., Jacobson*, 197 U.S. at 24-30.

131. *See, e.g., id.*; *Washington*, 494 U.S. at 222.

the less fundamental ground that it imposes reasonable limitations that can be demonstrably justified in a free and democratic society.[132]

In his book "The Plague," Camus expressed the idea that the consequences of an epidemic are not experienced by citizens individually, but by society as a whole in the form of a collective history.[133] It is exactly this characteristic—the collective nature of the health ramifications that can result from infectious diseases—that makes public health legislation so important. Public health law seeks to reduce the incidence of morbidity and mortality by preventing or curbing the spread of infectious diseases. Society has long considered the protection and preservation of the public health to be a value of fundamental importance and this sentiment persists to this day.[134] The state would clearly have a compelling interest in enforcing a surveillance system that aims to acquire epidemiological data that would permit health authorities rapidly to identify and contain infectious agents that could arise from xenotransplantation.

Yet, even when the state sets out to accomplish an important end point, the means by which it attempts to do so must be rationally related to the purpose of the legislation. In the case of public health legislation, the

---

132. The answer to this question should inform any constitutional analysis of xenotransplantation legislation, but is specifically required under section 1 of the *Charter*. *See* CAN. CONST. (Constitution Act 1982), pt. I (Canadian Charter of Rights and Freedoms), cl. 11 § 1. For the leading case on balancing under section 1 of the Charter, see R. v. Oakes, [1986] 1 S.C.R. 103.

133. *See* ALBERT CAMUS, THE PLAGUE 167 (Stuart Gilbert trans., Vintage Int'l 1991):

> Thus week by week the prisoners of plague put up what fight they could. Some . . . even contrived to fancy they were still behaving as free men and had the power of choice. But actually it would have been truer to say that by this time . . . the plague had swallowed up everything and everyone. No longer were there individual destinies; only a collective destiny, made of plague and the emotions shared by all.

134. *See*, Gostin, *The Future of Public Health Law*, *supra* note 107, at 483:

> Ultimately, the right of the state to take measures which avoid a probable and grave harm must be respected, even at the cost of individual civil liberties. It does no service to groups at risk for disease to fail to implement effective public health measures in the name of protection of their liberty. The health of the community is perhaps the most important human and societal value.

The Latin maxim *salus populi suprema lex*, meaning that the welfare or health of the people is the supreme law of the land, frequently appeared in nineteenth century cases such as *Haverty v. Bass*, 66 Me. 71 (1876). *See* WILLIAM J. NOVAK, THE PEOPLE'S WELFARE: LAW AND REGULATION IN NINETEENTH-CENTURY AMERICA (1996). *See also* Elmer E. Smead, Sic utere tuo ut alienum non laedas: *A Basis of the State Police Power*, 21 CORNELL L.Q. 276 (1936).

means, or the specific powers that the legislation grants, must be premised on the biological characteristics of the particular infectious disease threats from which the legislation seeks to shield society. For instance, although restrictions on the rights to liberty and association may be a valid policy in the case of airborne pathogens, they are not justified in the case of blood-borne pathogens such as HIV, whose transmissibility is limited to activities such as blood transfusions, sexual relations and/or needle-sharing.[135]

The biological reality of xenotransplantation is that animal agents residing in xenografts could infect xenotransplant recipients who could then pass the agents to the community at large. Although this infectious disease threat is foreseeable, the identity of the agents that are likely to infect recipients as a result of xenotransplantation, and the method of their transmission, remain unknown. Given this reality, the government's implementation of a surveillance system to collect data that will hopefully enable scientists to identify and track down infectious agents that might arise as a result of xenobiotechnology is unquestionably a rational means of protecting the public health. Moreover, requiring xenotransplant recipients to engage in conforming behavior would be central to the state's interest in having an effective surveillance system given that "[i]ncomplete and unreliable data [would] greatly reduce our power to detect and contain outbreaks of infectious disease."[136]

Such a surveillance system would also constitute the most equitable means of protecting the public health from the infectious disease risks associated with xenotransplantation. The government could take other approaches to fulfill this important objective such as isolating recipients or forbidding clinical xenotransplantations until more is known about the infectious disease risks. These approaches would be better suited to the task of protecting the public health but would involve far greater restrictions to the liberty and security interests of recipients. A surveillance system has the distinct advantage of offering an important means of protecting the public health while allowing recipients both to take advantage of xenobiotechnology and to retain their freedoms of movement and association within society. Thus, a surveillance system represents the best of the possible options.

It is important, however, not to make light of the fact that xenotransplantation legislation—by authorizing the periodic examination of asymptomatic xenotransplant recipients—would grant health authorities greater

---

135. L.O. Gostin, *The Resurgent Tuberculosis Epidemic in the Era of AIDS: Reflections on Public Health, Law, and Society*, 54 MARYLAND L. REV. 1, 8 (1995).

136. Florencio & Caulfield, *supra* note 8, at 284.

power than that provided by traditional public health legislation. It would, in other words, represent an extensive change to our existing law and would need to be rigorously justified by public policy. Policy matters involving extensive changes to the existing law are better left, in a constitutional democracy, to the legislative branch of government.[137] Correspondingly, when asked to review legislative solutions to complex matters of policy, the judiciary should extend to the legislature a sufficient degree of deference.[138] This is especially true when the policy matter relates to the protection of the public health.[139] If a court struck down xenotransplanta-

---

137. *See*, *e.g.*, Dobson (Litig. Guardian of) v. Dobson, [1999] 2 S.C.R. 753, 766 ("Matters of public policy are concerned with sensitive issues that involve far-reaching and unpredictable implications for Canadian society. It follows that the legislature is the more appropriate forum for the consideration of such problems and the implementation of legislative solutions to them."); s*ee also* Winnipeg Child and Family Servs. v. G.(D.F.), [1997] 3 S.C.R. 925, 960-961 (holding that it is not appropriate for a court to extend its power to order the detention of a pregnant woman for the purpose of preventing harm to her unborn child); Watkins v. Olafson, [1989] 2 S.C.R. 750, 764 (holding that in the absence of enabling legislation or the consent of all parties, a court cannot order that a plaintiff forego his traditional right to a lump-sum judgment for a series of period payments).

138. *See, e.g.,* McKinney v. Univ. of Guelph, [1990] 3 S.C.R. 229, 315:

> [H]aving accepted the importance of the legislative objective, one must . . . recognize that if the legislative goal is to be achieved, it will inevitably be achieved to the detriment of some. Moreover, attempts to protect the rights of one group will also inevitably impose burdens on the rights of other groups. There is no perfect scenario in which the rights of all can be equally protected.

See also Irwin Toy Ltd. v. Quebec (A.G.), [1989] 1 S.C.R. 927, 933 (sustaining the reasonableness of a legislative conclusion that a "ban on commercial advertising directed to children was the minimal impairment of free expression consistent with the pressing and substantial goal of protecting children against manipulation through advertising"); R. v. Edwards Books and Art, [1986] 2 S.C.R. 713, 787 (upholding the constitutionality of the Retail Business Holidays Act based on the stated legislative purpose). American case law also expresses the view that a degree of deference must be extended to the legislature. *See, e.g.,* Williams v. Mayor of Baltimore, 289 U.S. 36, 42 (1933) ("The judicial function is exhausted with the discovery that the relation between means and end is not wholly vain and fanciful, an illusory pretense. Within the field where men of reason may reasonably differ, the legislature must have its way.").

139. *See supra* note 129; s*ee also* Arizona ex rel. Conway v. Southern Pac. Co., 145 P.2d 530, 532 (Ariz. 1943) ("where the police power is set in motion in its proper sphere, the courts have no jurisdiction to stay the arm of the legislative branch") (quoting State v. Superior Court, 174 P.973, 976 (Wash. 1918).). *See generally* Lawrence O. Gostin, *The Americans with Disabilities Act and the Corpus of AntiDiscimination Law: A Force for Change in the Future of Public Health Regulation*, 3 HEALTH MATRIX 89 (1993) (arguing that the standard judicial review of the constitutionality of public health statutes is being replaced by disability law which is applicable to protect people with infectious conditions).

tion legislation on constitutional grounds, the capacity of the surveillance system to generate the data required for the protection of the public health would depend entirely on the willingness of recipients voluntarily to comply with the safeguards. In the absence of such willingness, the surveillance system would collapse and society could be left defenseless in the wake of an epidemic.

B. Freedom From Discrimination

Since xenotransplantation legislation would only apply to individuals who underwent a xenotransplant operation, one might ask whether the legislation violates section 15 of the *Charter* by infringing an individual's right to be free from discrimination.[140] In *Law v. Canada (Minister of Employment and Immigration)*, the Supreme Court of Canada recently restated the appropriate approach to conducting equality analyses.[141] The Court stated that a court making a discrimination inquiry should make the following inquiries:

> First, does the impugned law (a) draw a formal distinction between the claimant and others on the basis of one or more personal characteristics, or (b) fail to take into account the claimant's already disadvantaged position within Canadian society. . . .? Second, was the claimant subject to differential treatment on the basis of one or more of the enumerated and analogous grounds? And third, does the differential treatment discriminate in a substantive sense, bringing into play the purpose of s. 15(1) of the Charter in remedying such ills as prejudice, stereotyping, and historical disadvantage?[142]

A court making the above inquiry would not hold that xenotransplantation violates an individual's right to be free from discrimination. Xenotransplantation legislation would draw a formal distinction on the basis of whether or not individuals are recipents of animal cells, tissues and/or organs and would impose the burden of complying with the public health safeguards upon those who are recipients. This distinction, however, would not be based on an enumerated or analogous ground.[143] More-

---

140. CAN. CONST. (Constitution Act 1982), pt. I (Canadian Charter of Rights and Freedoms), cl. 11 § 15.

141. *See* Law v. Canada (Minister of Employment and Immigration), [1999] 1 S.C.R. 497, 524.

142. *Id.*

143. Some may argue that xenotransplantation legislation would distinguish individuals on the basis of physical disability which is an enumerated ground. Yet, the mere fact of having undergone a xenotransplantation and consequently of being a carrier of

over, even if one could persuasively argue that the legislation did distinguish on the basis of an enumerated or analogous ground, the legislation would not be discriminatory because it would not be based on stereotyping, historical disadvantage, or political and social prejudice in Canadian society. It would be based, rather, on sound scientific principles and the need to safeguard the health of society.

The corresponding analysis under the Equal Protection Clause of the Fourteenth Amendment to the U.S. Constitution is similar.[144] The law does not allow public health authorities to exercise their police powers in ways that discriminate based upon race or other suspect classes without a compelling state interest.[145] Governmental regulation of the public health, however, would not violate the Equal Protection Clause merely because it applies only to xenotransplant recipients and is, therefore, not all-encompassing.[146] Xenotransplantation legislation would apply uniformly to all xenotransplant recipients and therefore would only need to be rationally related to a legitimate government interest to survive constitu-

---

animal cells, tissues and/or organs does not render recipients physically disabled. There is no disability per se. If it were otherwise, then all individuals having undergone some form of surgery, or at least those having undertaken an allotransplantation, would be subject to the characterization of being physically disabled and would be deserving of constitutional protection. Interestingly, Professor Hogg has contended that legislative distinctions that are based on personal characteristics arising as a result of voluntary choices, such as the choice to undergo a xenotransplantation, are not deserving of constitutional protection. *See* PETER W. HOGG, CONSTITUTIONAL LAW OF CANADA 914-15 (4th ed. 1996):

> Another way of looking at immutability as the common element of the listed personal characteristics is to notice that the characteristics are inherent, rather than acquired. They do not reflect a voluntary choice by anyone, but rather an involuntary inheritance . . . . It is true that individuals may claim to be treated unfairly by the law for conditions that are their own responsibility, but this kind of claim even if fully justified does not warrant a constitutional remedy.

144. The Equal Protection Clause provides that the government may not deprive any person of life, liberty or property "without equal protection of the laws." U.S. CONST. amend. XIV.

145. *See*, *e.g.*, City of Cleburne v. Cleburne Living Ctr., 473 U.S. 432, 442-46 (1985) (declining to recognize the mentally retarded as a quasi-suspect class, and suggesting similar treatment for "the disabled, the mentally ill, and the infirm"); Coolbaugh v. State of La., 136 F.3d 430, 433-34 (5th Cir. 1998) (surveying federal case law denying heightened scrutiny for various forms of physical disability); Jew Ho v. Williamson, 103 F. 10 (N.D. Cal. 1900) (striking down a bubonic plague quarantine that affected only the Chinese population).

146. *See* Zucht v. King, 260 U.S. 174, 176-77 (1922).

tional scrutiny.[147] In light of the sound public health rationale for enacting xenotransplantation safeguards and the lack of any history of discrimination against xenotransplant recipients, narrowly drawn xenotransplantation legislation would survive challenge under the Equal Protection Clause.[148]

Although some may worry that officials may enforce xenotransplantation legislation in a discriminatory manner—namely, in a manner that is influenced by social characteristics instead of in a manner that is neutral and uniform—this risk does not speak to the constitutionality of the legislation itself. Should such difficulties arise, agencies such as human rights commissions[149] and/or ombudspersons[150] could remedy them. Interestingly, similar fears were raised [151] when the New York City Department of Health updated its Health Code to permit compulsory actions, such as the detention for treatment of persistently non-compliant tuberculosis infected individuals.[152] The anticipated discriminatory practices, however, never materialized.[153] Indeed, a recent follow-up study found that the Health Code was not enforced in a discriminatory fashion since patients were detained on the basis of their history of compliance, rather than on the basis of their social characteristics.[154]

---

147. *See*, *e.g.*, *City of Cleburne*, 473 U.S. at 442 (1985) (zoning regulations barring group home for the mentally disabled subject only to the rational basis test, not heightened scrutiny).

148. Indeed, it has been suggested that even legislation quarantining all HIV-infected individuals—a concept far more restrictive than most alternative strategies now in place to control the spread of HIV—would likely pass muster under the Equal Protection Clause. *See* 7 Deborah Jones Merritt, *Communicable Disease and Constitutional Law: Controlling AIDS*, 61 N.Y.U. LAW REV. 739 (1986).

149. *See*, *e.g.*, Human Rights Code, S.O. 1993, ch. H.19 (2001) (Can.).

150. *See*, *e.g.*, Ombudsman Act, R.S.O. 1990, ch. O.6 (2001) (Can.).

151. George J. Annas, *Control of Tuberculosis—The Law and the Public's Health* 328 NEW ENGL. J. MED. 585 (1993) (raising the concern that the tuberculosis regulations might be enforced in a discriminatory manner—i.e., that patients with a history of drug abuse or homelessness could be singled out for legal action).

152. N.Y. CITY HEALTH CODE § 11.47(d) (1994).

153. For an excellent discussion of the legal and policy issues surrounding the tuberculosis control measures that were adopted by the New York City Department of Health, see Carlos A. Ball & Mark Barnes, *Public Health and Individual Rights: Tuberculosis Control and Detention Procedures in New York* City, 12 YALE LAW & POLICY REVIEW 38 (1994).

154. M. Rose Gasner et al., *The Use of Legal Action in New York City to Ensure Treatment of Tuberculosis,* 340 NEW ENGL. J. MED. 359, 365 (1999).

IV. CONCLUSION

Given the significant risks of harm associated with xenobiotechnology, the scientific community agrees that robust public safety measures need to accompany the introduction of clinical xenotransplantation. There is a need to devise a legally effective means of ensuring adherence to such public safety measures because a recipient's refusal to comply voluntarily with the safeguards would leave society without any means of protecting itself in the event of emerging infectious diseases. This Article has argued that xenotransplantation-specific public health legislation presents the most effective means of enacting and enforcing the appropriate public health safeguards.

Neither consent law nor the law of contracts would be capable of accomplishing this important objective. Consent law is ill suited to enforce the specific performance of promises because lawmakers designed it to serve as a mechanism of communicating the waiver of legal rights on the part of the consenting party, thereby obviating liability on the part of the party who received the consent. In the case of xenobiotechnology, the consent of recipients to the xenotransplant procedure and to its accompanying safeguards, such as the periodic collection of bodily specimens, would merely indicate the acquiescence of recipients to having the interventions performed on their person. Importantly however, the recipients' consent would not legally bind them, because they could unilaterally withdraw their consent to the public health safeguards at any time after having received the xenotransplant.

Contract law would be similarly ineffective. Because it would be essential for recipients to comply personally with the public safety measures, the law of contracts would be unable to use state power to force the personal execution of contractual obligations. Moreover, because specific performance of these contracts would be incompatible with competing legal principles, including the inviolability of the human body, an invasion of civil liberties would need to be expressly authorized by legislation.

In addition, existing public health legislation is not capable of enforcing the necessary public health safeguards. Although existing public health legislation might be amended to incorporate the powers necessary for the periodic examination of asymptomatic xenotransplant recipients, such amendments might overburden and confuse the existing statutes. The better solution would be to enact new legislation specific to the underlying science and particular risks of harm associated with xenotransplantation.

Xenotransplantation legislation would be a legally effective means of compelling compliance with the safeguards. Such legislation could require

the performance of conforming behaviors and could authorize the issuance of monetary fines against recipients who, having benefited from the life saving intervention, refuse to honor their obligations under the legislation. Ultimately however, the ability of xenotransplantation legislation to guarantee the generation of the epidemiological data necessary to protect the public health will depend on its ability to withstand constitutional attack.

EXORCISING THE SPECTER OF A "PAY-PER-USE" SOCIETY: TOWARD PRESERVING FAIR USE AND THE PUBLIC DOMAIN IN THE DIGITAL AGE

By John R. Therien[†]

ABSTRACT

The Digital Millennium Copyright Act unconstitutionally limits the rights of users to make fair use of materials protected by technical protection systems (TPSs). By criminalizing the distribution of devices designed to circumvent digital fences, the DMCA prevents users who lack the technical facility to circumvent TPSs from accessing material protected by TPSs. As a result, it is impossible for users without the technical skill to circumvent TPSs to exercise their First Amendment right to make fair use of the material protected by TPSs. Courts, by giving a broad reading to the protections of the DMCA, have failed to militate against this restriction on fair use. Further, the fail-safe rulemaking provision provided for in the DMCA has failed to provide adequate protection for most fair use. Since the legislature has already spoken, it is up to the courts to interpret the DMCA in a manner that prevents content owners from using TPSs to erect digital fences throughout the public domain.

I. INTRODUCTION

The Internet has spurred a radical shift in the ability to reproduce, distribute, publish, and control media.[1] Digital content owners feel threatened by Internet users' ability to make and distribute digital copies. What once required a printing press can now be done quickly and easily with the click of a mouse. A compact disk containing the equivalent of 220,000

---

† Law clerk to the Honorable Margaret H. Marshall, Chief Justice, Massachusetts Supreme Judicial Court; J.D., 2001, University of California at Berkeley, Boalt Hall School of Law. This article was a co-recipient of Boalt Hall's 2001 Thelen, Marrin Prize for Law Journal Writing. Thanks to Professor Pamela Samuelson for her comments and review of earlier drafts, and especially warm thanks to my wife for her dedicated support and unflagging confidence in me.

1. *See* COMPUTER SCI. AND TELECOMM. BD. NAT'L RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE 4-5 (2000) [hereinafter DIGITAL DILEMMA].

pages of text can be copied perfectly in fifteen minutes[2] with equipment already present in half of American homes.[3] Because these copies are digital, the text, image, sound, or video will be reproduced perfectly every time.[4] Each copy then can be used to produce an unlimited number of additional perfect copies.[5] The potential for piracy is enormous,[6] and this problem is exacerbated because control over copying rests in the hands of millions of hard-to-identify individual users.[7] Complicating matters further is the fact that these users have little understanding of copyright law[8]

---

2. *See id.* at 31-32.

3. *See* Commerce.net, *Internet Demographics and eCommerce Statistics, at* http://www.commerce.net/research/stats/images/facts15.gif (last visited Sept. 1, 2001). By the end of the year 2005, seventy-five percent of Americans are expected to be online. At that point, an estimated 765 million people will use the Internet worldwide.

4. *See* DIGITAL DILEMMA, *supra* note 1, at 32.

5. *See id.*

6. Actual figures on copyright piracy are difficult to ascertain. Since illegal copying generally takes place in private, figures have to be extrapolated from limited information. *See id.* at 188. The International Intellectual Property Association, a private-sector coalition representing U.S. copyright industries, asserts that international piracy alone costs these industries as much as $22 billion per year. *See* International Intellectual Property Association, *Description of the IIPA, at* http://www.iipa.com/aboutiipa.html (last modified Aug. 2001); *see also* Software & Info. Indus. Ass'n, *SIAA's Report on Global Software Piracy 2000*, *available at* http://www.siia.net/piracy/pubs/piracy2000.pdf (last visited September 1, 2001).

7. Most online users leave little or no information about their identity or physical location in real-world space; adept users can be virtually untraceable. Geographic and personal anonymity make online personas hard to tie to individual persons. In the words of a notable New Yorker cartoon, "[o]n the Internet, nobody knows you're a dog." DIGITAL DILEMMA, *supra* note 1, at 50.

8. Some users believe that absence of copyright notice means the copy lacks copyright protection, that temporary downloading is not infringement, that noncommercial copies do not infringe, that personal use in the home is fair use, that license agreements made over the Internet are not binding, or that ignorance of the law absolves the user from liability. *See id.* at 124-25; *see also* Brad Templeton, *10 Big Myths About Copyright Explained*, *at* http://www.templetons.com/brad/copymyths.html (last visited September 1, 2001). Publicly held misconceptions are in part a result of the complexity of copyright law and the lack of the public's participation in its creation. *See* Jessica Litman, *Copyright Non-compliance (or Why We Can't "Just Say Yes" to Licensing)*, 29 N.Y.U. J. INT'L L. & POL. 237, 241 (1997) [hereinafter Litman, *Copyright Noncompliance*]; *see also* Jessica Litman, *Copyright, Compromise and Legislative History*, 72 CORNELL L. REV. 857 (1987) [hereinafter Litman, *Copyright, Compromise*]; Thomas P. Olson, *The Iron Law of Consensus: Congressional Responses to Proposed Copyright Reforms Since the 1909 Act*, 36 J. COPYRIGHT SOC'Y 109 (1989).

and a morality starkly different than that held by content owners.[9] Thus, content owners,[10] courts,[11] and the government[12] are understandably concerned about their ability to curb piracy and uphold proprietary rights on the Internet.[13]

In response to this situation, the producers and owners of copyrighted material have developed and implemented digital fences. This Comment refers to these fences as Technical Protection Systems ("TPSs"), although some commentators refer to them as copyright management systems[14] or

---

9. Many users who would trade music files on the Internet without regard to whether they were violating copyright would most likely not steal the same music from a record store. *But see* DIGITAL DILEMMA, *supra* note 1, at 127-28 n.11 (citing a nationwide survey released in October 1998, indicating almost half of all high school students admitted to stealing property from a store within the preceding year).

10. According to the president of Time Warner:

> This is a very profound moment historically. This isn't just about a bunch of kids stealing music. It's about an assault on everything that constitutes the cultural expression of our society. If we fail to protect and preserve our intellectual property system, the culture will atrophy . . . . Worst-case scenario: [t]he country will end up in a sort of cultural "Dark Ages."

Chuck Philips, *Music Giants Miss a Beat on the Web*, L.A. TIMES, July 17, 2000, at A1.

11. Judge Kaplan in the Southern District of New York found the situation serious enough to compare "[t]he spread of means of circumventing access to copyright works in digital form" to a "propagated outbreak epidemic" in which "[i]ndividuals infected with the 'disease' . . . cannot be relied upon to identify themselves to those seeking to control [it]." Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 331 (S.D.N.Y. 2000).

12. *See* H.R. REP. NO. 105-551, pt. 2, at 25 (1998).

13. Since information can be taken from computers anywhere in the world, even if authorities can locate the user, questions of what court should have jurisdiction and whose law should apply present serious problems. *See, e.g.,* Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 2d 692 (E.D. Va. 1999); *see also* David R. Johnson and David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); *see generally* Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA. J. L. & TECH. 3 (1997). Even assuming that courts can overcome these jurisdictional problems, enjoining Internet activities can be difficult. The Southern District Court of New York enjoined the posting of a decryption program designed to allow unauthorized access to DVDs, but the program was readily available on the Internet soon thereafter. *See generally Reimerdes*, 111 F. Supp. 2d 294.

14. *See, e.g.,* Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L. J. 161, 161-64 (1997).

automated rights management systems.[15] TPSs can protect content where the law cannot; they can be quite useful in overcoming problems of enforcement of proprietary rights for digital content owners. Strong TPSs are particularly appealing because they are extremely difficult to hack. Unfortunately, both strong and weak TPSs can offer greater protection than the law, until recently, has allowed. The recent change in the law is the Digital Millennium Copyright Act ("DMCA"), passed in 1998.[16]

Congress passed the DMCA to address the online piracy of digital media, the same threat targeted by TPSs.[17] The new law represents a shift in legislative focus from the use of information—the traditional purview of the Copyright Act—to the devices and means by which one delivers or uses this information.[18] The DMCA gives content owners a new right: the right to sue in court to prevent the circumvention of their TPSs.[19] Specifically, the statute's anti-circumvention provisions prohibit three things: first, the circumvention of TPSs that protect access to content that contains any copyrighted material;[20] second, the manufacture or distribution of de-

---

15. *See* Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998). TPS is used because the terms "copyright management systems" and "automated rights management systems" are too narrow: the former obscures the fact that technological means of protection may guard media that is not, and indeed cannot be, covered by copyright; the latter, like the former, includes the term "rights," the scope of which is a crucial question.

16. 17 U.S.C. §§ 1201-1203 (Supp. 2000).

17. The Congressional Commerce Committee stated in its report on the DMCA:

> [T]he digital environment poses a unique threat to the rights of copyright owners, and as such, necessitates protection against devices that undermine copyright interests. In contrast to the analog experience, digital technology enables pirates to reproduce and distribute perfect copies of works—at virtually no cost at all to the pirate. As technology advances, so must our laws.

H.R. REP. NO. 105-551, pt. 2, at 25 (1998).

18. *See* David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 683 (2000).

19. The statute may also be read to have created a new right similar in scope to those in the copyright bundle. Section 106 protects the rights to make copies, to prepare derivative works, to distribute copies to the public, to perform or display limited types of works, and to perform sound recordings by means of digital audio transmission. 17 U.S.C. § 106 (Supp. 2000). Jane Ginsburg argues that the DMCA creates an "access" right as an integral part of the copyright bundle. *See* Jane C. Ginsburg, *From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law*, *in* U.S. INTELLECTUAL PROPERTY: LAW AND POLICY 3 (Hugh Hanson ed., 2000).

20. 17 U.S.C. § 1201(a)(1)(A) (Supp. 2000).

vices designed to circumvent TPSs protecting copyrighted material;[21] and third, the manufacture or distribution of devices for circumventing TPSs protecting any exclusive right in copyrighted material.[22]

Congress recognized, however, that the indiscriminate legal reinforcement of TPSs favored digital media producers over users and therefore potentially threatened otherwise permissible access to—and traditional fair use of—copyrighted materials for valuable endeavors like education.[23] Congress, sensing that it was shifting the balance of intellectual property law too far toward copyright owners,[24] added a complex set of

---

21. *Id.* at § 1201(a)(2). The section provides in full:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

Id.

22. *Id.* at § 1201(b). This paragraph prevents the production of devices that would allow users who have lawfully acquired a work from making unauthorized access for uses inconsistent with the exclusive rights of the owner under copyright law.

23. *See* H.R. REP. NO. 105-551, pt. 2, at 36 (1998). *See also* 144 CONG. REC. S11887 (daily ed. Oct. 8, 1998) (statement of Sen. Ashcroft).

24. Exactly what the legislature intended regarding the balance is difficult to discern. Congress spoke with great reverence for fair use:

> The principle of fair use involves a balancing process, whereby the exclusive interests of copyright owners are balanced against the competing interests of users of information. This balance is deeply embedded in the long history of copyright law. . . . [C]opyright law for centuries has sought to ensure that authors reap the rewards of their efforts and, at the same time, advance human knowledge through education and access to society's storehouse of knowledge. . . . This critical balance is now embodied in [the author's exclusive rights] and in Section 107, which codifies the fair use doctrine. . . . Fair use, thus, provides the basis for many of the most important day-to-day activities in libraries, as well as in scholarship and education. It also is critical to advancing the personal interests of consumers. Moreover . . . it is no less vital to American industries.

H.R. REP. NO. 105-551, pt. 2, at 25-26 (1998).

exceptions to the general ban on circumvention. Good intentions aside, the exceptions that Congress included in the DMCA are not adequate safeguards to protect fair use and the public domain should the specter of reduced access and availability materialize.[25] In fact, since the DMCA, as currently interpreted by courts and the Register of Copyrights, will reinforce even overly restrictive TPSs, it seems that the final legislative product itself welcomed this threatening apparition. If technology develops so that decreased access and availability of digital media becomes the reality—if, as one Senator phrased it, a "pay-per-use" society[26] emerges—the current outlook for users is dim. The DMCA reinforces TPSs without a serious inquiry into their restriction of the public domain and fair use.

This Comment offers some first steps towards ensuring that the legal system preserves fair use and the public domain in the face of the current legal landscape. Part II of this Comment therefore discusses TPSs and how they implicate constitutional media use rights. In Part III, this Comment considers whether the DMCA's anti-circumvention regulations impermissibly convey a legal right to enforce technological restrictions on the speech of users. Section IV asserts that overly restrictive TPSs themselves should be subject to judicial regulation. Throughout the analysis, this Comment distinguishes between strong TPSs, which should be promoted and reinforced, and overly restrictive ones, which should not. The latter TPSs will effectively create new, broad proprietary rights in digital information. When this expansion of digital property restricts users' constitutional rights, courts should intervene.

These arguments lead to the Comment's two conclusions. First, courts should hold the DMCA anti-circumvention provisions unconstitutional where they impermissibly restrict usage rights by creating a right to legal reinforcement of TPSs. Second, for similar reasons, courts evaluate and

---

On the other hand, Congress recognized that the digital environment necessitates the modernization of the law, "including the rules that ensure that consumers have a stake in the growth in electronic commerce." *Id*. Thus it seems Congress intended to change or at least have some effect on fair use and the balance of intellectual property. It is clear from the legislative history that both sides of the debate seemed to consider themselves bound to preserve the intellectual property balance. Even the DMCA's proponents believed that it "fully respected and extended into the digital environment the bedrock principle of 'balance' in American intellectual property law for the benefit of both copyright owners and users." *Id.* at 26.

25. Note that a threat arises only where the digital work is available in no real-world form. Fencing off a copy of a book on the Internet that is also available in stores will have little effect on users' rights. *See* Nimmer, *supra* note 18, at 729.

26. 144 CONG. REC. S11887, S11888 (daily ed. Oct. 8, 1998) (statement of Sen. Ashcroft).

regulate TPSs directly on constitutional grounds or indirectly through the copyright misuse doctrine.

II. TECHNOLOGY DRIVING LEGAL LIMITATIONS ON USERS' SPEECH: TPSs' POTENTIAL EFFECT ON FAIR USE AND ENCLOSURE OF THE PUBLIC DOMAIN ON THE INTERNET

Content owners are understandably concerned about theft of their media on the Internet. Accordingly, the most problematic limitation of TPSs from content owners' perspective is their susceptibility to circumvention. The DMCA fills in the technological gap in protection left by imperfect TPSs by creating a right to legal reinforcement. The size of this gap varies dramatically among TPSs and continues to change with new technological developments.

The DMCA, however, protects all current and future TPSs indiscriminately,[27] even though the need for legal reinforcement decreases as digital fences get stronger. This broad-brush approach is least justified where least necessary, and strong TPSs are in the least danger from all but the most intrepid hackers. This is not to say that even strong TPSs warrant no legal backup, because they too can be cracked. But the justifications for the DMCA put forth by the motion picture and musical recording industries, which stem from the idea that technical protection alone is inadequate, are not as compelling where the digital fences are already very secure.[28] Conversely, the potential for strong TPSs to overly restrict users'

---

27. The DMCA does require that the TPS "effectively" protect the copyrighted work, but this is an exceedingly low threshold. The 40-bit encryption system used to protect DVDs was apparently quite easy to break through—so easy that the defendants in *Reimerdes* claimed it did not "effectively control" access to content on DVDs within the meaning of the DMCA. The court rejected this interpretation of the statute. *See* Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 317 (S.D.N.Y. 2000).

28. The copyright industry argued that content will not be provided on the Internet without legal backup and that as a result an important domestic industry will suffer. *See infra* text accompanying notes 165-69; *see also The WIPO Copyright Treaties Implementation Act*, *Hearing on H.R. 2281 Before the Subcomm. on Telecommunications, Trade, and Consumer Protection, House Comm. on Commerce*, 105th Cong. 56 (1998) (statement of Steven J. Metalitz, on behalf of Motion Picture Association of America) (defending provisions as necessary for robust electronic commerce) [hereinafter *Hearing on H.R. 2281*]; *see also id*. at 45 (statement of Hilary B. Rosen, President and CEO, Recording Industry Association of America) (supporting the provision); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 422 n.264 (1999).

rights is very high because so few people will have the technical ability to crack them in order to exercise their rights.

A. Technical Protection Systems

In order to understand what the DMCA protects, and to see why private parties create digital fences, one must first examine TPSs themselves. The development of digital fences and the protection they offer is constantly advancing and, absent legal limitations, it is the extent of the protection TPSs offer that will define the contours of information flow on the Internet.[29] Any evaluation of TPSs, and in turn the DMCA, therefore demands heightened sensitivity to the role of developing technology in shaping our information society.

The current statutory scheme, as courts have interpreted it thus far, confers legal reinforcement indiscriminately on all TPSs. It is therefore conducive to the creation of strong TPSs capable of extensive restrictions on content use. The DMCA's indiscriminate protection may stem in part from a clouded view of TPS technology.[30] TPSs may be helpful to copyright holders, but they are not a panacea. The fear of piracy, however, has given TPSs an unwarranted rosy tint. As such, the law must make a more

---

29. As Lawrence Lessig has pointed out, the belief—the "is-ism," as he puts it—that the Internet will always be a free forum for the exchange of information is not necessarily true. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 24 (1999). The technological architecture of the Internet, in which TPSs will play a role, will define the boundaries of information access online. If all information is available only on a pay-per-use basis, then users and exchangers of information will construct new boundaries.

30. The *Reimerdes* court, for example, blithely suggests in a footnote that "[i]t is conceivable that technology eventually will provide means of limiting access only to copyrighted materials and only for uses that would infringe the rights of the copyright holder. . . . We have not yet come so far." 111 F. Supp. at 330 n.206. Assuming this is actually conceivable, it is extraordinarily improbable. Relying on content owners alone to limit the scope of their exploitation of the cyberspace market to what is allowed under copyright laws seems naïve. Furthermore, it is highly unlikely that TPSs will ever be advanced enough to account for all non-infringing uses of protected material. The technical capacity of TPSs to allow for fair use would at best extend to uses that are always or nearly always fair. *Cf.* Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH L.J. 137, 152-53, 155-56 (1998). Fair use requires a complex case-by-case statutory analysis that computers cannot perform unless they develop human judgment abilities. For a possible solution to this problem, see Dan L. Burk and Julie E. Cohen, *Fair Use Infrastructure for Copyright Management Systems* (Georgetown Public Law Research Paper No. 239731, 2000), *available at* http://papers.ssrn.com/paper.taf?abstract_id=239731.

careful distinction between the abilities of different TPSs to prevent illegal use (their strength) and to prevent unauthorized use (their restrictiveness).

The first TPS—one that underlies many others—is encryption.[31] Cryptography can serve as both a means of maintaining protection, by keeping content secure, and as a means of identification, by certifying digital identities.[32] Relying on encryption alone, however, is dangerous because hackers can attack it at many levels. If someone breaks the code, the protected content becomes freely available. Perhaps most importantly, encryption provides no control over how one uses the media once it becomes accessible. Given that encryption is a relatively weak means of protection, the legal safety net created by the DMCA may be necessary for copyright holders who rely exclusively upon it.[33] Conversely, any technological threat posed to users' interests by encryption is somewhat minor.

It is for precisely these reasons that one rarely uses this technique alone; encryption often plays a role in more complex services whose larger goal is to control access.[34] Access control systems attempt to track the identity of the user, what content she accesses, and how she uses that content.[35] Even with access control in place, the consumer may still legally

---

31. This involves scrambling digital content so that it is unreadable until unscrambled with a key. *See* DIGITAL DILEMMA, *supra* note 1, at 155. A simple form of this technique, "symmetric-key" encryption, uses the same key to scramble and unscramble the content. *Id.* at 156. The danger here is that if the key, which must be used to decrypt the content, is intercepted, then the protection service fails. "Public-key" encryption, a more complicated service, uses two keys for each user, one of which is kept secret and the other of which is publicly available in a directory. *Id.* at 157; *see also* R.L. Rivest, A. Shamir and L.M. Adelman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 COMM. OF THE ACM 120-26 (1978). To send a message to a user, one encrypts it in his public key. It can then only be opened with his privately held key. Conversely, to send a message *as* a user, one encrypts it in his own private key. Decryption with one's public key proves that the proper user sent the message.

32. *See* LESSIG, *supra* note 29, at 36.

33. *Cf. Reimerdes*, 111 F. Supp. 2d at 294 (finding that, but for the prohibition of circumvention in the DMCA, the movie studios would presumably have had to develop another stronger TPS to protect the content on their DVDs once the first code was broken).

34. *See* LESSIG, *supra* note 29, at 40-42.

35. *See* DIGITAL DILEMMA, *supra* note 1, at 158. These occasionally have involved the use of a computer language to represent the conditions attached to the use of the digital media. *See id.* at 159; *see also* Arun Ramanujapuram and Prasad Ram, *Digital Content and Intellectual Property Rights*, 23 DR. DOBB'S J., Dec. 1998, at 20-27. Effective access control on an open network like the Internet has been difficult because unlike smaller communities where the users are all known, the millions on the Net cannot be

purchase and decrypt the media, and then pass it on to others without authorization. Further, one needs only small gaps in protection to capture the media. Such imperfections make these relatively weak TPSs and provide a good justification for legal protection. However, there are other techniques involving watermarking the media itself that make gaps in digital media protection even smaller.[36] So-called "web crawlers"—programs that methodically search the Net looking for unauthorized documents traceable by watermarks[37]—are in development and will soon be widely available.[38] Where content owners can use web crawlers, tracking infringement of copyrights on the Internet will prove easier than in the real world.[39] This

---

presumed to adhere to the conditions of use. *See* DIGITAL DILEMMA, *supra* note 1, at 160. Some techniques currently used involve posting documents in ways easily viewed but not easily captured from web browsers, or providing specially designed browser plug-ins without which the media cannot be accessed. *See id.* Other means focus on anchoring the digital media to something physical, such as encoding the identity of the user or a particular computer in the decryption key itself, making it possible to subsequently identify the person who has done the decoding from the media. *See id.* at 161.

36. A simple version of this method involves placing a copyright or authorized usage notice on the content. DIGITAL DILEMMA, *supra* note 1, at 165. This may at least deter users whose natural inclination is to make only legal (or "authorized") use of media from illicit behavior. A less frequently used but more subtle approach, targeted at maintaining the authenticity of digital documents, archives digital documents and affixes an authoritative, encrypted time-date stamp and content signature. *Id.*; *see also, e.g.,* Surety Inc., *Welcome to Surety*, *at* http://www.surety.com (last visited Sept. 1, 2001) (introducing Surety's patented service to authenticate digital documents and records); WebArmor, *WebArmor FAQ*, *at* http://www.webarmor.com/misc/faq.html (last visited Sept. 1, 2001) (discussing WebArmor's similar technology). A third, more common approach is steganography, the use of digital watermarks. Bits of information can be changed in digital media to contain usage rights information, author identity, and even information about the user who decrypted a digital file. The data can be readable by the user or can be imperceptible. Steganography does not directly prevent unauthorized use, but it is particularly useful for Internet monitoring schemes. For a sample and evaluation of several currently available PC programs that can embed information within JPEG images, see Neil Johnson, *History and Steganography*, *at* http://www.jjtc.com/stegdoc/sec202.html (last visited Sept. 1, 2001).

37. *See* DIGITAL DILEMMA, *supra* note 1, at 167.

38. Microsoft has developed an "aggressive Internet monitoring program" that has been implemented by the Association of American Publishers (AAP). This "intelligent . . . tool searches for pirated eBook content twenty-four hours a day, seven days a week." Association of American Publishers and Microsoft Corp., *Protecting Against ePublishing Piracy*, *at* http://www.microsoft.com/piracy/epub/enforcement.asp (last visited Sept. 1, 2000). The program is also designed to seek out "unauthorized distribution of information or programs that help to break security technologies." *Id.*

39. Web-crawlers can be countered, though, by password protection of web sites. Infringements in the body of or attached to e-mails will also be immune. Nevertheless,

technology, therefore, further reduces the gap in technical protection targeted by the DMCA, and increases companies' capability to effectively restrict users' rights.

Finally, the most developed and controversial form of access control is "trusted systems."[40] Though they are not yet used widely by content owners,[41] "trusted systems" offer a vision of where TPSs may be headed. The strength of protection and use control they offer make them appealing to content owners. They involve hardware, software, or a combination of both, and can be quite difficult to crack.

"Trusted" means the system will not allow any unauthorized action. In open-ended systems (e.g., programmable devices like home computers), designers use cryptography to authenticate each end user's system as trusted,[42] and the transaction will take place only when the system's identity is verified.[43] The systems also understand digital rights language—software code that allows price discrimination in digital billing.[44] Content owners can use digital rights language to configure the system so that each type of use costs a certain amount for a certain user.[45] Therefore, it is pos-

---

they will still have a significant effect on the ability to publish allegedly infringing materials on public web sites.

40. *See generally* Stefik, *supra* note 30.

41. Even if consumers are willing, there are still strong market and technological barriers to the trusted systems vision. Currently systems in development are proprietary and incompatible. *Id.* at 157. They are extremely expensive to design and manufacture, and they face a barrier to entry in a market where one operating system, Windows, exercises tremendous market power. *See* United States v. Microsoft, 87 F. Supp. 2d 30 (D.D.C. 1999); DIGITAL DILEMMA, *supra* note 1, at 168. The need for specialized hardware could make entry into the established PC market quite difficult, but the recently formed Trusted Computing Platform Alliance may change that need. The Alliance, whose 145 members include Microsoft, Intel, Hewlett-Packard, Compaq, and IBM, has developed a general purpose trusted subsystem targeted at the PC. Version 1.0 of the system's specification became available in early 2001. *See* Press Release, Trusted Computer Platform Alliance, Trusted Computing Platform Alliance Announces v.1.0 Specifications for Trusted Computing (Jan. 30, 2001), *available at* http://www.trustedpc.org/press/pdf/TCPA%20Final.pdf (last visited Sept. 1, 2001). The emergence of industry groups like the Alliance indicates that the trusted systems regime is coming.

42. Closed systems, like the DVD player, present fewer authentication problems, since the licensed system must merely be compatible with the licensed media it plays. They rely on symmetric-key cryptography. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317-18 (S.D.N.Y. 2000).

43. *See* Stefik, *supra* note 30, at 139-40.

44. *Id.* at 140.

45. *See id.* at 141.

sible for a work to have different versions of the same kind of right, each with different fees and conditions.[46]

In addition to offering price discrimination capabilities, trusted systems can track the number of existing copies of digital media, where they are located, and how they are being used.[47] Combined with web crawlers, one could conceivably use trusted systems to electronically cut off access to works on users' systems that the web crawler has detected on the Internet in unauthorized form. Because their protections are extensive and reliable, trusted systems need the least legal backup, and provide the greatest ability to limit and control information use. The DMCA, however, affords them the same protection as weak forms of encryption.

It is difficult, if not impossible, to predict where computer code will lead the protection of digital media on the Internet. As a result, it is difficult to determine the appropriate legal protections. Nevertheless, the information presented in this Comment should be particularly useful in illustrating the systems currently protected by the DMCA and helping to illuminate what will likely be protected in the future.

The need for a legal safety net decreases as technical protections get stronger. Additionally, the strength of copyright owners' claims that digital media cannot be safeguarded on the Internet is not equally compelling for all TPSs.[48] The ability of strong TPSs to prevent illegal uses is an undisputed benefit. But with strength comes a threat: the potential risks of

---

46. Perhaps most interestingly, trusted systems allow a technically sound method for *transfer* of a work—that is, the media effectively becomes unusable on the sender's system when received and used by the receiver's system. Because the original becomes unusable on the sender's system, there is no additional copy created. *See id.* at 145-46; *see also* Mark Stefik and Alex Silverman, *The Bit and the Pendulum: Balancing the Interests of Stakeholders in Digital Publishing*, 16 COMPUTER LAW. 1, 7 (1997). A technical ability to transfer works between users in this manner might ease some of the content industry's concern that copies will proliferate on the Internet without payment and authorization. Unfortunately, the creation of this capability requires the use of trusted systems, which allows for tracking and requiring payment for any type of use at all. Though a transfer right may be developed, it would most likely not lead content owners to ignore the other pay-per-use capabilities of trusted systems. Its possibility, therefore, does lessen the importance of legal scrutiny of the scope of TPSs, particularly ones as strong as trusted systems.

47. For example, digital billing systems keep track of what works a user has and how many times she has printed them. Each user has a software- or hardware-encoded identity necessary for authentication with the trusted system, making the location of the works known, as well. Stefik, *supra* note 30, at 141-42.

48. *See infra* Part IV.A.

extensive—and unconstitutional—use restrictions become more of a possibility than previously seen. Where users face the greatest limitations on their uses, TPSs and the DMCA anti-circumvention provisions become particularly problematic.

B. The Benefits and Drawbacks of TPSs

TPSs can be beneficial for content owners, and even for users. Foremost, TPSs prevent—or at least to some extent control—the illegal and unauthorized use of digital media. This in turn allows creators to exact payment for access to their content, thereby increasing their incentive to create works and put them on the Internet.[49] After all, creation takes work and requires resources; owners may fairly expect some remuneration. Moreover, a lower risk of media theft should lower the price at which creators can offer media to the public. TPSs also stand to increase efficiency in information access and distribution dramatically. With TPSs, the Internet has the potential to be an extremely efficient network that allows users to access larger amounts of better organized, authenticated data than they ever could offline.[50]

Not only might the Internet contain more data, it may also be cheaper to access. TPSs, like trusted systems, allow for price discrimination in media access. Content owners can charge more for a right to print than merely a right to download; users, in turn, can pay less for media of which they wish to make fewer uses. This may increase the breadth of media available to a given user with a fixed budget. Even if TPSs allow a content owner to charge a fee to obtain information over the Internet that would not require payment in the real world, it is wrong to assume that digital information will always cost more with TPSs.[51] This is true because transactions in real-world media, even those that do not require the user to pay a fee to the owner, are not costless. Thumbing through magazines requires going to the store. Getting information in a library requires travel and sometimes a laborious search in a card catalog.[52] Photocopying a book requires time, a photocopier, paper, and ink. Notwithstanding users' unfamiliarity and difficulties with the technology, the Internet drastically reduces these transaction costs.

---

49. Note, though, that an increased benefit conferred upon creators does not have an established relationship with increased creative production.

50. *See* Bell, *supra* note 15, at 581.

51. *See id.*

52. *See id.* at 580.

TPSs also increase certainty in both bilateral contracts and unilateral actions. Authentication is, of course, crucial to almost any utilization of information; for example, users will be able to know who the author of the piece is, and whether it has been modified by anyone since its digital publication.[53] Identification of users,[54] on the other hand, can help content owners regulate uses and engage in price discrimination because they know who will be using their media and how.[55] Digital rights languages could be used to make transaction negotiations easier, thereby empowering users by allowing individualized bargaining.[56] Furthermore, enumeration of authorized uses eliminates uncertainty on the part of both parties to the transaction; valuation of media becomes easier.[57] This is also true for unilateral actions by users; in tangible media, persons looking to reuse protected works must evaluate the risk of infringement or consult fair use experts.[58] TPSs, in contrast, allow the owner of the media to be contacted with relative ease.

Some aspects of TPSs redound primarily to the benefit of content owners. For instance, technological fences provide a two-fold boon by making unauthorized uses easier to track down and punish, which consequently deters those uses.[59] Microsoft's web crawler, for example, seeks out eBook piracy and programs designed to circumvent TPSs twenty-four

---

53. *See* DIGITAL DILEMMA, *supra* note 1, at 154. Identification of authors and authentication of works can also serve moral rights goals, including attribution and integrity. *See also* Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 J. LEGAL STUD. 393, 405 (1999).

54. Identification of users raises several privacy issues that are beyond the scope of this paper. Beneficial identification is used to mean the minimum required to conduct an online transaction. For an excellent discussion of this issue, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998).

55. *See* Stefik, *supra* note 30, at 141-43; *see also* Stefik and Silverman, *supra* note 46, at 7.

56. *See* Stefik and Silverman, *supra* note 46, at 8; *but see* Niva Elkin-Koren, *Copyrights in Cyberspace—Rights Without Laws*, 73 CHI.-KENT L. REV. 1155, 1180-81 (1998) (arguing that terms of mass-market digital contracts, even though they theoretically allow for individualized bargaining and consent, reflect only market power in practice).

57. *See* Stefik and Silverman, *supra* note 46, at 8.

58. *See* Bell, *supra* note 15, at 587.

59. *But see* Tom R. Tyler, *Compliance with Intellectual Property Laws: A Psychological Perspective*, 29 N.Y.U. J. INT'L L. & POL. 219, 224 (1997) (arguing that the deterrent function, particularly in the context of intellectual property, has almost no effect on behavior).

hours a day.[60] Knowledge of potentially constant observation is a significant deterrent to unauthorized activity. Less ominously, however, TPSs may simply serve to keep honest people honest.[61] They may have an effect on public mores in two ways: first, fences, digital or chain-link, make people aware that entry is not allowed; second, since TPSs might make a good deal of media cheaply and easily available, most people will probably prefer to buy it than steal it.[62] Finally, technological protections will eventually be able to prevent all uses content owners find objectionable. With the advent of trusted systems, a content owner who detects an unauthorized use by a web crawler could engage in electronic self-help and unilaterally remove all usage rights from the user's computer.[63] Content owners could even automate the process, suspending usage rights until the user defends her actions to the content owner.

The above examples imply, however, that some of the benefits enjoyed by content owners will come at the expense of users' interests. On a basic level, these result from the transfer of control over use of the content from the user to the distributor. TPSs allow content owners to restrict access in ways not possible in the physical world.[64] Price discrimination, for example, may allow a broader group of users to access works in some ways, but it may make some uses so expensive as to become effectively unavailable.

In addition, electronic self-help repossession and "regulation of performance" can sharply intrude into users' spatial privacy rights and restrict their autonomy.[65] Software applications are a good example; disablement of a program crucial to a user's business can cause catastrophic losses.[66] TPSs also rely upon real-world notions of property that might, from a user's perspective, best be left behind in the move to the digital environment. The attempt to categorize intangible media as real-world products may deny consumers the benefits innovative business models would cre-

---

60. *See supra*, note 46 and accompanying text.

61. *Cf.* Litman, *Copyright Noncompliance, supra* note 8, at 239.

62. *See* Dam, *supra* note 53, at 409-10.

63. *See* Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L. J. 1089, 1106 (1998). Julie Cohen offers a colorful analogy for future digital self-help capabilities: "Imagine, for example, that a team of high-tech repo men [could use] a transporter device to 'beam' your sofa out of your living room and back to the furniture store." *Id.*

64. *See* DIGITAL DILEMMA, *supra* note 1, at 104.

65. Cohen, *supra* note 63, at 1108.

66. Courts, accordingly, have uniformly required contractual notice in self-help repossession of computer software. *See id.* at 1112 n.81 (collecting cases).

ate.[67] Finally, TPSs facilitate a license-based business model rather than a real-world sale model—a change that potentially allows greater restriction of usage rights.

The greatest threat posed to users by TPSs, however, is the overprotection of creative and informational digital media through use restrictions. Real-world media is protected primarily by the Copyright Act, which strikes a delicate, constitutional balance between the interests of creators and the interests of users of media.[68] Copyright law, through the fair use doctrine and various exceptions to the exclusive rights it affords, allows some reuse of expression in an otherwise protected work.[69] TPSs, however, do not recognize the fair use doctrine or these exceptions.[70] When the copyright term expires, for example, the work falls into the public domain and becomes freely usable.[71] TPSs do not have to expire. Similarly, copyright does not protect facts, ideas, or functional principles; it instead commits them to the public domain and preempts state laws that would do otherwise.[72] TPSs, on the other hand, can potentially protect any use on the Internet of copyrighted works, uncopyrightable works, or works that have fallen into the public domain.

From the perspective of users, this is bad news. The advent of strong TPSs can greatly restrict the uses and access currently available in the real world and on the Internet. Further, the DMCA reinforces any technical

---

67. *See* DIGITAL DILEMMA, *supra* note 1, at 177. Some alternative business models include: giving away the information product to sell an auxiliary product or service, giving away the initial product and selling upgrades, giving away media that complements a real-world product, custom-tailoring for individual users such that no other user would want the product, providing the product for free but charging for software that increases usability, giving away one digital product that creates a market for another, or allowing free distribution but requesting payment. *See id.* at 181-82.

68. The balance derives from the Intellectual Property clause itself: "The Congress shall have the Power To . . . promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. CONST. art. I, § 8, cl. 8.

69. 17 U.S.C. §§ 107, 109-112, 117 (Supp. 2000) (detailing fair use and limitations on exclusive rights).

70. The first sale doctrine, *id* at § 109(c), implicates TPSs only in the sense that they help facilitate the paradigm shift from sale to license on the Internet. The exception applies only to owners of copies of copyrighted works, so licensees do not enjoy its benefits. A real-world example is software purchases; since they are technically shrinkwrap licenses, purchasers are not owners and therefore are not protected by section 109(c).

71. *Id.*at §§ 302-305.

72. *Id.* at § 301; H.R. REP. NO. 94-1476, at 129-133 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, *129-33.

protection that effectively protects a work with some copyrighted element, but does not limit liability to circumvention aimed to infringe a valid copyright. This means that TPS users can bootstrap unprotectible material, or material that receives a "thin" copyright,[73] onto a fully enforceable legal right to prevent access. The capability to enclose the public domain and restrict fair use by employing advanced TPSs—reinforced by the DMCA—is unprecedented in intellectual property law.

C. Constitutional Information Use Rights

Copyright law, previously the sole legal protection for creative and informational works, grants only limited rights.[74] Congress's power to create the right derives from Article I, Section 8, Clause 8 of the Constitution (the "Intellectual Property Clause"). The Intellectual Property Clause provides that Congress shall have Power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries . . . ."[75] The statutory monopoly must, under the Constitution, be designed to further this "Progress." Courts consequently have excluded aspects of works crucial for future creation, e.g., ideas,[76] methods,[77] facts,[78] utilitarian objects,[79] titles,[80] plots,[81] and style,[82] from this monopoly.[83] These building blocks lay the subconscious foundation for communicative proc-

---

73. Thin copyright works consist primarily of public domain matter unprotected by copyright, but incorporate some copyrightable element that confers some protection to the work as a whole. Databases, for example, may be protected by virtue of the selection and arrangement of unprotectible material. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,566 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201).

74. 17 U.S.C. § 107 (Supp. 2000); *see also id.* at §§ 109-112, 117.

75. U.S. CONST. art. I, § 8, cl. 8.

76. *See* Baker v. Selden, 101 U.S. 99 (1879).

77. *See* Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807 (1st Cir. 1995), *aff'd by an equally divided court*, 516 U.S. 233 (1996).

78. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv., 499 U.S. 340 (1991).

79. *See* Mazer v. Stein, 347 U.S. 201 (1954).

80. *See, e.g.*, Weissman v. Radio Corp of Am., 80 F. Supp. 612 (S.D.N.Y. 1948); Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965, 993 n.169 (1990).

81. *See* Nichols v. Universal Pictures Corp., 45 F.2d 119 (2d Cir. 1930).

82. *See, e.g.*, Franklin Mint Corp. v. Nat'l Wildlife Art Exch., 575 F.2d 62 (3d Cir. 1978), *cert. denied,* 439 U.S. 880 (1978); Litman, *supra* note 80, at 993 n.175.

83. Litman, *supra* note 80, at 1016.

esses; they make up the experience of the speaker and are inextricably tied to the thought processes involved in the production of speech.[84]

Despite this tailoring of the copyright monopoly to maximize production of new works, courts have been loath to give any explicit content to the term "Progress." Nevertheless, constitutional principles other than those present in the Intellectual Property Clause have guided the courts in drawing the boundaries of copyright law. For example, the First Amendment has played an important, but mostly implicit role in carving out areas of the monopoly. As the DMCA places fair use and the public domain in jeopardy, identifying the constitutional core of these doctrines becomes imperative. A better understanding of the interaction between the Intellectual Property Clause and the First Amendment is therefore necessary in any constitutional analysis of intellectual property rights.

1. Copyright and the First Amendment

Creation of new works is of course expression and therefore implicates the First Amendment.[85] Copyright law silences an infringer's speech through legislative mandate by compelling courts to intervene to suppress a work that infringes any of the statutory rights of the author.[86] Accordingly, even though the First Amendment does not explicitly override copyright law,[87] the legislature and the judiciary have designed limitations on

---

84. *See id.* at 1010-11.

85. Julie Cohen has articulated a compelling argument that there is a First Amendment "right to read anonymously" implicated by the development of TPSs. Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996). Her argument flows partly from the blurred boundary between speaking and reading in cyberspace, since reading is an active, constructive process on the web. *Id.* at 1005-06. In this sense, it is similar to the argument presented here. A major part of her analysis, however, relies on the chilling effect on speech created by the disclosure of reading preferences and on freedom of association. *Id.* at 1003-19. The ultimate target of her paper is the ability of TPSs to disclose information about consumers' content choice and uses. *Id.* at 981-82. Although this is clearly an important point, it is somewhat tangential to the argument the Comment makes here—that TPSs, and the DMCA's reinforcement of them, may impermissibly limit fair use and the public domain.

86. Benkler, *supra* note 28, at 393. Benkler also notes that the important copyright scholars of the 1970s, Melville Nimmer, Paul Goldstein, and Robert Denicola, all understood the scope of the public domain to raise constitutional questions under the First Amendment. *Id.* at 390.

87. *See* Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985) (declining to create a fair use defense to infringement of subject matter that holds great public interest).

authors' rights: "copyright laws are not restrictions on freedom of speech . . . copyright protects only form[s] of expression and not the ideas expressed."[88]

The Supreme Court's most extensive foray into the conflict between the First Amendment and copyright law came in the *Nation* case, which involved the unauthorized publication of quotes from President Ford's memoirs.[89] Defendants argued that the First Amendment permitted this publication as a fair use because the story was in the public interest. The Court declined to create such an exception, however, noting that:

> It should not be forgotten that the Framers intended copyright itself to be the engine of free expression. . . . The [basis of the Intellectual Property Clause] is the conviction that encouragement of individual effort by personal gain is the best way to advance public welfare through the talents of authors and inventors in "Science and useful Arts."[90]

Deeming this particular use fair did not, in the Court's judgment, promote "Progress" because it would decrease incentives to create the very works the public wants.[91] This was a sufficient basis from which the Court could dispose of the case, so it did not have to specify explicitly how copyright law satisfies First Amendment requirements.

Nevertheless, the Court identified and addressed, however briefly, a possible vehicle for intratextual interaction between the First Amendment and the Intellectual Property Clause: the word "Progress."[92] This interac-

---

88. *Id.* at 556 (citing New York Times Co. v. United States, 403 U.S. 713, 726 (1971) (Brennan, J., concurring)).

89. *Id.*

90. *Id*. at 558 (internal citation omitted). How the Court divined such an intent for the Framers is unclear. The ratification debates in the Federal Convention offer no guidance in the few places the Copyright Clause is even mentioned. *See* 5 JONATHAN ELLIOT, DEBATES ON THE ADOPTION OF THE FEDERAL CONSTITUTION 440, 511, 561 (William S. Hein 1996) (1891). Madison's comments in the Federalist were only slightly more enlightening:

> The utility of this power will scarcely be questioned. The copyright of authors has been solemnly adjudged in Great Britain, to be a right of common law. The right to useful invention seems with equal reason to belong to the inventors. The public good fully coincides in both cases with the claims of individuals.

THE FEDERALIST NO. 43 (James Madison).

91. *Nation*, 471 U.S. at 557.

92. "Intratextualism" has recently been postulated as a way of reading the Constitution by analyzing words and phrases as they appear in one part in light of how those

tion has two layers. The first is that the First Amendment is itself an explicit limitation on Congress's power to pass laws abridging the freedom of speech. Copyright, in tension with this limitation, gives authors an enforceable right to restrict others' expression. This interaction is not very helpful though; under this argument, only in the extreme case of an unlimited copyright can one say confidently that the First Amendment would be a bar to statutory speech restrictions. Statutory copyright has never been perpetual,[93] and even the new rights under the DMCA are not unlimited. The second layer of the interaction is more interesting: the First Amendment itself may help define "Progress." Unfortunately, the text of the amendment defies clause-bound interpretation,[94] and originalist arguments are generally unavailing since the text is singularly unhelpful and evidence of intent is scant.[95] The principles underlying First Amendment law, however, offer guidance as to what "Progress" means (and also what it does not mean).

Although there are several understandings of the First Amendment, the one that has had the most influence in shaping the American doctrine relies on democratic theory, which has two formulations.[96] First, the act of speaking is necessary for the participation in public discourse by which

---

same or similar words appear in another part. *See* Akhil Reed Amar, *Intratextualism*, 112 HARV. L. REV. 747 (1999). The Copyright Clause and First Amendment offer little in terms of linguistic parallels. This analysis derives more from John Hart Ely's treatment of Constitutional clauses which "cannot intelligibly be given content solely on the basis of their language and surrounding legislative history . . . certain of [which] seem on their face to call for an injection of content from some source beyond the provision." JOHN HART ELY, DEMOCRACY AND DISTRUST 12 (1980).

93. American courts first had occasion to interpret the "limited Times" language of the Intellectual Property Clause with regard to copyright when the first Copyright Act was passed in 1790. Act of May 31, 1790, ch. 15, 1 Stat. 124 (repealed 1834). Common law copyright then existed in perpetuity, which was deemed inconsistent with the text of the Constitution. The Supreme Court therefore held that all literary rights previously held in works but not expressed in the 1790 Act passed into the public domain upon vesting of federal statutory copyright. *See* Wheaton v. Peters, 33 U.S. (8 Pet.) 220 (1834); Howard B. Abrams, *The Historic Foundation of American Copyright Law: Exploding the Myth of Common Law Copyright*, 29 WAYNE L. REV. 1119 (1983); Litman, *supra* note 80, at 978.

94. ELY, *supra* note 92, at 13.

95. Originalist arguments are uncommon in First Amendment jurisprudence. *See, e.g.,* 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 517 (Scalia, J., concurring) (suggesting the parties and amici should have offered evidence as to the state legislative practices regarding commercial speech at the time the First and Fourteenth Amendments were adopted).

96. Robert Post, Lectures in Constitutional Law III, University of California, Berkeley, Boalt Hall (Spring 2001) (on file with author).

individuals mediate their interaction with collective government.[97] This is the participatory theory, or the public discourse model.[98] Second, speech is necessary to give individuals all the information they need to be autonomous in public decisionmaking.[99] This is the audience-centered theory.[100]

The former rationale has been dominant, ultimately finding expression in *New York Times Co. v. Sullivan*.[101] In *New York Times*, the Supreme Court held that speech could not be regulated without regard to the underlying value of the speech, as it previously had been in common-law libel. Criticism of public officials is crucial to the purpose of speech under this formulation of the democratic theory, as a vehicle to bring about political change. The fundamental value of political speech in our society therefore trumps public officials' privacy interests.

This participatory democratic theory shows some of what the word "Progress" does *not* mean. It cannot mean the furtherance of a certain set of community norms, like privacy, dignity, and protection from offense, at the expense of others.[102] Copyright cannot, for example, allow an author of a book to "maintain a monopoly of sentiment and opinion respecting it."[103] Nor can it allow Howard Hughes to purchase a series of articles written about him in order to ensure, through suits for copyright infringe-

---

97. *Id.*
98. *Id.*
99. *Id.*
100. *Id.*
101. 376 U.S. 254 (1964).
102. Robert Post notes:

> The specific 'outrageousness' standard at issue in [*Hustler Magazine v.*] *Falwell*, [485 U.S. 46 (1988),] for example, can have meaning only within the commonly accepted norms of a particular community. . . . [T]he constitutional concept of public discourse forbids the state from enforcing such a standard within the 'world of debate about public affairs,' because to do so would privilege a specific community and prejudice the ability of individuals to persuade others of the need to change it. . . . [A]n 'outrageousness' standard is unacceptable . . . because it would enable a single community to use the authority of the state to confine speech within its own notions of propriety.

Robert Post, *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and* Hustler Magazine v. Falwell, 103 HARV. L. REV. 603, 631-32 (1990); *see also* Boos v. Barry, 485 U.S. 312 (1988); Cohen v. California, 403 U.S. 15 (1971); Cantwell v. Connecticut, 310 U.S. 296 (1940).

103. Carr v. Hood, 170 Eng. Rep. 985 (K.B. 1808) (Lumbard, J., concurring).

ment, that "nothing was written about [him], the publication of which he could not control."[104] Thus, the First Amendment offers not just a limitation on the scope of the Intellectual Property Clause, as in the unlimited copyright example, but also on the purpose the monopoly may serve.

The second formulation of democratic theory—the audience-centered theory—has played a somewhat less important role in shaping First Amendment doctrine. Alexander Meiklejohn, the leading authority advocating this theory, conceptualizes freedom of speech as a vehicle for political self-government: "the point of ultimate interests is not the words of the speakers, but the minds of the hearers. The final aim is . . .the voting of wise decisions."[105] Courts rely upon this theory primarily in the commercial speech cases, where they seek not to protect the act of speaking, but societies' "interest in the free flow of . . . information."[106]

This audience-centered democratic theory of the First Amendment shows some of what "Progress" *does* mean. Courts should interpret the Intellectual Property Clause with reference to information's central purpose in self-government. Meiklejohn points out that legislation to enlarge and enrich freedom of speech is by no means prohibited by the First Amendment:

> The freedom of mind which befits the members of a self-governing society is not a given and fixed part of human nature. It can be increased and established by learning, by teaching, by the unhindered flow of accurate information . . .by bringing them together in activities of communication and mutual understanding. And the federal legislature is not forbidden to engage in that positive enterprise of cultivating the general intelligence upon which the success of self-government so obviously depends.[107]

---

104. Rosemont Enters., Inc. v. Random House, Inc., 366 F.2d 303, 313 (2d. Cir. 1966) (finding defendant's biography a fair use); Benkler, *supra* note 28, at 388 n.149; Paul Goldstein, *Copyright and The First Amendment,* 70 COLUM. L. REV. 983 (1970) (quoting *Rosemont Enters.*, 366 F.2d at 313);.

105. ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE 26 (1948).

106. *See, e.g.,* Zauderer v. Office of Disciplinary Counsel, 471 U.S. 626, 651 (1984) ("[T]he extension of First Amendment protection to commercial speech is justified principally by the value to consumers of the information such speech provides . . . ."); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 764 (1975) (striking down a state statute prohibiting advertising of prices for prescription drugs).

107. MEIKLEJOHN, *supra* note 105, at 19-20.

Copyright law, bound by its constitutional commitment to "promote the Progress of Science and useful Arts," is, at least vis-à-vis the First Amendment, such legislation. This is likely what the Supreme Court intended when it said in *Nation* that the Framers intended copyright to be the engine of free expression.[108] Copyright promotes the production of creative and informational works by giving incentives to authors to create those works. When James Madison wrote, "[t]he public good fully coincides in [the copyright of authors] with the claims of individuals," the public good to which he referred was likely the furtherance of self-governance.[109]

The Meiklejohnian theory provides a description of what might be considered the primary purpose of copyright and the core definition of "Progress." Although it is difficult to articulate the principle as a positive requirement, it provides a guideline for how Congress may or may not structure copyright law. The law must further the constitutional purpose of "Progress," making legislation aimed at restricting the flow of information impermissible. As the Comment demonstrates below, the fair use doctrine is indispensable, as it provides the only vehicle under copyright law that can ensure that monopoly does not restrict information flow.

2. The (Non) Constitutional Doctrine of Fair Use

Courts have developed the copyright fair use doctrine as a non-constitutional expression of First Amendment principles. No finding of fair use relies on the First Amendment as its source of authority, yet the doctrine is driven to a great extent by the First Amendment's interaction with the Intellectual Property Clause. This is not surprising, since the Constitution seems as good a place as any other to look for foundations of new

---

108. Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985).

109. THE FEDERALIST NO. 43 (James Madison). The Preamble to the Constitution supports this inference:

> We, the People of the United States, in order to form a more perfect Union, establish justice, insure domestic tranquillity, provide for the common defense, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity, do ordain and establish this Constitution of the United States of America.

U.S. CONST. pmbl. The overriding purpose of the document is to establish and maintain a system of self-government. *See* MEIKLEJOHN, supra note 105, at 18 ("All other purposes, whether individual or social can find their legitimate scope and meaning only as they conform to the one basic purpose that the citizens of this nation shall make and shall obey their own laws, shall be at once their own subjects and own masters.").

new legal doctrines.[110] Such nonconstitutional development, however, may lead to at least two problems, the resolution of which demands recognition of the constitutional bases of the fair use doctrine itself.

The first of these problems provokes a conventionalist response: because the doctrine lacks a core theoretical definition, it is difficult for judges to make good decisions on seemingly easy questions.[111] For example, courts have difficulty applying fair use doctrine to unpublished works. The *Nation* opinion observed that the unpublished nature of a work is a "key, though not necessarily determinative factor" in the fair use decision, "tending to negate the defense."[112]

Authors have a legitimate interest in preventing the publication of their works insofar as it decreases the incentive granted under the Intellectual Property Clause to create the works in the first place.[113] But a ban on fair use of unpublished documents, which the Court's language suggests might be acceptable, would limit historians, who wish to quote from the unpublished papers of a deceased public figure, to the whims of that person's heirs, as enforced by a federal court.[114] This cannot be right. Insulation of public figures from criticism is an unacceptable purpose for copyright.[115] The Court seems to have understood this principle in its reasoning; the critical element in *Nation* was that President Ford wrote his memoirs for publication.[116] Thus, the holding balanced the legitimate copyright concern of the author with the ultimate value of the work intended for publication. Nevertheless, subsequent decisions have read the *Nation* decision much more broadly.[117] A more clearly articulated understanding

---

110. Goldstein, *supra* note 104, at 1001.

111. This argument is analogous to David Strauss's conventionalist justification for why text matters in his common law account of constitutional interpretation. There, interpreters, though not bound by the text, do not abandon it because it provides a set of societal ground rules for what is out of bounds to argue. "[N]ot accepting that answer has costs—in time and energy spent on further disputation, in social division, and in the risk of a decision that (from the point of view of any given actor) will be even worse than the constitutional decision." David Strauss, *Common Law Constitutional Interpretation*, 63 U. CHI. L. REV. 877, 907-08 (1996).

112. *Nation*, 471 U.S. at 554 (internal citation omitted).

113. Judge Leval has already identified the disconnect between copyright's goals and the interest in preventing publication except as it relates to maintaining the incentives to create in the first place. He, like courts interpreting fair use, relies implicitly—but strongly—on First Amendment principles. *See* Pierre N. Leval, *Commentary: Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1117-22 (1990).

114. *Id.* at 1118.

115. *See supra* notes, 101-04 and accompanying text.

116. *Nation*, 471 U.S. at 555; *see also* Leval, *supra* note 113, at 1120.

much more broadly.[117] A more clearly articulated understanding of how fair use accommodates First Amendment concerns about copyright would have allowed the Court to provide a proper and easily understood directive to the lower courts.

A second, more serious problem is that nonconstitutional development obscures what is a constitutionally necessary role of the fair use doctrine in the current statutory framework. The question of whether Congress can legislate section 107 fair use out of existence is a difficult one because its constitutional core is largely undefined. An evaluation of the doctrine in light of the constitutional interaction between the Intellectual Property Clause and the First Amendment[118] shows that much of it is constitutionally based, and indeed some of it is constitutionally required.

Fair use consists of four doctrinal factors, the first of which requires the court to examine the purpose and character of the secondary use.[119] The Supreme Court's most coherent articulation of this factor came in the *Campbell* case:

> The central purpose of this investigation is to see. . . whether the new work merely "supersede[s] the objects" of the original creation. . . or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message; it asks, in other words, whether and to what extent the new work is "transformative."[120]

The transformative use inquiry is at the heart of the fair use doctrine. Although a nontransformative use may be considered fair, this occurs only when the plaintiff cannot show any economic harm caused by the use, i.e., when the use does not reduce the incentive to create.[121] Absent those circumstances, a secondary use will only be deemed fair to the extent that the quoted matter is transformed in the creation of "new information, new aesthetics, new insights and understandings."[122]

---

117. *See, e.g.,* New Era Publications Int'l v. Henry Holt & Co., 884 F.2d 659 (2d. Cir. 1989); Salinger v. Random House, Inc., 811 F.2d 90 (2d. Cir. 1987), *cert. denied*, 484 U.S. 890 (1987); Leval, *supra* note 113, at 1117-22.

118. *See supra* Part II.C.1.

119. 17 U.S.C. § 107 (Supp. 2000).

120. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994) (citing Folsom v. Marsh, 9. F. Cas. 342, 348 (C.C.D. Mass. 1841) (No. 4,901) and Leval, *supra* note 113, at 1111).

121. Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 456 (1984).

122. Leval, *supra* note 113, at 1111.

This is entirely consonant with the Meiklejohnian theory of "Progress." He writes:

> If, for example, at a town meeting, twenty like-minded citizens have become a "party," and if one of them has read to the meeting an argument which they have all approved, it would be ludicrously out of order for each of the others to insist on reading it again.[123]

Protection of duplicative information in the town meeting wastes time that should be available for free discussion. A finding of noninfringement for nontransformative use stalls "Progress" because it removes copyright's monetary incentive to create without any addition to the flow of information to the public. Conversely, courts should almost always deem a highly transformative use fair because it increases the flow of valuable nonduplicative information to the public.[124] Thus, the transformative use inquiry should be based in the First Amendment's commitment to maintaining the production and distribution of information necessary for democratic decisionmaking.[125]

---

123. MEIKLEJOHN, *supra* note 105, at 26.

124. This is not the first time that a Meiklejohnian analysis of the interface between copyright and the First Amendment has been suggested. Paul Goldstein's "first accommodative principle," that "copyright infringements must be excused if the subject matter of the infringed material is relevant to the public interest and the appropriator's use of the material independently advances the public interest," reflects in part the Meiklejohnian audience-centered theory. Goldstein, *supra* note 104, at 988-89. In Goldstein's view, fair use's "paramount objective is to broaden public access to expression." *Id.* at 1015. This would call for an evaluation of the original work's public interest value—an inquiry rejected by the Court in *Nation* 15 years after Goldstein's article was published: "It is fundamentally at odds with the scheme of copyright to accord lesser rights in those works that are of greatest importance to the public. Such a notion ignores the major premise of copyright and injures author and public alike." Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 559 (1985). In contrast, this Comment's view of the First Amendment's role of the transformative use inquiry focuses solely on the use itself and whether it can be said to contribute non-duplicative information to the public discourse—that is, not whether it broadens public access to expression, but whether it broadens the expression to which the public has access.

125. However, this is not the whole of the justification for transformative fair use. Meiklejohn himself noted "that the people do need novels and dramas and paintings and poems, 'because they will be called upon to vote.'" MEIKLEJOHN, *supra* note 105, at 263. Thus democratic theory is informed by another First Amendment value—self-expression. Martin H. Redish, *The Value of Free Speech*, 130 U. PENN. L. REV. 591, 607, 627 (1982); s*ee also* Whitney v. California, 274 U.S. 347, 375 (Brandeis, J., concurring) ("Those who won our independence believed that the final end of the State was to make

The second fair use factor, the nature of the copyrighted work, recognizes "a greater need to disseminate factual works than works of fiction or fantasy."[126] Accordingly, if the original work is of the former rather than latter type, a court is more likely to find that the secondary use is fair.[127] This valuation of works is an offshoot of another accommodation between copyright and the First Amendment, the idea/expression distinction, which limits protection to the author's expression, not the underlying ideas or facts.[128]

This interaction is also consistent with the Meiklejohnian theory of the First Amendment; self-government requires that all the facts and ideas are available for public use.[129] It does not matter whether everyone gets to speak, only that "everything worth saying shall be said."[130] Under this theory, courts do not protect expression for its own sake, but rather for the sake of those who hear it. Where it is not clear whether the information presented in the secondary use is duplicative, courts can more easily presume the use to be fair if the primary work is predominantly factual; the secondary work more likely presents information worthy of First Amendment protection. Where the primary work is predominantly fanciful, it is further from the core of information necessary to public decisionmaking. Therefore, a secondary use is less likely to present information of public value. It will accordingly be harder to call it a fair use.

Ultimately though, the second factor is rarely dispositive, and is often of little help in the fair use determination. In fact, it has only proven criti-

---

men free to develop their faculties; and that in its government the deliberative forces should prevail over the arbitrary. They valued liberty both as an end and as a means."). The combination of the two protects any information necessary for the individual's formation of a public persona. The powerful role advertisements play in popular culture and accordingly, people's sense of self, is an example of this phenomenon. And of course advertisements are protected under the commercial speech doctrine without serious inquiry into whether the particular information conveyed is necessary for voting. *Cf.* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 787 (Rehnquist, J., dissenting) (dissenting on grounds that First Amendment protection of information necessary to public decisionmaking does not extend to decisions about which type of shampoo to use). *See also* Goldstein, *supra* note 104, at 989.

126. *Nation*, 471 U.S. at 563.

127. *Id.*

128. *Id.* at 556. The idea/expression dichotomy has been the primary tool of harmonization of copyright and the First Amendment. *See, e.g.,* New York Times, Inc. v. United States, 403 U.S. 713, 726 (Brennan, J., concurring). However, the idea/expression dichotomy is not sufficient. Sometimes the use of someone else's expression is necessary to the exercise of First Amendment rights.

129. MEIKLEJOHN, *supra* note 105, at 26.

130. *Id*.

cal in cases concerning the fair use of unpublished works, as discussed above.[131] And there, the public discourse theory of the First Amendment provides a direct limitation on the purposes of the copyright monopoly.[132]

The third factor, the amount and substantiality of the material taken in relation to the copyrighted work as a whole, is basically a tool to aid in the evaluation of factors one and four.[133] If a work takes more of the original than is necessary to its purpose, a court is less likely to find fair use.[134] Similarly, if a work takes a substantial amount from the original, it is more likely to affect the market for the original.[135]

The fourth factor requires a court to look at this market effect.[136] A use that diminishes the market for a work decreases incentives to produce it; accordingly, courts are less likely to find any use that decreases these incentives to be fair. Notably, unless the use is transformative under the first factor, an effect on the market for the original will almost certainly result in a determination that the use was not fair.[137] If the secondary use merely wastes public resources by contributing nothing new, and does so at the expense of the system that ensures the flow of creative and informational works, it would undermine this entire system to exempt the secondary user from liability. Under the Meiklejohnian metaphor, the citizens at the town meeting would waste their valuable time, time that could instead be devoted to hearing all possible information.[138] Under copyright law, the analogous threatened resource is the incentive structure of the statutory monopoly.

Another crucial aspect of the fourth factor is that certain market effects do not matter. The doctrine distinguishes between a market effect caused by displacement and one that is caused by disparagement.[139] Displacement occurs when a secondary work fills the same niche as the primary work, and thereby diminishes the market for the latter. Disparagement decreases the market for the work by making it less attractive through criticism.

---

131. Leval, *supra* note 113, at 1116-17; Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586 (1994).

132. *See supra* notes 114-15 and accompanying text.

133. Leval, *supra* note 113, at 1122-23.

134. *Id.*

135. *Id.*

136. 17 U.S.C. § 107 (Supp. 2000).

137. Leval, *supra* note 113, at 1116.

138. MEIKLEJOHN, *supra* note 105, at 26.

139. *See, e.g.,* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 591-92 (1994) (citing Fisher v. Dees, 794 F.2d 432, 437-38 (9th Cir. 1986)).

Only displacement counts against the secondary user, but the cases do not explain why.[140] Participatory democratic theory, however, provides an explanation. Published works are part of the public discourse, and therefore must freely be subject to criticism. As discussed earlier in connection with the unpublished memoirs cases, a court could not allow copyright to shield against quotation for the purposes of a critical review under the First Amendment.

In sum, the First Amendment has a twofold relevance to nonconstitutional fair use doctrine. First, it helps explain the purposes of the doctrine's focus on transformative use and the factual/fanciful nature of the original copyrighted work. The Meiklejohnian account of the First Amendment, as it interacts with "Progress" in the Intellectual Property Clause, also explains much of the shape and goals of fair use doctrine. It provides an understanding of what is not a transformative use, and what, therefore, courts should not deem fair. More importantly, it provides a limit on the scope of the copyright monopoly: where the secondary use is highly transformative, a court must deem it fair. To do otherwise would restrict the flow of information. Admittedly, the boundaries of this limitation are hard to define. Nevertheless, it establishes an important constitutional restriction on the scope of the copyright monopoly—one that only the fair use doctrine is capable of enforcing under the current statutory framework.

Second, the dominant public discourse model of the First Amendment requires restrictions on the scope of the copyright monopoly. Copyright law cannot be used to protect privacy or dignity, or to prevent offense to authors.[141] The second and fourth fair use factors accommodate this requirement. The unpublished nature of a work can prevent fair use only to the extent that the work is on its way toward publication, and the secondary use would diminish the copyright incentives to create in the first place. Thus, for example, copyright cannot protect memoirs of a public figure from criticism.[142] Additionally, only certain diminishments of copyright incentives matter in the fair use determination. Fair use allows quotation for the purposes of disparaging a work because published works are part of the public discourse. As with the Meiklejohnian restriction on injunctions against transformative works, the facilitation of criticism of published and unpublished works comes solely through the fair use doctrine.

---

140. *Id.*
141. *See supra* notes 101-04 and accompanying text.
142. Leval, *supra* note 113, at 1122.

As lawmakers restrict fair use, they also restrict the ability to create new works because many works necessarily draw on previous works. Thus, the fair use doctrine is not merely a subsidy to users, but is a constitutionally required element of information regulation and promotion in our society.[143] Conferring greater rights to exclude uses of informational and creative media to authors necessarily limits free speech. Judicial interpretations of the DMCA thus far have not adequately taken this principle into account. Accordingly, lawmakers and courts have poorly served the constitutional mandate of "Progress." As discussed more fully in Part III, the right to sue to enforce the legal protection of TPSs created by the DMCA—at least as courts currently interpret it—is perpetual and fails to maintain users' rights.

D. Enclosure of the Public Domain and Restriction of Information Use Rights by TPSs

Restricting use of public domain materials through TPSs has a similarly deleterious effect on the production of new works. Yochai Benkler has offered a functional analysis of how the enclosure of the public domain threatens free speech.[144] Although he addresses the effect of statutes that fence off the public domain,[145] his analysis is also applicable to the independent effect of fencing by TPSs on the constitutional rights of users.

Benkler shows how enclosure, and information producers' corresponding reliance on the sale of rights to attain profits, affects different types of information outputs differently.[146] The core of the problem is that information producers who use business strategies that do not incorporate the benefits of increased protection will suffer.[147] These producers derive value through alternative means to sale or licensing, such as free distribution of their content to maximize effect on a correlated market (as in the case of the noncommercial development of the Linux operating system) or free exchange of ideas (as in the academic setting).[148] These information

---

143. *See* Benkler, *supra* note 28, at 363 n.33 (collecting articles arguing that the public domain is merely a redistribution of value of copyright to users or a subsidy in favor of uses with public benefits).

144. *See* Benkler, *supra* note 28.

145. The state action doctrine is obviously implicated with regard to TPSs, since the First Amendment is generally thought to apply only to government actions that restrict free speech. See *infra* Part IV.C for further discussion of this problem.

146. *See* Benkler, *supra* note 28, at 400-08.

147. *Id.*

148. *Id.* at 404.

producers must face the increased costs of purchasing rights to information inputs not previously enclosed, without an offsetting increase in benefits.[149] Furthermore, forms of speech valued under statutory fair use—criticism, comment, reporting, teaching, scholarship and research—may suffer the most, since they are less frequently undertaken for monetary gain than other content creation. As the public domain is enclosed, producers of information particularly valued under the Copyright Act, according even to Congress,[150] thus face the largest obstacles to creation of new works.

The result is that the disparate impact felt by these organizations will cause a concentration of information production in large commercial organizations that vertically integrate the sale and management of owned inventory with the creation of new information.[151] In other words, large profit-maximizing companies with vast internal libraries of content at their disposal will increasingly be the ones best able to produce content. Greater limitation of fair use and the public domain with TPSs will not necessarily lead, as some commentators contend, to greater production and dissemination of information.[152] Instead, diversity of content will decrease and large companies will become the locus of production.[153] And as an added detriment to media users, quality may decrease as well, because large content producers relying on a broad audience will produce what will sell the most to the greatest number of people, regardless of quality.[154]

A related effect TPSs may have on the production of new media works is the creation of an "anticommons . . . a property regime in which multiple owners hold effective rights of exclusion in a scarce resource."[155] When too many individuals have rights of exclusion to a scarce resource, rational individuals, acting separately, may collectively underuse the resource.[156] If all authors must seek permission for every use from each of

---

149. *See id.* at 409.

150. "Fair use, thus, provides the basis for many of the most important day-to-day activities in libraries, as well as in scholarship and education. It is also critical to advancing the personal interests of consumers. Moreover . . . it is no less vital to American industries, which lead the world in technological innovation." H.R. REP. NO. 105-551, pt. 2, at 25-26 (1998).

151. *See* Benkler, *supra* note 28, at 410.

152. *Cf.* Bell, *supra* note 15.

153. *See* Benkler, *supra* note 28, at 411.

154. *Id.*

155. Michael Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621, 668 (1998).

156. *Id.* at 677.

their predecessors, fewer new works are likely to appear.[157] Some commentators argue that TPSs will have the opposite effect on the production of new works.[158] It is unclear, however, even where licensing transactions are costless, how allowing protection of media will make using these protected types of media *easier* than in their currently unprotectible state.

TPSs are capable of creating an anticommons because they control access and track similarities between works—even those based on material that the law cannot directly protect. Because the protected media can contain public domain material to which nobody previously had a legal claim under copyright, there will be many overlapping claims. Further, TPSs will make these claims easily detectable and provable. Multiple owners will hold effective rights of exclusion in a scarce resource,[159] creating an anticommons. The public domain building blocks will be underused because of these potential claims, and fewer works will be created. The effect of TPSs and the DMCA on speech is twofold: not only will content owners easily be able to prevent objectionable uses of previously legally unprotectible works by preventing fair use, they will also be able to limit *creation* of future works by enclosing the public domain.

The public domain and fair use are not merely vestigial tails of copyright that exist because of market inefficiency; they are fundamental to information production. The Supreme Court has interpreted its free speech cases to stand for the proposition that "the State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge."[160] The DMCA's invocation of governmental machinery to enforce restrictive TPSs[161] threatens the amount, diversity, and quality of

---

157. *See* Litman, *supra* note 80, at 1019.

158. *See* Bell, *supra* note 15. Bell argues that the efficient usage rights system resulting from TPSs will make it easier for authors to create new works. *See also supra* notes 49-53 and accompanying text.

159. Heller, *supra* note 155, at 668.

160. Griswold v. Conn., 381 U.S. 479, 482-83 (1965) (citing a collection of First Amendment "peripheral rights," without which "the specific rights would be less secure"); Sweezy v. N.H., 354 U.S. 234 (1957) (finding a freedom of the university community)); Wieman v. Updegraff, 344 U.S. 183 (1952) (upholding the freedom to teach); Martin v. City of Struthers, Ohio, 319 U.S. 141 (1943) (finding a right to read); Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925) (upholding a right to educate one's children); Meyer v. Neb., 262 U.S. 390 (1923) (finding a right to study as one chooses).

161. Notwithstanding the state action doctrine, constraint of the public domain and free speech by TPSs alone is analytically identical to constraint by a statute conferring an indiscriminate right to legal reinforcement of them. More narrowly, the fact that TPSs constrain constitutional rights of users does not necessarily mean the statute granting

information production. In doing so, the DMCA contracts the amount of current and future knowledge. Because the public domain and fair use are grounded in the constitutional commitment to free speech, any legal constraint upon them must have more than a merely plausible justification. Claims that reinforcement of TPSs by the DMCA is necessary must be "real, not merely conjectural," and the reinforcement must further these goals in a "direct and material way."[162] As the following section shows, the legislature has not made its case for indiscriminate protection of TPSs.

III. JUSTIFYING RESTRICTIONS ON SPEECH? THE CONSTITUTIONALITY OF BROAD READINGS OF THE DMCA'S ANTI-CIRCUMVENTION PROVISIONS

Given the numerous benefits of TPSs, it was certainly rational for Congress to choose to promote them. Strong TPSs in particular will be quite useful in preventing illicit uses of copyrighted material. The DMCA as currently drawn, however, creates a right to legal reinforcement without regard to potentially serious drawbacks for users.[163] Were these drawbacks simply an inconvenience to users, the statute might be justified on its evaluation of TPSs' desirability in general. Congress's reliance on such a broad generalization to justify the DMCA is insufficient, however, because the legislation impinges upon users' constitutional rights. The new right provided by the DMCA protects even overly restrictive TPSs, and therefore implicates constitutional concerns underlying information use and the public domain. Thus, one may bring a constitutional challenge against the DMCA where the statute compels a court to legally reinforce a TPS that prevents fair use of media a user has lawfully acquired or encloses public domain materials.

The question of whether the DMCA would compel violation of users' constitutional rights turns on judicial and administrative[164] interpretation

---

legal reinforcement constrains equivalently if the statute can be given a limiting interpretation. I turn to the matter of interpreting the DMCA in Part III.B. Part IV.C, which discusses direct judicial regulation of TPSs, addresses the state action question.

162. Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 664 (1994) ("When the Government defends a regulation on speech as a means to redress past harms or prevent anticipated harms, it must do more than simply posit the existence of the disease sought to be cured. It must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way.") (internal citations omitted); *see also* Benkler, *supra* note 28, at 423.

163. *See supra* notes 68-73 and accompanying text.

164. Section 1201(a)(1)(C) requires a rulemaking procedure be undertaken by the Librarian of Congress on the recommendation of the Register of Copyrights two years

of the statute. As the Comment discusses in Parts III.B and III.C, current judicial and administrative interpretations of the DMCA—the anti-circumvention provisions in particular—may lead to violations of users' constitutional rights. Given this potential, the legislature should revisit these provisions.[165] Until the legislature revises these provisions, the courts should hold them unconstitutional.

A. Constitutional Imbalance: Indiscriminate Reinforcement of TPSs vs. Restriction of Users' Rights

Justification for the DMCA stems primarily from the idea that legal protection is necessary to reinforce available technical protection. No technical protection protects fully; therefore TPSs alone cannot provide adequate protection to copyright owners. Three arguments made to Congress by the motion picture and musical recording industries[166] reflect this premise: first, without adequate protection, content will not be made available;[167] second, copyright industries are an important sector of the domestic economy that should be protected;[168] and, third, the DMCA must prohibit circumvention without regard to infringing activity because legal enforcement of copyright is more difficult than using TPSs.[169] These arguments influenced Congress to pass a statute which, if read broadly, pro-

---

after the DMCA's passage and every three years thereafter. 17 U.S.C. § 1201(a)(1)(C) (Supp. 2000). This procedure is designed to identify whether any exceptions to the anti-circumvention provisions are warranted. The first rulemaking was issued on October 27, 2000. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201). This rulemaking is discussed in detail in section III.C.

165. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,556.

166. *See Hearing on H.R. 2281*, *supra* note 28 at 56 (statement of Steven J. Metalitz, on behalf of Motion Picture Association of America) (defending provisions as necessary for robust electronic commerce); *see also id*. at 45 (statement of Hilary B. Rosen, President and CEO, Recording Industry Association of America, supporting the provision); Benkler, *supra* note 28, at 422 n.264.

167. *See Hearing on H.R. 2281*, *supra* note 28, at 36 (statement of Robert W. Holleyman, II, President and CEO, Business Software Alliance, noting that software piracy costs the industry almost $13 billion each year); *id.* at 43 (statement of Hilary B. Rosen: "Copyrighted works will not have a business online unless copyright owners. . .are convinced that their products are secure."); Benkler, *supra* note 28, at 423 n.266.

168. *See Hearing on H.R. 2281*, *supra* note 28, at 36-37 (statement of Robert W. Holleyman, II, suggesting that eliminating piracy will create jobs); Benkler, *supra* note 28, at 423 n.267.

169. *See Hearing on H.R. 2281*, *supra* note 28, at 106 (testimony of Steven J. Metalitz, discussing limitations of linking act of circumvention to infringement); Benkler, *supra* note 28, at 423 n.268.

tects any TPS that "effectively protects" digital media regardless of its actual restriction of users' rights.[170] Currently, it is assumed that the anti-circumvention provisions must be read broadly—a proposition supported by judicial interpretations.[171] Accordingly, one must weigh the above justifications for the provisions against the greatest restrictions of which TPSs are capable—prevention of all unauthorized use of protected materials, some of which may be part of the public domain.[172]

None of the justifications for the statute are compelling in the face of the statute's impairment of users' constitutional rights. The first justification, that content will not be produced without legal backup, is undermined by the breadth and depth of content already available on the Internet. So far, Internet entrepreneurs have managed to adopt business models to account for the lack of legal backup of technical measures. Thousands of web sites use advertising revenue-based business models, giving their content away for free.[173] These have, in recent days, been less than a shining example, but other innovative models exist and surely more will be

---

170. *See, e.g.,* H.R. REP. NO. 105-551, pt. 2, at 9 (1998). Congress stated:

> SEC. 107. DEVELOPMENT AND IMPLEMENTATION OF TECHNOLOGICAL PROTECTION MEASURES. (a) STATEMENT OF CONGRESSIONAL POLICY AND OBJECTIVE: It is the sense of the Congress that technological protection measures play a crucial role in safeguarding the interests of both copyright owners and lawful users of copyrighted works in digital formats, by facilitating lawful uses of such works while protecting the private property interests of holders of rights under title 17, United States Code. Accordingly, the expeditious implementation of such measures, developed by the private sector through voluntary industry-led processes, is a key factor in realizing the full benefits of making available copyrighted works through digital networks, including the benefits set forth in this section.

Id.

171. *See infra* Part III.B.

172. There is not a ready example of such a TPS, and one might not even exist yet. However, if the anti-circumvention provisions are to be successfully challenged, it will most likely be by users who have had their desire to make fair use of copyrighted materials or to use public domain materials frustrated by such a restrictive digital fence.

173. These range from online newspapers, like the *New York Times*, to humor magazines like *The Onion*. *See* N.Y. Times Co., *New York Times Online*, *at* http://www.nytimes.com (last modified Sept. 1, 2001); Onion, Inc., *The Onion*, *at* http://www.theonion.com (last modified Aug. 29, 2001).

created.[174] Without legal backup, content owners will not allow the value of the Internet to go unexploited; they will simply find other ways to do it.

In addition, the industry's claim for the need of TPSs diminishes in force as the strength of TPSs increases. TPSs will guard media from all but an extremely small fraction of individuals, so the need for legal protection is not as dire when, as here, we are discussing the strongest TPSs. This is not to say the DMCA should not protect powerful TPSs; in fact, strong TPSs are desirable because they will be the best safeguards against illegal uses. This obvious point that theft should be discouraged does not, however, support the DMCA's broad approach, because the desire to promote strong fencing does not necessitate or justify indiscriminate protection of all TPSs. Strong digital fences have a great capacity to impinge upon users' rights and thus need the least legal reinforcement. The theft-reduction rationale for reinforcing even powerful, overly restrictive TPSs is extremely dubious in the face of a legal right to restrict users' speech.

Ultimately, the copyright industry's argument—that content cannot be provided—is a claim that the law should protect brick and mortar business models in the digital environment. In this regard, their claims eerily echo the motion picture industry's attempt to maintain the status quo by making claims—which ultimately proved mistaken—that the VCR would destroy the movie business.[175] Government assertions that legal facilitation of old business models will enable the Internet to realize "its full potential" therefore seem disingenuous (unless "full potential" means unregulated control by the industry).[176] It is impossible, however, to predict how industry control will affect the market. Because it is not axiomatic that such a policy would have a positive effect for consumers,[177] the claim is at best "conjectural," to use the language of the Court, and cannot pass First Amendment muster.

The second argument, that the copyright industry—the makers of movies, music, and books—is an important sector of the domestic econ-

---

174. See *supra*, note 67, listing models based on giving away the initial digital media in order to sell auxiliary products, upgrades, or other real-world products.

175. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 454 (1984).

176. *See Joint Hearing on S. 1284 and H.R. 2441 Before the Subcommittee on Courts and Intellectual Property of the House Comm. on the Judiciary and the Senate Comm. on the Judiciary*, 104 Cong. 35 (1995) (testimony of Bruce A. Lehman, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks).

177. *Cf.* Benkler, *supra* note 28, at 424 (arguing that certain types of producers that do not derive monetary benefits from increased propertization are also likely to suffer); *see also supra* notes 141-49 and accompanying text.

omy, is more convincing. The industry employs many Americans, and producers in this particular industry are more often domestically based than are their consumers.[178] Thus, Congress could have been legitimately concerned by an ultimatum from the copyright industries. This concern does not, however, militate in favor of indiscriminately protecting TPSs under the law. The copyright industry has never been dependent on an undifferentiated right to control its media. Copyright in tangible media, with all its exceptions, has been more than adequate to allow the industry to grow and provide thousands of jobs in this country. There is no evidence that the industry will suffer if the law forces strong TPSs to maintain fair use and the public domain. The point that the copyright industry provides many jobs is of course real and verifiable, but the illogical extension of that fact—that it will no longer be able to do so without indiscriminate protection of TPSs—is conjecture at this stage.

The copyright industries' third argument—that the DMCA must prevent all circumvention, not just that undertaken for the purposes of infringement—also fails to justify the DMCA's broad provisions. The industries claim that if the law recognizes circumvention as a legitimate way to make protected uses of media, the industries' only remaining option would be to sue distributors of circumvention devices for contributory infringement.[179] This claim is unattractive for two reasons. First, they would have to prove the underlying infringement by users, which requires tracking of actual media uses. Although this is possible on the Internet,[180] it is more difficult than simply showing that a device can circumvent a TPS. Second, contributory infringement is itself a limited claim. Under the *Sony* decision, providers of anti-circumvention devices are not liable for contributory infringement of copyright—and, by logical extension, the DMCA—if their devices an absence of are merely capable of a substantial noninfringing use.[181] Facilitating fair use and access to public domain materials would almost surely qualify under this standard.[182] Thus, the *Sony* rule would shift the burden of proof of

178. *See id.* at 425.

179. A party "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.'" 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04 (citing Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

180. *See supra* notes 36-40 and accompanying text.

181. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

182. *See* Benkler, *supra* note 28, at 426.

rule would shift the burden of proof of showing substantial noninfringing uses to the plaintiff.[183] The plaintiff, therefore, would have to prove underlying infringement for a court to find the distributors of circumvention devices liable under section 1201(a)(2) of the DMCA. The copyright industry convinced Congress that this is problematic because infringement is particularly difficult to track down and prove on the Internet.[184] The result is that the DMCA makes it easier for plaintiffs to legally reinforce their TPSs by effectively presuming that circumvention is illegitimate. This presumed illegitimacy contradicts the reality that in some cases, circumventing TPSs is the only way for users to make constitutionally protected uses of media. The DMCA's presupposition that circumvention and devices that facilitate circumvention are always illegitimate—especially in light of their necessity to fair use—is at best conjecture.

Lastly, some commentators have argued that the increased efficiency afforded by TPSs will not only outweigh the burdens to users, but may also increase content production.[185] According to this view, TPSs actually promote speech. This efficiency argument relies on the premise that "[b]ecause automated rights management creates well-defined and readily transferable property rights to information, it puts the power of the market in the service of consumer demand."[186] Although this is true for content that can be accurately valued, it fails to account for the loss of content from producers who do not rely on sale or licensing to derive value from their products.[187] Because of the decrease in that type of content production,[188] the claim that greater rights in information leads to an increased amount or diversity of creative output is open to challenge and is at least, in part, conjecture.

If the DMCA affords legal reinforcement to TPSs that protect digital media to a greater extent than is possible under copyright or other intellec-

---

183. 17 U.S.C. §§ 1201(a)(2)(A)-(B) (Supp. 2000) (exempting circumvention devices not "primarily designed or produced for the purpose of circumventi[on]" and having more than "limited commercially significant purpose or use other than to circumvent."). Presumably where a device can circumvent plaintiff's TPS, the burden would be on the defendant to prove it was exempt under these sections. *Cf.* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 318-19 (S.D.N.Y. 2000) (finding that a device was designed primarily to circumvent is prima facie evidence that it lacks other commercially significant purpose).

184. See *supra* notes 6-13 and accompanying text.

185. *See* Bell, *supra* note 15, at 585-89.

186. *Id.* at 589; see also *supra* notes 53-58 and accompanying text.

187. *See supra* note 148 and accompanying text.

188. *See supra* notes 141-45 and accompanying text.

tual property law, then the courts should do one of three things. Each option requires sensitivity to the constitutional problem that arises when users' rights are restricted. First, courts should read the statute narrowly—though in line with legislative intent—to avoid the constitutional problem.[189] If it is not susceptible to such a limiting interpretation, then the courts should address directly whether the interests furthered by the statute outweigh the limitations it imposes on speech. As discussed above, a court making such a determination should find that the justifications do not warrant the constitutional infirmities. Accordingly, the last step for the courts is to strike down the DMCA's anti-circumvention provisions on the ground that Congress's creation of a legal right to enforcement of all TPSs exceeded its power under the Intellectual Property Clause and impermissibly restricted speech in violation of the First Amendment.

B. Judicial Interpretations of the Anti-Circumvention Provisions

The previous section evaluated the constitutionality of the DMCA anti-circumvention provisions based on the assumption that they would be read broadly to protect TPSs that restrict constitutionally protected users' rights. As described below, that is exactly what courts have done. Courts need not, however, read the statute so broadly. Concerned that TPSs would shift us towards a "pay-per-use" society,[190] Congress incorporated a detailed set of exceptions to the DMCA's bans on circumvention and devices to circumvent.[191] Although the exceptions are numerous and complex, they do not cover all types of fair use.[192] In order to determine the status of uses not specifically provided for in the exceptions, one must turn to the separate fair use and free speech provisions in the statute.[193]

---

189. *See* Miller v. French, 530 U.S. 327, 341 (2000) ("And while this construction raises constitutional questions, the canon of constitutional doubt permits us to avoid such questions only where the saving construction is not plainly contrary to the intent of Congress.") (internal citation omitted).

190. 144 CONG. REC. S11887, S11888 (daily ed. Oct. 8, 1998) (statement of Sen. Ashcroft).

191. For a discussion of how these exceptions interact with each of the bans on circumvention, see Nimmer, *supra* note 18, at 700-02; *see also*, Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519, 537-43 (1999).

192. *See* Nimmer, *supra* note 18, at 738-39.

193. There is no public domain exception. The statute affords access protection to "a work protected under [the Copyright Act]," whether the user wishes to make unauthorized use of protected expression or unprotectible material. 17 U.S.C. § 1201(a)(1)(A) (Supp. 2000). However, a proper fair use exception should take care of this problem. Use

The DMCA contains three provisions dedicated to protecting fair use and free speech. Section 1201(c) states the first two: "(1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title. . . . (4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products." The remaining provision, 1201(a)(1), requires the Register of Copyrights to conduct an administrative rulemaking procedure to exempt classes of works with regard to which the DMCA has adversely affected users ability to make noninfringing uses. Courts, however, have failed to consider adequately the importance of these sections to the protection of First Amendment rights.

In *Universal City Studios v. Reimerdes*,[194] the federal court for the Southern District of New York decided a claim by a group of movie studios against Eric Corley and his company, 2600 Enterprises, Inc.[195] Defendants posted a copy of DeCSS—a decryption program designed to break CSS, the TPS used by DVD players to prevent home users' access to DVDs on nonlicensed systems—on their web site.[196] The program's creator claimed he created it so he could play his lawfully purchased DVDs on his home computer, which ran an operating system incompatible with CSS.[197] Plaintiffs claimed that by posting DeCSS on http://www.2600.com, the defendants violated section 1201(a)(2) of the DMCA by distributing a circumvention device.[198] The court held in favor of the plaintiffs and enjoined the defendants from posting DeCSS or linking to sites posting it.[199]

---

of public domain materials is generally considered a noninfringing use. *See, e.g.,* Sheldon v. Metro-Goldwyn Pictures Corp., 81 F.2d 49 (2d Cir. 1936); Nichols v. Universal Pictures Corp., 45 F.2d 119 (2d Cir. 1930). Fair use, on the other hand, is a defense to infringement. *See* 17 U.S.C. § 107 (Supp. 2000). The distinction matters little, however, as far as protecting access to public domain materials is concerned. In a typical suit, the defendant either claims "I have a right to use this" (fair use) or "you have no right to sue me" (public domain). Substantively, the former can include the latter, so adequate provision for fair use in the DMCA should suffice to protect users' rights without explicit reference to the public domain.

194. 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

195. 2600 Enterprises, Inc. publishes *2600: The Hacker Quarterly* and maintains a web site devoted to hacker issues. 2600 Enters., Inc., *2600: The Hacker Quarterly*, *at* http://www.2600.com (last visited Sept. 1, 2001).

196. *See Reimerdes*, 111 F. Supp. 2d at 309.

197. *See id.* at 310.

198. 17 U.S.C. §1201(a)(2) (Supp. 2000).

199. *Reimerdes*, 111 F. Supp. 2d at 345.

The court rejected defendants' statutory fair use claim, holding that one violates the DMCA even if the circumvention measures are absolutely necessary to facilitate fair use.[200] The effect of this holding is that even if users have a constitutionally protected right to make certain uses of protected media, they will lack the means to exercise their right unless they are technically capable of circumventing the TPS themselves. The court did not mention Congress's explicit recognition in section 1201(c)(1) that "[n]othing in this section shall affect rights, remedies, limitation, or defenses to copyright infringement, *including fair use*, under this title."[201] Nor did it point out section 1201(c)(4)'s commitment to maintaining the status quo of free speech involving telecommunications or computers.[202] Rather than considering the implications of these statements, which might militate in favor of a narrow reading of 1201(a)(2),[203] the court ignored them entirely. Instead of relying on the language of the statute, the court relied on the legislative history suggesting that fair use is limited to situations in which "access is authorized."[204] Thus, untroubled by the question that section 1201(c) raises as to whether Congress intended to limit fair use rights to the technically savvy,[205] the court broadly interpreted the statute to prohibit all circumvention devices covered by section 1201(a)(2), regardless of their necessity to speech rights.[206]

Admirably, the court acknowledged the serious question as to whether courts should interpret the DMCA to make any fair use of plaintiff's copyrighted works difficult or impossible.[207] It ultimately deferred to Con-

---

200. *Id.* at 323-24.

201. 17 U.S.C. §1201(c)(1) (Supp. 2000) (emphasis added).

202. 17 U.S.C. §1201(c)(4) (Supp. 2000).

203. *Cf.* Samuelson, *supra* note 191, at 551.

204. *Reimerdes*, 111 F. Supp. 2d at 323 (quoting H.R. REP. NO. 105-551, pt. 2, at 18 (1998).

205. *See* Samuelson, *supra* note 191, at 551; *but see* Nimmer, *supra* note 18, at 738 (arguing that Congress's half-hearted effort at protecting users' rights, in comparison with the detailed exceptions for other uses in sections 1201(d)-(j), indicates the intent not to protect them is relatively clear); *see also supra* note 24.

206. The facts of the *Reimerdes* case, at least from the court's perspective, gave little reason to be careful with language. The court obviously thought Johansen's claim that he made DeCSS to circumvent CSS primarily for fair use of the protected material was a ruse. *See Reimerde*s, 111 F. Supp. 2d at 320. A more sympathetic case might at least have prompted an acknowledgment that the DMCA might leave open some possibility of distribution of circumvention devices necessary to fair use. As a precedent, *Reimerdes* leaves little room for such a defense. For a hypothetical example of a sympathetic case, see Samuelson, *supra* note 191, at 551-52.

207. *Reimerdes*, 111 F. Supp. 2d at 322.

gress's determination that the law could maintain the intellectual property balance without a fair use exception to circumvention.[208] The court made three points in support of its decision. First, Congress left fair use fully applicable to all uses of works obtained with authorization.[209] Second, Congress provided for administrative rulemaking in section 1201(a)(1) to determine whether users' rights were being adversely affected.[210] And third, the DMCA includes a detailed set of exceptions to the circumvention ban "for certain uses Congress thought 'fair.'"[211]

The problem with the court's approach is that these limitations do not completely eliminate the possibility of unconstitutional restrictions on speech. On the first point, fair use of TPS-protected works will always depend on access, which, because of the anti-circumvention provisions, requires authorization. However, although the DMCA contains several exceptions for particular types of uses, it lacks a specific exception to make fair use possible without authorization or circumvention. Thus, under the court's interpretation, only the rulemaking provision can save fair use. The rulemaking provision, as discussed in Part III.C, is not up to the task. Thus, the *Reimerdes* court's statutory construction places the DMCA within the constitutionally problematic zone identified above in Part III.A.[212]

The only other case that deals with the DMCA's anti-circumvention provisions in detail comes from the Western District of Washington. In *RealNetworks, Inc. v. Streambox Inc.,*[213] plaintiff, RealNetworks claimed defendant, Streambox impermissibly developed and distributed a device to circumvent the TPS protecting RealNetworks' media delivery service, RealServer/RealPlayer.[214] Essentially a software-based trusted system, the service allows content owners to stream media using RealServer to users using RealPlayer and to technologically control whether or not the user

---

208. *Id.*
209. *Id.*
210. *Id.*
211. *Id.*
212. *See supra* notes 163-75 and accompanying text.
213. No. C99-2070P, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000). One other court dealt specifically with the DeCSS controversy, but considered only a trade secret misappropriation claim and did not address any questions under the DMCA. *See* DVD Copy Control Ass'n, Inc. v. McLaughlin, No. CV786804, 2000 WL 48512 (Cal. Sup. Ct. Jan, 21 2000).
214. *Id.* at *1.

can make an unauthorized copy.[215] Streambox's product, the "VCR," spoofed the authentication program and appeared to the RealServer as if it were a RealPlayer. The VCR also ignored the technical control signal from RealServer that prevented unauthorized copying on a RealPlayer.[216]

Streambox defended its action on the grounds that the VCR allowed consumers to make fair use of files available only through RealServer.[217] The defendants apparently limited their argument to a claim that under *Sony* they could not be liable for contributory infringement because the VCR was "capable of substantial noninfringing uses."[218] The court, noting that a claim under the DMCA's anti-circumvention provisions is not a suit for copyright infringement, held that the question of the defendants' liability for contributory infringement was irrelevant.[219]

This holding is reasonable, but had the court considered section 1201(c)(1) of the DMCA protecting fair use,[220] it should have noticed that the question of whether *users'* fair use rights are being restricted is not so easily dismissed. Instead it dismissed the claim, stating that here, unlike in *Sony*—where many copyright holders either authorized or did not object to the home use—content owners attempted to prevent the use.[221] Fair use, however, has nothing to do with whether or not the content owner authorizes the use.[222]

The end result of overlooking this crucial issue was the court's unqualified assertion that "[u]nder the DMCA, product developers do not have the right to distribute products that circumvent [TPSs] that prevent consumers from gaining unauthorized access to or making unauthorized copies of works protected by the Copyright Act."[223] In other words, the DMCA prohibits even circumvention measures necessary to enable the exercise of free speech rights. Again, the court placed the anti-circumvention provisions into a constitutionally suspect zone.

---

215. *Id.* at *2.
216. *Id.* at *4.
217. *Id.* at *8.
218. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).
219. *See RealNetworks*, 2000 WL 127311 at *8.
220. The opinion makes no reference to either section 1201(c)(1) or 1201(c)(4).
221. *RealNetworks*, 2000 WL 127311 at *8.
222. "If the use is otherwise fair, then no permission need be sought or granted. Thus, being denied permission to use a work does not weigh against a finding of fair use." Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 585 (1994).
223. *RealNetworks*, 2000 WL 127311 at *8.

Whether Congress intended to limit speech and fair use when it drafted the DMCA is open to debate. The care taken to make sure other exemptions were viable, such as reverse engineering and encryption testing, suggests that Congress may have realized the importance of its actions for users' rights.[224] If it intended this limitation, the *Reimerdes* and *Streambox* courts were right not to read the statute narrowly. This Comment has argued, however, that the exceptions in sections 1201(c)(1) and (c)(4) might militate in favor of a more limited reading,[225] particularly since the courts' broad reading of the statute creates a questionable legal right to prevent others' speech. Courts, on the other hand, have relied on the section 1201(a)(1) administrative rulemaking provision to protect users' rights. As the Comment discusses below, the rulemaking provision is inadequate to protect users' rights because it is severely limited in two important ways.

C. A "Fail-Safe" Mechanism? The Section 1201(a)(1) Rulemaking Provision

After the DMCA was reported out of the House Judiciary Committee, it was referred to the House Committee on Commerce. The Commerce Committee expressed some reservations that the DMCA might undermine Congress's commitment to fair use.[226] These concerns led the Committee to propose a "fail-safe" mechanism—one that would allow the Librarian of Congress, upon recommendation by the Register of Copyrights, to selectively waive the enforceability of the prohibition against circumvention if it was necessary to maintain the availability of a particular category of copyrighted materials.[227] That mechanism is the rulemaking process laid out in section 1201(a)(1).[228]

---

224. *See* Nimmer, *supra* note 18, at 738-39.

225. One possible limited reading is offered by Jane Ginsburg. *See* Ginsburg, *supra* note 19. She asserts that the syntax of section 1201(c)(1) permits an argument that "including fair use," as set off in commas, modifies not the immediately preceding phrase "or defenses to copyright infringement," but "limitations . . . under this title." *Id.* at 15. The interpretation finds support in fair use's original judicial nature, its applicability to other areas of intellectual property law, such as trademark, and Congress's disavowal of any intent to "freeze" the judge-made doctrine by codification in 17 U.S.C. § 107.

226. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,557 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201).

227. *See id.* at 64,558.

228. The section provides in full:

§ 1201. Circumvention of copyright protection systems

(a) Violations regarding circumvention of technological measures.

(1) (A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter [enacted Oct. 28, 1998].

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine—

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

Put simply, the rulemaking is designed to publish a class of copyrighted works, the fair use of which the DMCA has adversely affected.[229] The Register of Copyrights is to make determinations two years after the statute became effective, and every three years thereafter.[230] The first rulemaking decision issued on October 27, 2000, one day before the 1201(a)(2) anti-circumvention regulation went into effect.[231]

The first problem with the "fail-safe" mechanism arises out of the structure of the statute itself: the exemption only applies to the statute's prohibition of circumvention.[232] The statute still prohibits manufacturing and distributing devices to circumvent TPSs, even those specifically designed to facilitate the narrow exemption granted in the rulemaking.[233] Therefore, even if the Register of Copyrights finds that the DMCA adversely affects users' rights, users get an exemption in name only.

The upshot is that the fail-safe mechanism protects only the constitutional rights of users capable of circumventing TPSs on their own. This group is already an extremely small one. As TPSs become more advanced, even fewer people will possess the programming skills required to crack TPSs in order to exercise their constitutional use rights. That these hackers' rights are not diminished is irrelevant: restriction of some users' rights is not any more constitutional by virtue of the fact that other users' rights are not restricted.[234] Thus, unless future courts utilize the section 1201(c) limitations to reach a narrower reading of the statute, the presence of the statutory rulemaking provision cannot make the anti-circumvention provisions constitutional.

---

229. 17 U.S.C. § 1201(a)(1)(D) (Supp. 2000).

230. *Id.* § 1201(a)(1)(C).

231. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201). That decision exempted compilations of web sites blocked by filtering software applications and literary works, including computer programs and databases, protected by TPSs that fail to permit access because of malfunction, damage or obsoleteness. 37 C.F.R. § 201.40 (2001).

232. *See* Nimmer, *supra* note 18; *see also* Samuelson, *supra* note 191.

233. *See* Nimmer, *supra* note 18, at 736-37. Nimmer argues that there is good reason not to allow manufacture and distribution of circumvention devices that could be used to facilitate more than just exempted circumvention. The exception would swallow the rule.

234. *See* Planned Parenthood of Southeastern Penn. v. Casey, 503 U.S. 833, 894 (1992) ("Legislation is measured for consistency with the Constitution by its impact on those whose conduct it affects . . . . The proper focus of constitutional inquiry is the group for whom the law is a restriction, not the group for whom the law is irrelevant.").

Congress could lessen the problem with the rulemaking provision by amending it so that exemptions it grants would also extend to the circumvention devices capable only of facilitating those exemptions. This would make the exemptions meaningful for all users regardless of technical skill. This also might mitigate the constitutional problem presented by limiting lawful use rights, but it would most likely not solve it because of the second problem with the rulemaking provision: the framework of the provision itself is not able to produce exemptions sufficient to protect users' rights.

Section 1201(a)(1)(C) requires the Register of Copyrights to determine whether noninfringing use of a particular *class of works* is, or is likely to be adversely affected by the DMCA.[235] "Class of works," as interpreted by the Register of Copyrights, means a "narrow and focused subset of the broad categories of works of authorship . . . . identified in section 102 [of the Copyright Act]."[236] A class can include works from more than one category of works, but is necessarily narrower in scope than any single category.[237] Thus, if users of law casebooks or computer games generally find their uses restricted on the Internet, the Register of Copyrights may exempt those classes of works in a future rulemaking.[238] The legislative history supports this interpretation of "class of works."[239]

In the rulemaking issued on October 27, 2000, the Register argued that though a reference to the medium of work or the TPS applied could narrow the class, the statute does not permit classifying a work solely by reference to the type of use or users.[240] Indeed, Congress could have written

---

235. 17 U.S.C. §§ 1201(a)(1)(B), (a)(1)(C) (Supp. 2000).

236. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,560. Section 102 includes but is not limited to: literary works, musical works, dramatic works, pantomimes and choreographic works, pictorial, graphic and sculptural works, motion pictures and other audiovisual works, sound recordings, and architectural works. 17 U.S.C. § 102 (1994).

237. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,560.

238. *See* NIMMER & NIMMER, *supra* note 179, § 12A.03[A][2][b] (Copyright Protection Systems and Management Information, Special Pamphlet).

239. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,560-64,561 (citing H.R. REP. NO. 105-551, pt. 2, at 36-38 (1998); and STAFF OF HOUSE COMM. ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, at 7 (Comm. Print 1998) (Rep. Coble)).

240. *Id.*

section 1201(a)(1) not to rely upon types of works but upon types of uses. It instead chose to advert to language in the Copyright Act itself.[241] This creates an odd juxtaposition.

Congress deliberately wrote the DMCA to provide a separate cause of action from those provided by the Copyright Act.[242] The DMCA premises liability on access and the means by which it is achieved, regardless of the content protected.[243] Copyright law, in contrast, protects certain expressive content from unauthorized use.[244] Given their respective purposes, the predicate for liability in each of these statutes makes sense. Whether copyright law protects a work should turn on the nature of the work itself, not how users access it. Conversely, the DMCA seeks to provide legal reinforcement to digital fences; accordingly, it should generally focus liability on bypassing fences without regard to what they protect. But by using copyright language in the DMCA's rulemaking provision, Congress provided an incongruous content-limited fair use exemption to a content-neutral cause of action. It is the only exception to the DMCA not based on the type of use for which a user accesses a work.[245]

The end result is that exemptions will only protect users of specific types of works, like law textbooks or computer games. This fact highlights the constitutional problem with the limited definition of a "class of works." The fit between what the provision seeks to protect (fair use) and the provision's criterion for protecting it (the DMCA's adverse effect on the use of a class of works) is a poor one. Fair use is usually determined

---

241. *See supra* note 236.

242. In the amendments proposed by the Committee on Commerce, the DMCA was to be a free-standing set of provisions. Proposed section 102(c)(1), the analogous provision to enacted section 1201(c)(1), read: "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, *under title 17, United States Code*." H.R. REP. NO. 105-551, pt. 2, at 3 (1998), (emphasis added). As enacted, the provision is the same except for the italicized portion above, which reads: "under this title [17]." 17 U.S.C. 1201(c)(1) (Supp. 2000).

243. *See supra* notes 17-22 and accompanying text.

244. *See* 17 U.S.C. § 102 (1994).

245. *See* 17 U.S.C. § 1201(d) (Supp. 2000) (access for nonprofit library's determination of whether to purchase a work); *id.* § 1201(e) (access for law enforcement purposes); *id.* § 1201(f) (access to reverse engineer in order to achieve interoperability of programs); *id.* § 1201(g) (access to conduct encryption research); *id.* § 1201(h) (access to produce technology with the sole purpose of limiting access of minors to material on the Internet); *id.* § 1201(i) (access to identify and disable a TPS's ability to collect and disseminate personal identifying information about a natural person); *id.* § 1201(j) (access for security testing purposes).

without reference to the type of work used—except in the very broad sense of whether the work is factual or fanciful.[246] It turns, instead, on how the user uses the work and the type of use to which the user puts the work.[247] Under the Register's interpretation of the statute, however, there is no room for acknowledgment of the types of uses users wish to make under the rulemaking analysis.[248]

Under the rulemaking procedure, the Register is to consider public comments, including possible exemption classes. The proposed "Fair Use Works" exemption illustrates the difficulty of the content-based definition of "class of works."[249] Proponents of the exemption class defined it as the types of works most likely to be used by libraries and educational institutions for purposes of fair use.[250] The problem with drawing the boundaries of such a proposal—and in part the reason the Register rejected it—is that it is too broad unless it can be limited to access for fair use or by certain users (e.g., public libraries).[251] As the exemption's proponents recognized, it is wrong to presume that every circumvention is fair just because the

---

246. *Id.* § 107(2); *see* Campbell v. Acuff-Rose Music, Inc., 510 U.S 569, 586 (1994) ("Th[e second statutory fair use] factor calls for recognition that some works are closer to the core of intended copyright protection than others, with the consequence that fair use is more difficult to establish when the former works are copied. *See*, *e.g.*, Stewart v. Abend, 495 U.S. [207,]237-38 (1990) (contrasting fictional short story with factual works); Harper & Row [Publishers, Inc. v. Nation Enters.], 471 U.S. [539,]563-64 (1985) (contrasting soon-to-be-published memoir with published speech); Sony [Corp. of Am. v. Universal City Studios], 464 U.S. [417,]455 n.40 (1984) (contrasting motion pictures with news broadcasts); Feist [Publ'ns, Inc. v. Rural Telephone Service], 499 U.S. [340,]348-51 (1991) (contrasting creative works with bare factual compilations).").

247. 17 U.S.C. § 107 (Supp. 2000).

248. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,566-64,573 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201) (rejecting for failure to describe a statutory "class of works" proposed exemptions for "Sole Source Works"); *id.* at 64,567 ("Computer Programs and Other Digital Works for Purposes of Reverse Engineering"); *id.* at 64,570 ("Fair Use Works"—rejecting proposal to extent it sought to limit applicability to certain classes of users or uses); *id.* at 64,571 ("Material that Cannot be Archived or Preserved"); *id.* at 64,572 ("Works Embodied in Copies Which Have Been Lawfully Acquired by Users Who Subsequently Seek to Make Non-infringing Uses Thereof").

249. *See id.* at 64,571-64,572.

250. *See id.* at 64,571.

251. *Id.* (noting that witnesses testifying on behalf of the proposed exemption explained that the works should be exempted when the purpose of use was fair use, and that the exemption should also be limited to a specific class of persons who were likely to be fair users).

types of works cited are often put to fair use.[252] It is for this reason the approach taken by the proponents of the exemption here, though laudable, will probably never work under the statute. Once one defines a class of content by actual or likely uses, taking away the criteria used to define the class makes it unreasonably large.

Notwithstanding the language of the statute, relying on use in defining the class is logically the best way to protect fair use. This approach could ensure congruence between fair uses prevented by the anti-circumvention provisions and fair uses protected by the rulemaking provision. A use-based approach would also alleviate a related problem the rulemaking provision creates: by using a content-based definition of an exempted class, it necessarily must rely on aggregate, rather than individual cases of attempted fair use. If the Register of Copyrights granted a content-based exemption because of a single owner's restriction of fair use,[253] all owners of a particular type of content would be unable to prevent circumvention. This would be unfair, so the standard must aggregate frustrated attempts at fair use for the entire class of content.

The resulting standard is that users of a class of works must have experienced "distinct, verifiable, and measurable impacts" on lawful use of the entire class of works before the Register will grant them an exemption.[254] "[M]ere inconveniences, or individual cases" do not warrant an exemption.[255] This standard limits the right of fair use to the rare situation[256] in which a substantial number of people wishing to make fair use of a particular type of work have had that right restricted by TPSs and the DMCA. Not surprisingly, the Register struck down many proposals for lack of evidence of adverse effect in the aggregate.[257]

---

252. *Id.*

253. *See id.* at 64,560: "For example, if a showing had been made that users of motion pictures released on DVDs are adversely affected in their ability to make noninfringing uses of those works, it would be unfortunate if the Librarian's only choice were to exempt motion pictures."

254. H.R. REP. NO. 105-551, pt. 2, at 37 (1998).

255. STAFF OF HOUSE COMM. ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, at 6 (Comm. Print 1998) (Rep. Coble).

256. This was explicitly contemplated by Congress: "In any 3-year period, it may be determined that the conditions for the exemption do not exist." H.R. REP. NO. 105-551, pt. 2, at 36.

257. See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,566-64,573 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201), rejecting for failure to establish substantial

Ultimately, the substantial effect requirement may be susceptible to constitutional challenge because it mistakenly treats information as a fungible commodity. In essence the provision states that if a user cannot use a particular law text or computer game, she must go out and make use of another. Only if a TPS shields all law texts or computer games from fair use will an exemption lie under section 1201(a)(1). Fair use, however, is not merely a general right to use information; it exempts lawful use of information the user actually chooses to use. This reflects the First Amendment right to acquire knowledge of one's choice.[258] Thus the rulemaking provision fails to protect the constitutional right to make fair use of a particular lawfully acquired work by limiting relief to those situations in which lawful use of a whole class of works has been substantially affected.

Overall, the rulemaking provision is unlikely to help those wishing to make fair use of digital works. Even if Congress amends it to extend exemptions to circumvention devices capable of facilitating only protected uses, the exemptions themselves do not adequately protect fair use. The rulemaking provision does not narrow courts' broad readings of the anti-circumvention provisions enough to protect constitutional speech rights. Where the statute reinforces overly restrictive TPSs, it fosters only protection, not "Progress," because it limits the protected speech of users. Accordingly, the broad reading of the DMCA is constitutionally unsound.

Nevertheless, the broad reading is not inescapable. Courts have yet to acknowledge the section 1201(c) fair use and free speech safeguards. One commentator, for example, interpreted section 1201(c)(1) to mean that fair use must be an available defense to all challenges under the anti-circumvention provisions.[259] As yet, however, no court has hinted at any similarly limiting approach. If courts cannot come to a narrower interpretation of the anti-circumvention device provision—one which protects us-

---

adverse effect proposed exemptions for "Thin Copyright Works," *id.* at 64,566, "Sole Source Works," *id.* at 64,567, "Audiovisual Works on Digital Versatile Discs (DVD)," *id.* at 64,567-64,570, "Video Games in Formats Playable Only on Dedicated Platforms," *id.* at 64,570, "Computer Programs and Other Digital Works for Purposes of Reverse Engineering," *id.* at 64,570, "Encryption Research Purposes," *id.* at 64,571, "Fair Use Works," *id.* at 64,571, "Material that Cannot be Archived or Preserved," *id.* at 64,572, and "Works Embodied in Copies Which Have Been Lawfully Acquired by Users Who Subsequently Seek to Make Non-infringing Uses Thereof," *id.* at 64,572-64,573.

258. *See* Meyer v. Neb., 262 U.S. 390, 390 (1923) (striking down as inconsistent with the First Amendment a statute that prohibited teaching of German, but not ancient Greek, to a minor).

259. *See supra*, note 225.

ers' free speech rights—courts should hold this section of the DMCA unconstitutional.

IV. BEYOND THE DMCA: PRIVATE AND JUDICIAL ORDERING OF TPSs

Even if courts declare the DMCA's anti-circumvention provisions unconstitutional, this would not directly affect the technology they protect. A court is most likely to find the statute unconstitutional where an especially restrictive TPS is challenged by people who have lawfully acquired digital media but are unable to make fair use of it. The court, if it perceives itself to be bound by the language, legislative history, and prior judicial interpretation of the DMCA, may strike down the anti-circumvention provisions as unconstitutionally conveying a right to restrict users' speech by use of this particular TPS. It would be unnecessary, however, for the court to rule on the right of the content owner to use the TPS itself to reach its holding. Thus, even if a court struck down the challenged statutory provisions, access to protected works will still depend on availability of technical circumvention means. As a practical matter, this will probably foreclose some legitimate uses.[260]

In Part II, this Comment argued that the scope of the anti-circumvention provisions depends on the strength and restrictiveness of the TPSs they reinforce. This section addresses the potentially problematic TPSs themselves. The concern with TPSs is the same as the one that motivated the analysis of the DMCA: content owners should not be able to restrict constitutionally protected user rights by using TPSs to protect digital media.

As this Comment has indicated throughout, however, TPSs are important to digital content development and can be extremely beneficial to both producers and users. TPSs offer benefits to owners and users, such as

---

260. TPSs offer protection from all but a tiny fraction of users. Of the fifty percent of Americans on the Internet today, very few have the technical skills necessary to break through even simple digital fences. Despite the ease with which Jon Johansen cracked the DVD protection code CSS, it had been around for three years before he broke it. *See* Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 311 (S.D.N.Y. 2000). Assuming anyone previously thought to break it in those three years, easy as it may have been for Johansen to do, it was apparently beyond other people's limited capabilities. Furthermore, hackers are still a fringe element in society, and given that the very word has become a pejorative epithet in judicial use, there is reason to believe they will be relegated further from the mainstream in the future.

reduced media theft, potential increases in access and distribution, authentication and certainty in uses and transactions, and facilitation of streamlined negotiations. Most importantly, TPSs will allow content owners to capture value previously unavailable from their works without recourse to copyright law. Given the difficulties of enforcing copyright law on the Internet, TPSs are necessary to media production. The music and movie industries, for example, have claimed that they will not produce content on the Internet without them.[261] Thus, the law should permit, and even encourage, the development of TPSs.

The stronger the TPS, the easier it is to recognize these potential boons. Unfortunately, the most powerful TPSs also pose the greatest threat to users' rights. Thus, the law must balance the rights of users and the needs of copyright owners. The legal system's goal, then, should be a legal and judicial environment in which content owners can develop TPSs extensively but carefully.

A. The Problem with Private Ordering by TPSs

The current statutory and judicial framework places TPSs outside the scope of direct regulation. This is troubling because copyright owners' overriding concern is to derive the most value from their media. In addition, the DMCA's current indiscriminate reinforcement of TPSs encourages the creation of the strongest, most restrictive protection systems. Even without the DMCA, content owners would have a powerful incentive to create strong TPSs: if a TPS failed without the DMCA, there would be no legal recourse for the copyright owner. This incentive structure suggests the need for legislative or judicial regulation, because preservation of user interests is unlikely to occur under a system of private ordering through the market. As this Comment has already discussed the problems with the current legislative scheme,[262] it now explores the likelihood that the private market will produce TPSs that preserve fair use rights and the public domain, before turning to judicial options.

So far, commentators have discussed technical protections primarily in the context of their facilitation of electronic contracts.[263] The main point

---

261. *See supra* notes 173-77.

262. *See supra* Part III.

263. *See* Bell, *supra* note 15; Cohen, *supra* note 63; Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462 (1998) [hereinafter Cohen, Lochner *in Cyberspace*]; Elkin-Koren, *supra* note 56; Fisher, *supra* note 301; David Friedman, *In Defense of Private Orderings: Comments on Julie Cohen's "Copyright and the Jurisprudence of Self-Help,"* 13 BERKELEY TECH L. J. 1151 (1998); Michael J. Madison, *Legal-Ware: Contract and*

of contention in these discussions is whether a private ordering system, through contract, will adequately protect the public domain.[264] Proponents of the private exchange view maintain that rational parties do not participate in transactions that are not beneficial to them.[265] They also believe that because contracts express autonomous choices and accurately reflect the intent of the parties, they are more legitimate than rules made by centralized bodies.[266] This belief, however, assumes that the contracting parties know the terms of the contract and give their meaningful assent to the terms.[267] When these assumptions break down, the private exchange view loses much of its bite.

The main problem with the private exchange view is that, while individuals may have knowledge of the terms of, and give meaningful assent to, individually negotiated transactions, this is not the case with mass-market contracts.[268] In mass-market contracts, terms are standardized. A market governed by these standard contracts is likely to produce little competition, leaving users no choice among terms.[269] Further, even assuming that a user could negotiate any terms, this model ignores the fact that non-price terms are more difficult to negotiate than price.[270] Yet another problem with the private exchange view is that users cannot easily predict the value that they will derive from future uses of media.[271] In con-

---

1151 (1998); Michael J. Madison, *Legal-Ware: Contract and Copyright in the Digital Age*, 67 FORDHAM L. REV. 1025 (1998).

264. *See supra* note 263.

265. *See* Elkin-Koren, *supra* note 56, at 1166.

266. *See id.* at 1172.

267. *See* Cohen, Lochner *in Cyberspace*, *supra* note 263, at 482.

268. The market for creative and informational works on the Internet is generally governed by standardized form contracts, which offer the consumer no opportunity to negotiate terms. *See* Elkin-Koren, *supra* note 56, at 1182-83. For example, an eBook version of Lewis Carroll's *Alice in Wonderland*, published by VolumeOne for the Adobe Acrobat eBook Reader comes with the following use restrictions attached:

> COPY: No text selections can be copied from this book to the clipboard.
> PRINT: No printing is permitted on this book.
> LEND: This book cannot be lent to someone else.
> GIVE: This book cannot be given to someone else.
> READ ALOUD: This book cannot be read aloud.

eVIL, HARPER'S, Mar. 2001, at 18.

269. *See* Elkin-Koren, *supra* note 56, at 1183.

270. *See* Cohen, Lochner *in Cyberspace*, *supra* note 263, at 488.

271. It is difficult to predict future uses because creative and informational works can be used in so many ways. Since many of the definitions of these uses rely on obscure legal terms—like fair use—restrictions may not be easy for purchasers to understand.

trast, content owners, who engage in many transactions, are better able to predict value than single-exchange users and therefore have a bargaining advantage.[272] Thus, in the mass-market contract context, users frequently have few options and inadequate knowledge to make an informed choice among them. The private ordering rationale for contract-based transactions in intellectual property fails in this context because the contract does not reflect the will of both of the parties.

The use of TPSs to order information transactions implicates all of the same concerns that arise in the mass-market contract context, and in addition, a few others. TPSs are never negotiable; instead, they are product-defining. They need not be transparent either: they can define products vis-à-vis their uses without telling the user that she will not be able to make fair use quotations or use public domain aspects of the work. In the alternative, content owners could design TPSs to provide this information to the user at the onset. In fact, this would ensure that both parties have full knowledge of the terms of the transaction and therefore would facilitate fair negotiation of terms. In contrast to contracts, however, there are no laws or regulations requiring copyright owners relying on TPSs to make these disclosures.[273] Ultimately the dispute need not reach the courts because content owners can engage in electronic self-help without relying on legal reinforcement.

In sum, the very nature of TPSs undermines the assumptions made by the private exchange view of market transactions. In addition, the fact that TPSs do not enjoy the system of oversight in place for contracts further limits the applicability of the private exchange view to TPSs. Therefore, it is dangerous to unquestioningly relegate the control of TPSs to private ordering.

Apart from questions of information and assent, private ordering of information markets threatens the production of benefits that the market is unable to value. Julie Cohen has provided a devastating critique of private ordering of intellectual property rights on the Internet.[274] Of particular relevance is her inquiry into the relationship between information and so-

---

Finally, information on the cost and benefit of each use is likely to be difficult to obtain. *See* Elkin-Koren, *supra* note 56, at 1181-82.

272. *Id*.

273. Enforcement of contracts, at least, is subject to judicial inquiry for notice, assent, and unconscionability. The UCC also contains consumer protections, such as implied warranties and remedies. These are on the decline even for digital contracts, however. The Uniform Computer Information Transactions Act, which limits these protections, has been adopted by at least two states.

274. *See* Cohen, Lochner *in Cyberspace*, *supra* note 263.

cial welfare.[275] Cohen argues that information is inherently transformative because its shared benefits are central to the social self-definition of individuals.[276] Information use creates ancillary social value by shaping public opinion, interactions, and political participation, and provides a feedback circuit for further information production and receipt.[277] The current real-world common ownership model—the public domain—facilitates this cross-pollination, amplifying information's transformative effects.[278]

These ancillary social benefits require a network of information users to achieve their value, which raises a collective action problem.[279] From the perspective of an individual user, the ability to share information with others is of uncertain value since it involves hypothetical future uses.[280] Accordingly, users undervalue the right to take part in this sharing of information. From the owner's perspective, this same uncertainty causes them to overvalue a right to share because they want to collect on every potential use.[281] An individual user is therefore unlikely to value privileges provided for future uses highly enough to pay the price the owner demands for them. The result is that, in a purely market-driven system where TPSs control all types of use, uses of information that are particularly valuable in the aggregate will not occur because individual users will not pay owners for those rights. Allowing content owners to use TPSs to control access to their works will not only give owners benefits previously unavailable to them because of real-world market inefficiency, it will also qualitatively change the nature of information use.[282] Media will no longer play the socially beneficial role it has in the past because the market cannot capture the uses of media that accomplish that function.

This is not to say that the market should not play a part in the regulation of information production in our society. Congress created copyright law in part as a response to the market failure arising from the public goods aspect of creative and informational works.[283] Without a system of exclusive rights, some authors will not be able to capture the value of the works they create. However, since TPSs may be unilaterally imposed by

---

275. *See id.* at 538-59.
276. *See id.* at 544-47.
277. *Id.*
278. *See id.* at 547.
279. *See id.* at 544-46.
280. *See id.* at 547.
281. *See id.* at 549.
282. *See id.* at 550.
283. *See id.* at 471.

content owners and do not require informed consent, leaving their regulation to the market is cause for concern.

Content owners have little reason to avoid infringing users' rights. Copyright owners, motivated by payment for access to, and use of, copyrighted materials are unlikely to favor careful development and implementation of TPSs. Therefore, courts should scrutinize TPSs that come before them. If a TPS expands the owner's intellectual property rights to limit the user's constitutional use rights, courts should refuse to give it effect. Finally, as the Comment describes in Parts IV.C and IV.D, below, courts should seek to create an incentive scheme that favors development of strong, carefully implemented TPSs.

B. Judicial Delineation of the Public Domain and Fair Use

Although Congress has played a major role in shaping copyright law, judicial opinions have always defined its contours. American courts began defining the public domain shortly after Congress passed the first Copyright Act in 1790.[284] In *Wheaton v. Peters*, the Supreme Court held that the common law copyright—which then existed in perpetuity—was inconsistent with the "limited Times" language of the Intellectual Property Clause.[285] The Supreme Court therefore held that all previous literary rights not expressed in the 1790 Act passed into the public domain upon vesting of federal statutory copyright.[286] Since then, the federal courts have defined the public domain by holding that the copyright grant does not protect ideas, systems,[287] methods,[288] facts,[289] utilitarian objects,[290] titles,[291] plots,[292] style,[293] or federal government works.[294] They have similarly delineated the fair use doctrine.[295]

---

284. Act of May 31, 1790, ch. 15, 1 Stat. 124 (repealed 1834); *see also* Litman, *supra* note 80, 978 n.76.

285. *See* Wheaton v. Peters, 33 U.S. (8 Pet.) 591 (1834); Howard B. Abrams, *Exploding the Myth of Common Law Copyright*, 29 WAYNE L. REV. 1119 (1983). *See also* Litman, *supra* note 80, at 978. Litman has closely traced the judicial development of the public domain; many cases she relies on are noted in this part of the discussion.

286. *Peters*, 33 U.S. (8 Pet.) at 591.

287. Baker v. Selden, 101 U.S. 99 (1879).

288. Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807 (1st Cir. 1995), *aff'd by an equally divided court*, 516 U.S. 233 (1996).

289. Feist Publ'ns, Inc. v. Rural Tel. Serv., 499 U.S. 340 (1991).

290. Mazer v. Stein, 347 U.S. 201 (1954).

291. *See, e.g.*, Weissman v. Radio Corp. of Am., 80 F. Supp. 612 (S.D.N.Y. 1948); Litman, *supra* note 80, at 993 n.169.

292. Nichols v. Universal Pictures Corp., 45 F.2d 119 (2d Cir. 1930).

In subsequent versions of the Copyright Act, Congress has frequently followed the courts' rulings on the limitations imposed on copyright by the public domain and fair use.[296] Courts, then, have been the primary delineators of the scope of the public domain and fair use doctrine. As discussed previously in Part III.A, these aspects of informational and creative works comprise the building blocks of authorship, and consequently speech. Thus, even if the federal judiciary has never explicitly acknowledged this role (or arguably even been aware of it[297]), the courts have always been a primary forum for the shaping of the intersection between intellectual property rights and free speech. In the real world, courts have been responding to a statutory monopoly. However, the limitations they have placed on that monopoly derive not from statutory language, but from concerns about continued creative and informational output and the constitutionally limited nature of intellectual property.[298] Courts must continue to address these concerns as protection of intellectual property shifts from law to technology. In the following sections the Comment offers two approaches the courts should take: first, direct regulation of TPSs on constitutional grounds; second, indirect regulation through the copyright misuse doctrine.

---

293. *See, e.g.*, Franklin Mint Corp. v. Nat'l Wildlife Art Exch., 575 F.2d 62 (3d Cir.), *cert. denied,* 439 U.S. 880 (1978); Litman, *supra* note 80, at 993 n.175.

294. *See, e.g.*, Scherr v. Universal Match Corp., 417 F.2d 497 (2d Cir. 1969), *cert. denied*, 397 U.S. 936 (1970); Litman, *supra* note 80, at 993 n.176.

295. *See, e.g.,* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994); Alfred Bell & Co. v. Catalda Fine Arts, 74 F. Supp. 973, 977 (S.D.N.Y. 1947).

296. *See* 17 U.S.C. § 102(b) (1988) (ideas, systems); 17 U.S.C. §§ 101, 113 (Supp. 2000) (useful articles); 17 U.S.C. § 105 (1994) (federal government works); Litman, *supra* note 80, at 992 n.163.

297. *See generally,* Litman, *supra* note 80.

298. *See, e.g.*, Baker v. Selden, 101 U.S. 99, 104 (1879) ("[T]he teachings of science and the rules and methods of useful art have their final end in application and use; and this application and use are what the public derive from the publication of a book which teaches them. But as embodied and taught in a literary composition or book, their essence consists only in their statement. This alone is what is secured by the copyright."); Nichols v. Universal Pictures Corp., 45 F.2d 119, 122 (2d Cir. 1930) ("[G]ranting that the plaintiff's play was wholly original, and assuming that novelty is not essential to a copyright, there is no monopoly in such a background ['a quarrel between a Jewish and an Irish father, the marriage of their children, the birth of grandchildren and reconciliation']. Though the plaintiff discovered the vein, she could not keep it to herself; so defined, the theme was too generalized an abstraction from what she wrote. It was only a part of her 'ideas.'"); Feist Publ'ns, Inc. v. Rural Tel. Serv., 499 U.S. 340, 346 (1991) ("[T]he Court made it unmistakably clear that [the terms "authors" and "writings"] presuppose a degree of originality . . . . The originality requirement is constitutionally mandated for all works.").

C. Direct Judicial Regulation of TPSs

A court directly regulating TPSs would enjoin the use of a particular TPS if it impermissibly restricts users' rights. The constitutional analysis of the TPS would rely on the same facts about available access and use as a court would in evaluating the broad reading of the DMCA.[299] There, the propriety of the anti-circumvention provisions was a function of whether the technology they protected was overly restrictive of users' rights. Here, if a TPS prevents fair use and access to the public domain, the effect on speech rights of users is no less significant. Therefore, the judiciary must protect the public domain and fair use, whether impinged upon by technology-derived statutory rights or the technology itself. Injunctions against the use of particular TPSs—notwithstanding the possible state action objections discussed below—would be an appropriate means for the courts to preserve users' rights.

The constitutional question in these cases differs slightly from that in the DMCA cases. The justifications discussed in Part III.A for TPS-based restrictions of fair use and the public domain[300] are all diminished for individual content owners in comparison to the government, because the magnitude of each concern is smaller where only single producers are concerned. On the other hand, they still can rely on the argument that producers of intellectual property have a right to protect it. The underlying sense that people's product is their own, that intellectual property is its owner's to do with as he pleases, has much intuitive appeal.[301] It may in fact be one consideration keeping courts from squarely addressing the implications of TPSs for users' rights.

It is the scope of that intellectual property, however, that is the issue here, not the ownership. Once an author publishes a work, the law has always implied consent to reasonable use as necessary for constitutional promotion of "Progress."[302] TPSs can prevent this reasonable use. But a content owner should not receive a stronger right to monopolize published media simply because he has published his work in a digital environment.

---

299. *See supra* Part III.

300. These justifications were: unwillingness to produce content on the Internet, the importance of the copyright industry to the domestic economy, and the difficulties of tracking copyright infringement on the Internet. *See supra* Part III.A.

301. *Cf.* William W. Fisher III, *Property and Contract on the Internet,* 73 Chi.-Kent L. Rev. 1203 (1998) (discussing the Lockean justification for intellectual property as a natural property right to the fruits of one's labors).

302. *See* Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 549 (1985).

The desire and newfound ability to adopt overly restrictive fencing of published material does not justify restriction of users' constitutional rights. TPSs cannot stand where they impermissibly restrict users' rights.

The state action doctrine presents the most serious obstacle to direct regulation of TPSs. This doctrine holds that the Constitution's limitations apply only to government conduct.[303] TPSs, as private digital fences, are arguably beyond the reach of the courts because the government is not intervening on content owners' behalf. Paul Schiff Berman has recently discussed the particular state action issues raised by constitutional discourse in cyberspace.[304] The typical criticisms of the doctrine focus on the pervasive part played by law in every aspect of public and private lives.[305] Negative decisions to allow behavior, i.e., the absence of regulation, play as much of a role in shaping society as government intervention to proscribe actions.[306] The distinction between legally allowed and prohibited behaviors is a product of state decisionmaking, not an intrinsic characteristic of the behavior itself. It is therefore incoherent to limit constitutional discourse to acts of government intervention.[307]

With regard to digital fences, it makes little sense to say Congress may not create an unlimited copyright grant, but must allow content owners to do so using TPSs. Government inaction in the face of overly restrictive TPSs shapes our information society just as much as an unlimited legal monopoly in digital media would.

However, there is a strong appeal to the idea that people should be able to control what they produce.[308] Even if it is incoherent, the pub-

---

303. For the genesis of the state action doctrine, see The Civil Rights Cases, 109 U.S. 3 (1883). At least one court has applied the doctrine to a question of an Internet service provider limiting its users' speech. *See* Cyber Promotions, Inc. v. Am. Online, 948 F. Supp. 436 (E.D. Pa. 1996) (holding AOL to be a private actor not subject to the First Amendment's strictures); Paul Schiff Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private Regulation,"* 71 U. COLO. L. REV. 1263, 1283 (2000).

304. Berman, *supra* note 303, at 1266.

305. *Id.* at 1278 (citing Morris Cohen, *Property and Sovereignty*, 13 CORNELL L.Q. 8 (1927)).

306. "[A]ll private actions take place against a background of laws. These laws embody state decisions either to permit or proscribe behavior. For example, legally permitted actions are permitted solely because the state has made a decision not to prohibit those actions. If such actions ultimately cause harm, it is therefore difficult to say the state has played no role." Berman, *supra* note 303, at 1279.

307. *Id*.

308. *Cf. supra* note 301.

lic/private distinction intuitively resonates with notions of freedom in our society. Thus the incoherence argument is not enough to overcome the state action doctrine alone. Nevertheless, fundamental values underlying the limited nature of intellectual property do not cease to be of importance when private action implicates them. Lawrence Lessig has noted:

> If code functions as law, then we are creating the most significant new jurisdiction since the Louisiana Purchase, yet we are building it just outside of the Constitution's review. Indeed, we are building it just so that the Constitution will not govern—as if we want to be free of the constraints of value embedded by our traditions.[309]

As technology supplants law as the primary means of media protection on the Internet, private actors are likely to threaten constitutional values with their actions. Furthermore, the threats will increase not only in number but also in magnitude as new technologies protected by TPSs become a more important source of information in society. Thus, preserving fair use and the public domain against private, not government action, will be of crucial importance in the digital age.

Berman offers a "constitutive constitutionalism" argument to circumvent the state action doctrine. His theory focuses on the symbolic role the Constitution plays in cultural and societal discourse.[310] Because it is a document constitutive of the people, courts adjudicating constitutional issues write the collective story of the people.[311] The story supplies a structure for citizens to make judgments about the shape of their society.[312] Society thereby articulates fundamental values through constitutional decisionmaking on a collective level with strong symbolic power.[313] A failure to engage in a discussion of fundamental speech values when TPSs implicate them silently writes them out of the story. Conversely, acknowledging the issue triggers the courts' institutional role as deliberative fora for

---

309. LESSIG, *supra* note 29, at 217.

310. Berman, supra note 303, at 1290; *see also* Reva B. Siegel, *Collective Memory and the Nineteenth Amendment: Reasoning About "The Woman Question" in the Discourse of Sex Discrimination*, *in* HISTORY, MEMORY, AND THE LAW 131 (Austin Sarat & Thomas R. Kearns eds., 1999); Robert M. Cover, *Nomos and Narrative*, 97 HARV. L. REV. 4 (1983).

311. *See* Siegel, *supra* note 310, at 134; Berman, *supra* note 303, at 1293.

312. *See* Siegel, *supra* note 310, at 134; Berman, *supra* note 303, at 1293.

313. *See* Berman, *supra* note 303, at 1293.

fundamental values.[314] Constitutional interpretation here can be valuable because it will require courts, through principled decisionmaking, to harmonize the new face of intellectual property law on the Internet with the two-hundred year story of fair use and the public domain.[315] In other words, it would be best for courts—the primary delineators of the doctrines—to continue the discussion they began in 1790. Constitutional discourse can ensure the choices made are well thought-out and reflect the balance of interests of society as a whole. Reliance on the state action doctrine to take the issue away from courts cuts off a vital forum for formulation of our information law. Furthermore, the fact that the current statutory landscape protects TPSs without regard to their restrictiveness confirms that the public—who stands to lose the most if the public domain is enclosed—cannot expect much from the legislature.[316] The courts are the public's only other option.

Apart from the state action doctrine, there is nothing about regulation of TPSs to suggest that the topic is beyond judicial competence. The technical issues raised by TPS regulation are substantially similar to those involved in enforcing the DMCA. Technological restrictions on fair use and enclosure of the public domain are as easily susceptible to evidentiary proof and disproof as circumvention and devices used to circumvent. Further, it is just as much within Congress's power to regulate locks as lockpicks. Accordingly, it is also within the courts' power to enforce a hypothetical statute limiting the permissible scope of protection by TPSs. Thus, there is nothing inherent in programs that fence that makes them less regulable than programs that cut fences. If the courts can overcome the state

---

314. *See* Owen Fiss, *The Supreme Court, 1978 Term—Foreword: The Forms of Justice*, 93 HARV. L. REV. 1, 10 (1979) (implying that courts are more "ideologically committed [and] institutionally suited to search for the meaning of constitutional values" than legislatures); Berman, *supra* note 303, at 1298.

315. *See* Ronald Dworkin, *The Moral Reading and the Majoritarian Premise*, *in* FREEDOM'S LAW: THE MORAL READING OF THE AMERICAN CONSTITUTION 1, 2, 30 (1996) (Courts must seek "the best conception of constitutional moral principles . . . that fits the broad story of America's historical record;" "Individual citizens may be able to exercise the moral responsibilities of citizenship better when final decisions are removed from ordinary politics and assigned to the courts, whose decisions are meant to turn on principle, not on the weight of numbers or the balance of political influence."); Berman, *supra* note 303, at 1299.

316. *Cf.* Litman, *Copyright Noncompliance, supra* note 8, at 240-41 (showing that users are not among the represented stakeholders in the creation of laws protecting media).

action obstacle, then there is nothing intrinsic to TPSs that places them outside the purview of the courts.

Should courts decide to address TPSs directly, a ruling that a particular TPS unconstitutionally restricts users' rights would have a significant impact on the direction in which the technology moves. Content owners would face two development paths: either create weak TPSs that do not infringe users' constitutional rights, or opt out of the intellectual property system by relying solely on strong and restrictive TPSs.[317] The constitutional line drawn by courts would necessarily leave at least a small range of TPSs beyond the protection of law. Because perfect technical protection is impossible, there would be an area of tremendous risk for content owners in which neither law nor technology could reliably guard their media. Therefore the risks inherent in choosing the all-technology route would probably lead most content owners to favor a constitutionally acceptable TPS that can be backed by law. Strong TPSs will be perfectly acceptable, even desirable, as long as they do not overly restrict users' rights. As in the constitutional evaluation of the DMCA in Part III, courts must carefully distinguish between the strength of the TPS and its restrictions on users' rights because only the latter are constitutionally problematic. A well-reasoned ruling would therefore give no disincentives to create TPSs that are extremely difficult to crack, provided they allow for constitutionally protected users' rights.

What such a TPS might look like is still unclear. It is unlikely that the court would provide specific guidelines for what the technology can and cannot do, given the technologies' complexities and the courts' general distaste for judicial legislation. As noted earlier, TPSs will always prevent some noninfringing uses of protected material. Even at their best TPSs designed to allow fair use will only be able to identify those uses which are always or nearly always fair.[318] Content owners could code a gateway for these limited uses directly into the digital fence. More often, though, fair use requires a complex case-by-case statutory analysis, which will be beyond the capacity of computers until they develop human judgment abilities. It therefore seems likely that to effectively preserve users' rights

---

317. Those content owners who completely opted out of federal protection could still turn to state contract law, of course. But contracts are subject to preemption under 17 U.S.C. § 301 where they conflict with copyright law. *See* Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CAL. L. REV. 111, 157 (1999).

318. *See supra,* note 30.

and to maintain the public domain, content owners will have to use a system external to the TPSs. Dan L. Burk and Julie Cohen argue that combined with the limited coded fair use defaults sketched above, an escrow system under which users apply to a trusted third party for keys to circumvent TPSs could help solve the problem.[319] Whatever the eventual solution, the courts' delineation of fair use and the public domain in the digital environment is an essential first step in resolving the problem of TPSs.

D. Indirect Regulation through the Copyright Misuse Doctrine

Copyright misuse, an issue not yet considered by the courts in the context of TPSs, may provide an effective means for judicial discussion and regulation of TPSs. The doctrine renders a copyright unenforceable if the owner has attempted to extend or broaden the scope of the copyright monopoly in licensing or enforcement.[320] The doctrine developed recently, having only seriously been considered in district courts for the past ten years.[321] As such, its boundaries are still fuzzy.[322]

The principle of the doctrine is that courts should not play a role in extending the copyright monopoly beyond its statutory bounds.[323] Copyright misuse does not require a violation of antitrust laws.[324] Nor does it require the defendant to have actually been subject to or affected by the restriction that exceeded the scope of copyright.[325] So far, courts have found misuse where content owners: 1) used a copyright license clause precluding development of competing software for ninety-nine years;[326] 2) used a li-

---

319. *See* Burk and Cohen, *supra* note 30.

320. *See* Lemley, *supra* note 317, at 151.

321. *See id.* at 152.

322. For example, defendants in the *Napster* case argued the record companies' attempt to enforce their copyrights was misuse on the ground that it would have the effect of controlling what other copyright holders chose to do with their media. Although the argument holds some intuitive appeal, as a matter of law it is hard to see why plaintiffs should be precluded from enforcing their copyrights merely because the technology being used to violate them is incapable of preventing only selected uses. *See* A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 923 (N.D. Cal. 2000).

323. *See* Lemley, *supra* note 317, at 153.

324. *See* DSC Communications Corp. v. DGI Techs., 81 F.3d 597, 601 (5th Cir. 1996).

325. *See* Lasercomb Am., Inc. v. Reynolds, 911 F.2d 970, 979 (4th Cir. 1990). Mark Lemley has criticized such broad remedial application of misuse in the patent context. *See* Mark A. Lemley, Comment, *The Economic Irrationality of the Patent Misuse Doctrine*, 78 CAL. L. REV. 1599, 1614-20 (1990).

326. *See Lasercomb*, 911 F.2d 970.

cense clause precluding use of a competing work;[327] 3) sued to prevent temporary copying needed to make competing hardware interoperable with plaintiff's copyrighted operating system;[328] and 4) similarly attempted to expand their copyright.[329] Application of the doctrine to TPSs would be simple in principle: use of any technological barrier that effectively broadens the content owner's rights beyond the constitutional balance would render the copyright unenforceable.

Copyright misuse is an appropriate tool for dealing with TPSs for several reasons. Pragmatically, it could address the interests of users without having to deal with collective action problems. It is unlikely that any of the millions of noncommercial home users will have sufficient incentive or capacity to bring a lawsuit. As such, they will probably forego unauthorized uses. If one is sued for infringement, however, copyright misuse can be a powerful defense. Next, because copyright misuse directly implicates questions about the scope of intellectual property, it will highlight the question of what constitutional balance is appropriate for copyright on the Internet. In addition, because it is merely a refusal to set in motion governmental process, rather than action against a private party through direct regulation of TPSs, copyright misuse will allow the court to undertake a constitutionally-grounded analysis without facing the state action dilemma. Finally, copyright misuse will force content owners to choose whether or not to opt out of copyright—the same decision that direct regulation on constitutional grounds forced in the previous section—which may be quite dangerous if TPSs cannot protect works satisfactorily on their own. Content owners would still have recourse to state contract law to reinforce their technological fences, but courts may render the contracts unenforceable on similar facts to those warranting a finding of copyright misuse.[330]

The major limitation of copyright misuse is that it is only a threat to content owners who are seeking to safeguard works protected by copy-

---

327. *See* Practice Mgmt. Info. Corp. v. Am. Med. Ass'n, 121 F.3d 516 (9th Cir. 1997).

328. *See* DSC Communications Corp. v. DGI Techs., 81 F.3d 597 (5th Cir. 1996).

329. *See* Lemley, *supra* note 317, at 153 n.195 (collecting cases). One court stated "it is copyright misuse to exact a fee for the use of a musical work which is already in the public domain." F.E.L. Publ'ns, Ltd. v. Catholic Bishop, 214 U.S.P.Q. (BNA) 409, 413 n.9 (7th Cir. 1982).

330. *See* Lemley, *supra* note 317, at 157 (noting that copyright misuse cannot be contractually waived, and so may defeat a copyright claim, but will not of its own force render a contract unenforceable).

right. It will thus have no bearing on the development of TPSs by creators of currently uncopyrightable collections of information. Even holders of thin copyrights would be less deterred than owners of expression entitled to full legal protection. Thus, copyright misuse may be of limited use in preserving the public domain on the Internet. On the other hand, it may be quite valuable as a means of ensuring fair uses of copyrighted works that are available in the digital environment.

The powerful threat of nullifying the content owner's copyright would provide them with a strong incentive to ensure the availability of fair use to users who have lawfully acquired copies. This, however, highlights a problem with the doctrine in general: making the copyright completely unenforceable is a harsh remedy. Judges may therefore be reluctant to apply copyright misuse to TPSs.[331]

Finally, as with direct judicial regulation, copyright misuse does not address how content owners should develop strong, but not overly restrictive TPSs. As discussed in the previous section, trusted third party involvement will likely be necessary to accomplish this end. Ultimately, like direct regulation, controlling the use of TPSs with the copyright misuse doctrine will not solve the problem of how to preserve fair use and the public domain. It will, however, provide incentives to content owners and the legislature to figure out a better solution than the one currently in place.

V. CONCLUSION

The specter of a "pay-per-use" society has not yet materialized. Informational and creative works that are available in digital form still, for the most part, exist in non-digital form as well. But Congress and the courts have not prepared an adequate framework for dealing with the apparition if and when it becomes a reality. The courts and the Register of Copyrights have read the DMCA to convey a right to enforce any TPS, regardless of how restrictive it is on users' constitutional rights. Development and use of TPSs themselves are currently in the hands of content owners, beyond serious consideration by the legislature or the judiciary. These two problems weave together a welcome mat for restrictions on fair use and foreclosure of the public domain. Society needs

331. However, the freedom with which it has been used since its inception may indicate otherwise. *See, e.g.,* Practice Mgmt. Info. Corp. v. Am. Med. Ass'n, 121 F.3d 516 (9th Cir. 1997) (finding, without any inquiry into antitrust issues, copyright misuse for inclusion at the plaintiff licensee's request of a contract provision requiring exclusive use of defendant licensor's copyrighted work).

foreclosure of the public domain. Society needs better wards against diminishing access and availability of digital media.

Since the legislature has already spoken, the next step is for the courts to create a better framework to protect users' constitutional rights. If users find their rights dwindling under the current legal regime, they must be able to turn to the judiciary to protect their interests. Courts must recognize that the DMCA—if broad interpretations so far are inevitable—creates, in some cases, a legal right to silence the constitutionally protected speech of others. Content owners' justifications for invoking a governmental process to effect this right are speculative and insufficient. Accordingly, if compelled by the statute to enforce a TPS that restricts users' constitutional rights, courts should refuse to enforce it and strike down the anti-circumvention provisions. Similarly, since the legislature has declined to consider the restrictions on constitutional speech rights that TPSs may create, courts should evaluate and regulate digital fences directly on constitutional grounds or indirectly through the copyright misuse doctrine. Content owners cannot be allowed to expand their monopolies at the expense of the public interest simply because technology is supplanting law as the primary means of protection in the digital environment.

Finally, in judicial decisions and future legislation, lawmakers must provide content owners with proper incentives to develop TPSs that are strong, but not overly restrictive of users' rights. Content owners have not yet created such TPSs, though some commentators have made suggestions as to how more careful fencing might be implemented. In all likelihood, the market will ultimately solve the problem. The key is that unless given proper limitations, the market will not work toward a solution that accounts for users' interests. And, given today's legal landscape, it is clear that judicial acknowledgment and action on the constitutional issues raised by restriction of fair use and enclosure of the public domain on the Internet will be a first crucial step on the path toward the answer.