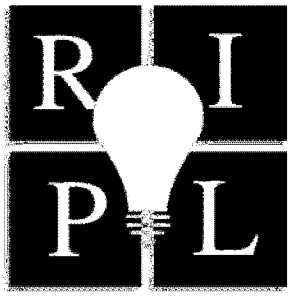
THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW



COPYRIGHT & PRIVACY – THROUGH THE PRIVACY LENS

NOVEMBER 18, 2004

JULIE E. COHEN, DAVID E. SORKIN AND PETER P. SWIRE

ABSTRACT

What legal tools do privacy advocates have available to defend an individual's right to privacy? How far does this right go? How should these rights be defended—or if necessary—curtailed? What is the role of Government, of the practicing bar and of academics?

Cite as Julie E. Cohen et al., *Copyright & Privacy – Through the Privacy Lens*, 4 J. MARSHALL REV. INTELL. PROP. L. 273 (2005).

COPYRIGHT & PRIVACY – THROUGH THE PRIVACY LENS*

NOVEMBER 18, 2004

JULIE E. COHEN, DAVID E. SORKIN AND PETER P. SWIRE

I. PETER P. SWIRE

PROF. SWIRE:[1] My talk today is about privacy law and First Amendment content. The question for my talk is: will they—roughly speaking, the government—know what the users have agreed to say? The answer is: there is a robust history in the United States of legislative problems in limiting content. What we have is a substantial history of the law stepping in to put limits on what the government can see about what a person writes or reads. This talk proposes that good procedures can be created for future surveillance of content. The overview of the talk: there will be a section about how there were multiple statutes, long before the creation of peer-to-peer ("P2P") technology, which created procedures and privacy protections for First Amendment content; the *Verizon* case was an example for procedural protections.[2] Next, we will revisit the reasons for privacy protections that have grown up around the use of First Amendment content. There is a tradition in the

---

* Adapted from presentations delivered on November 18, 2004 at the Standard Club in Chicago, Illinois as part of a conference entitled *Copyright & Privacy: Collision or Coexistence?* and hosted by The John Marshall Law School Center for Intellectual Property Law. Please note that the statements made in this article are based upon a transcript of the aforementioned conference and are not necessarily verbatim. In addition, while efforts have been made to ensure accuracy, the nature of the transcription process is such that the statements made in this article are subject to errors and omissions.

[1] Peter P. Swire is Professor of Law and John Glenn Scholar of Public Policy Research at the Moritz College of Law of the Ohio State University in Columbus, Ohio. Prof. Swire is Director of the law school's Washington, D.C. summer program. Prof. Swire also serves as a consultant to the law firm of Morrison & Foerster LLP, with a focus on medical privacy issues.

From 1999 until January 2001, Prof. Swire served as the Clinton Administration's Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that position, Prof. Swire coordinated Administration policy on the use of personal information in the public and private sectors. Prof. Swire was White House coordinator for the proposed and final HIPAA medical privacy rules, and played a leading role on topics including financial privacy, Internet privacy, encryption, public records and privacy, e-commerce policy, and computer security and privacy.

Prof. Swire co-authored the book *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, which was published by Brookings in 1998. Prof. Swire has published extensively and is quoted frequently in the national and international press. Many of Prof. Swire's writings appear at http://www.peterswire.net. With Lawrence Lessig, Prof. Swire serves as Editor of the Cyberspace Law Abstracts of the Social Science Research Network.

Prof. Swire graduated *summa cum laude* from Princeton University and in law school was a Senior Editor of the *Yale Law Journal*. Prof. Swire received a Rotary Fellowship to study European Community Law in Brussels in 1981–1982 and clerked for Judge Ralph K. Winter, Jr., of the Second Circuit Court of Appeals. Prior to becoming a professor of law, Prof. Swire practiced in the Washington, D.C. office of Powell, Goldstein, Frazer & Murphy from 1986–1990.

[2] RIAA v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 347 (2004).

United States, and an understanding of the need and the process, to limit abuse by those who seek surveillance.

What I am going to do now is go through some statutes that were on the books long before the privacy problems of the copyright wars. The first statute, not chronologically, but the most familiar, is the Video Privacy Protection Act that was passed in 1988.[3] As many of you know, a reporter got hold of Judge Bork's video records when he was being nominated to the Supreme Court. The reporter was probably trying to get information that was embarrassing, that Judge Bork had seen some inappropriate films or something of that nature. What I have heard, although I have not verified this, was that it was a lot of John Wayne movies. You can be a good Republican and believe in John Wayne, and that is apparently what he did. The law passed almost instantly. As a result we ask the deep and probing public-choice question: why would this have been?

My proposal is that quite a number of Senators had seen movies their constituents might not like. It might be embarrassing to have that out there. That hypothesis in some ways was confirmed, or at least repeated, when Congress considered the Financial Privacy Law in 1999.[4] What is interesting is that what we see here is a mechanism for why privacy protections for First Amendment content have more friends in the legislative process than you may think. When we look at the privacy laws, we see quite strict rules. There is an opt-in rule before the video store can disclose what you have rented.[5] Court orders are quite strict. In the context of copyright battles, court orders shall issue only with prior notice to the consumer and only if the agency shows there is probable cause to believe that the records are relevant to a legitimate law enforcement inquiry.[6] That is probable cause with prior notice—a whole bunch of due process. Beyond that, the court is specifically told it can quash or modify these orders if the amount of records or information in the records requested is voluminous in nature.[7] And there is even more protection. Information or records obtained in a manner other than as provided in the Video Privacy Act shall not be received into evidence in any trial hearing, et cetera.[8] There is a very wide suppression rule if somebody somehow gets the video records: they cannot use them in court.[9] Remember, this is before 1988; before we knew how to spell P2P.

There are other statutes which are similar. In fact, four years prior, in the Cable Communications Policy Act of 1984,[10] we saw another set of strict rules that limited anybody from finding out what pay-per-view television shows you received.[11] If you get the Playboy® channel, it is a violation of federal law for the cable company

---

[3] Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C. § 2710 (2000)).

[4] Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12, 15 U.S.C.).

[5] 18 U.S.C. § 2710(b)(2)(D)(i) (2000).

[6] *Id.* § 2710(b)(3).

[7] *Id.*

[8] *Id.* § 2710(d).

[9] *See id.*

[10] Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (codified as amended in scattered sections of 47 U.S.C.).

[11] 47 U.S.C. § 605(a) (2000).

to tell anybody about it. There is an annual notice to the customers about their personal information.[12] There is an opt-in provision which requires prior written or electronic consent before anything about the content of your viewing can be divulged.[13] There is a lesser opt-out provision applicable to information contained in financial institutions' customer lists.[14] There is a liquidated damages provision which says a hundred dollars per day per customer or a thousand dollars total, whichever turns out to be greater, plus actual damages, plus punitive damages, plus attorney's fees.[15]

How about court orders? How easy is it to find out what Prof. Swire is watching on television? The answer is: not very easy. There has to be clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and the information has to be material.[16] In addition, the subject of the information is afforded the opportunity to appear and contest any such claim.[17] Before you see anything about my cable records, you have to go through this quite serious procedure.

Another similar law is the Privacy Protection Act of 1980 that has to do with publishers, giving special protections for the people who publish content.[18] There was a Supreme Court case called *Zurcher v. Stanford Daily* that said there were no Fourth Amendment protections when the government got access to various records connected to a student paper at Stanford.[19] Right after that, Congress responded saying there has to be a full search warrant for records held by publishers.[20] These broad rules saying you cannot get these records unless you get a full search warrant very possibly apply to people who are website publishers. Notwithstanding any other law, it shall be unlawful for a government officer in connection with investigating a criminal offense to search for any work product materials possessed by a person. Who is a publisher? A publisher is someone who reasonably believes he has a purpose to disseminate to the public a newspaper, book, broadcast or other similar form of public communication.[21] If you are involved in disseminating this First Amendment content, the government has to get a search warrant, which is pretty strict, before they enforce any intellectual property or criminal laws.[22] If somebody wants to engage in a search procedure, they are going to have to specifically overrule the Privacy Protection Act or else live with the strict terms of that law.

There are even more rules on content about what you say, what you hear or what you read. For instance, the content of telephone calls and the content of e-mails also has a number of fairly strict legal protections. Notably, Title III of the 1968 crime law sets very strict rules before the government can wire-tap your phone calls

---

[12] *Id.* § 551(a)(1).

[13] *Id.* § 551(b)(1).

[14] 15 U.S.C. § 6802(b) (2000).

[15] 47 U.S.C. § 551(f)(2).

[16] *Id.* § 551(h).

[17] *Id.*

[18] Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (codified as amended at 42 U.S.C. § 2000aa, aa-5, aa-6, aa-7, aa-11, aa-12 (2000)).

[19] Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

[20] 42 U.S.C. § 2000aa(a).

[21] *Id.*

[22] *See id.*

or put bugs in and listen to your conversations.[23] Those provisions were extended in 1986 to include electronic communications, including your e-mails, et cetera.[24] As a result, (subject to a case called *Councilman*, which is a separate thing that we are not getting into today), interception of e-mails gets the same standards of protection as interception of phone calls.[25] There was an understanding right at the beginning of the e-mail age and the web age that we needed to have protection of content.

Also in 1986 there was something called the Electronic Communications Privacy Act, which raised the standard for protection beyond what existed before.[26] When the content is what you hear, what you say or what you write, there are fairly strict protections. The rules are much more lenient when there is no content. Trap and Trace Rules have to do with phone calls; specifically, with what phone numbers you dial.[27] This is not the content of what you said, it is just the number you dialed. Those rules are not as strict.

Also, in a related area, the Telecommunications Act of 1996 provides that your phone call records can only be shared with other people subject to consumer choice; subject to an opt-out provision.[28] If the records reveal something about who you communicate with, there are legal rules in place that place limits on what can be revealed.

To sum up, we have seen the Video Act, the Cable Act, the publisher's rule and Electronic Communications Protection Act and how these laws relate to the First Amendment. This was the list before we got to P2P.

Now, to the *Verizon* case.[29] Some of you know that I was the expert declarant for Verizon in the district court in that case. I did not write the word copyright or say anything about copyright, but I did say some things about appropriate privacy and due process. My concerns in that case were about what I called "the new spam." Those concerns relate to the very, very bad procedures that were provided for under § 512(h).[30] As many of you know, § 512(h) required a very minimal showing to get a subpoena. It required some basis for thinking there might be an infringement somewhere. It did not say that in those words, of course, but it was a minimal showing all the same. There was also really no protection against fraud. You did not have to be a member of the bar to sign the affidavit, you did not need a bar number or even be subject to any professional discipline. The signature could be a paralegal—it could even be a fake name. The information could be sent to a post office box somewhere in a strip mall. It did not even have to be a real company. So, as you can see under the rules of § 512(h), as the recording industry saw it, any website could take any IP address. All the companies had to do was submit one of these § 512(h) subpoenas, and Verizon, or whoever, would have to hand over the name, address and phone number of its subscribers. If the website was a porn site trying to embarrass the customers and engage in blackmail, or if it was a marketing

---

[23] 18 U.S.C. §§ 2510–2520 (2000).

[24] *Id.* § 3121.

[25] *Id.* § 2510.

[26] *Id.*

[27] *Id.* § 3121–3124.

[28] 541 U.S.C. § 253 (2000).

[29] RIAA v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 347 (2004).

[30] 17 U.S.C. § 512(h) (2000).

site that wanted to get the full name and address list of people who happen to stop by the website, the process for getting that information was trivial. All you had to do is use the IP address; that is the way the internet works. You take the IP address, track it back through Verizon or another ISP, and you get a name, address and phone number of the subscriber. There is no way to stop it under § 512(h). This is clearly not a good way to protect people from being tracked down from any website they go to.

Now, as Mr. Oppenheim said today, the D.C. Circuit decided *Verizon* on boring statutory grounds.[31] There was no mention of policy anywhere in the opinion. However, I think, having read the papers and watched the proceedings, the court was fully aware of these painfully weak procedural protections. We knew that bad procedures create a threat to privacy. As I mentioned earlier, anybody could find out who surfed at any website. The threat to the First Amendment—the chilling effect on speech that would result if I could be tracked down by simply looking at an inappropriate site or a site with political values—causes an even greater threat to these values. The D.C. Circuit did the easy thing. It interpreted the statute so that it did not have to address the lack-of-due-process problems, the First Amendment problems or the privacy problems. If it had ruled the other way, it would have had to write a big long opinion about why the decision is consistent with due process and the First Amendment. The D.C. Circuit simply took the easy way out.

I would like to conclude by giving you a few thoughts about how to organize this. For video, cable, publishers, phone calls and e-mails in the United States, we have seen repeated (and often quite strict) statutory protections against surveillance when that surveillance involves First Amendment content—what you see, what you say, what you hear. We have seen high standards for court orders long before there was any worry about downloading songs online. In addition, we have seen prior notice to subscribers to let them contest the divulgence of their personal information. We have also seen that limits on burdens and discovery requests to the intermediaries do not have to comply and be the playthings of the enforcement entities. This was all in place before P2P. The kind of things we are getting in these *John Doe* suits—the kind of due process that is now being asked for—was all there for First Amendment content long before it had anything to do with the current debates around P2P.[32]

So, learning from this history is a matter of how America seems to work—what is likely to happen next? There is a striking, and I think often overlooked, pattern of protection in U.S. law. We should remember that the behavior of members of Congress is on the line here. Everything they do is also subject to disclosure. They are not all perfect and careful at all times. So I think going forward, it is quite possible that there will be significant procedural protections before First Amendment content is turned over to enforcers.

Looking ahead as a matter of prescription, I am going to be really radical here, but I think due process should be in place. I think there should be protections against fraudulent and abusive enforcement, which § 512(h) lacked. I think innocent defendants should be able to win without suffering crushing costs.

---

[31] *See* Sarah B. Deutsch et al., *Copyright & Privacy – Through the Copyright Lens*, 4 J. MARSHALL REV. INTELL. PROP. L. 212, Part II (2005).

[32] *See id.* Part III (discussing the due-process issues and the procedures involved in the recording and motion picture industries' *John Doe* suits).

The main lesson from today is that privacy—discussed here generally—does not prevent well-founded prosecution. When you have probable cause to build your case, you should be and are able to get the job done as an enforcer. However, privacy protections have been and will be quite substantial for sensitive First Amendment content. To conclude, in the copyright wars that we have heard about in the debate today, privacy protections should be understood as meaning that there is due process before a privacy intrusion occurs. Thank You.

II. JULIE E. COHEN

PROF. COHEN:[33] For those of you who know me, it will come as no surprise that I am going to be slightly less optimistic than Prof. Swire. That usually happens. However, it will come as a surprise that I am not going to talk about Digital Rights Management ("DRM") much. Instead, I am going to talk about possible trajectories for legal change in the area of user privacy. Some of the procedures that we have heard a lot about today, particularly the governing subpoenas issued pursuant to § 512(h)[34] or in *John Doe* lawsuits, do not seem to value user privacy very highly. One therefore might think of user privacy as a lost cause. Alternatively, one might think of user privacy as a potential new paradigm in search of a framing conception.

It used to be, in the good old days of copyright law, that no theory of the ordinary user was needed either with respect to privacy or more generally with respect to what counted as ordinary, lawful uses of content. There were direct infringement suits against large commercial organizations. There were occasional indirect infringement lawsuits predicated on direct infringement by ordinary users. Even then, though, there was little interest in knowing much about ordinary users and certainly no interest in suing them.

Today, things are very different. With apologies to McDonald's, today we see thousands and thousands sued. From Mr. Oppenheim's slides, I noticed that my RIAA numbers are low.[35] Nobody knows how many suits the MPAA just filed.[36] In

---

[33] Julie E. Cohen is Professor of Law at Georgetown University Law Center in Washington, D.C. Prof. Cohen teaches and writes about intellectual property law and data privacy law, with particular focus on computer software and digital works and on the intersection of copyright, privacy and the First Amendment in cyberspace. Prof. Cohen is co-author of *Copyright in a Global Information Economy* (Aspen Law & Business 2002) and is a member of the Advisory Boards of the Electronic Privacy Information Center and Public Knowledge. From 1995–1999, Prof. Cohen was Assistant Professor of Law at the University of Pittsburgh School of Law in Pittsburg, Pennsylvania. From 1992–1995, Prof. Cohen practiced with the San Francisco firm of McCutchen, Doyle, Brown & Enersen, where she specialized in intellectual property litigation. Prof. Cohen received her A.B. from Harvard-Radcliffe and her J.D. from the Harvard Law School, where she was a Supervising Editor of the *Harvard Law Review*. Prof. Cohen is a former law clerk to the Honorable Stephen Reinhardt of the U.S. Court of Appeals for the Ninth Circuit.

[34] 17 U.S.C. § 512(h) (2000).

[35] *See* Deutsch at al., *supra* note 31, Part II.

[36] *See, e.g.*, Twentieth Century Fox Film Corp. v. Does 1–9, No. 04CV02006 (D.D.C. filed Nov. 16, 2004); New Line Prods., Inc. v. Does 1–18, No. 04CV01578CAS (E.D. Mo. filed Nov. 16, 2004); Twentieth Century Fox Film Corp. v. Does 1–12, No. C04-4862 (N.D. Cal. filed Nov. 15, 2004); Metro-Goldwyn-Mayer Pictures Inc. v. Does 1–10, No. 04CV2005 (D.D.C. filed Nov. 15, 2004); Universal City Studios Prods. LLLP v. Does 1–8, No. 04CV3343 (N.D. Ga. filed Nov. 15, 2004);

addition, there are the DirecTV suits against all the folks who purchased smart card reader equipment.[37]

Also emerging is a selective and very strategic pattern on the part of the major content industries of avoiding disputes with certain categories of end users who might be in a position to raise facially plausible and equitably compelling fair use claims. Such lawsuits, if allowed to proceed, might create law on the books of a very different sort.

Finally, we are seeing that precise information about users is increasingly critical to the outcome of indirect infringement lawsuits. To the extent that there is a circuit split between the Seventh and Ninth Circuits on the legality of P2P file sharing, it relates to the question of how much knowledge, or control, the equipment or service vendor is obliged to design into the software at the outset.[38] This question also arose in the ReplayTV litigation, in which a discovery magistrate issued a very controversial order requiring ReplayTV's manufacturer, Sonic Blue, to start keeping records of what users were doing to facilitate investigation of the claimed infringements.[39] The District Court overturned that order, and the litigation was later terminated by bankruptcy, sale of the business, and redesign of the equipment.[40] However, the question about design obligations remains, and may be squarely raised if the Supreme Court grants certiorari in *Grokster*: What kinds of things do you need to know about your users?[41] More generally, what obligations, if any, does the designer of P2P software have to design for control? Quite often with control comes more knowledge.

In this environment, I submit, a theory of the ordinary user is urgently needed. The privacy statutes that we have talked about, without exception, were framed in an environment in which people were not thinking about civil copyright infringement liability or any other potential conflict between privacy and economic rights. They were thinking within a very traditional First Amendment framework, about freedom from government-driven harassment. In general, courts and policymakers have found the arguments about the need to maintain a balance between privacy and economic rights less compelling.

What we are seeing as a result of this mismatch is that in the civil copyright infringement context the privacy interests of users are framed in such a way that they fall automatically in the face of a prima facie case of civil infringement of economic rights. If we look at the DMCA subpoenas which cover hosted material,

---

Disney Enters., Inc. v. Does 1–19, No. 04CV3344 (N.D. Ga. filed Nov. 15, 2004); Paramount Pictures Corp. v. Does 1–19, No. 04CV3345 (N.D. Ga. filed Nov. 15, 2004); Universal City Studios Prods. LLLP v. Does 1–53, No. 04CV9000 (S.D.N.Y. filed Nov. 15, 2004); *see also* Columbia Pictures Indus., Inc. v. Does 1–10, No. 04CV2697-T-17TBM (M.D. Fla. filed Dec. 14, 2004); Twentieth Century Fox Film Corp. v. Does 1–12, No. C04-4862 (N.D. Cal. filed Nov. 16, 2004) (granting defense motion to dismiss charges for all defendants except Doe 1 as improperly joined).

[37] *See, e.g.*, Direct TV, Inc. v. Legans, No. 03-1071-T, 2004 U.S. Dist. LEXIS 972 (W.D. Tenn. Jan. 9, 2004).

[38] *Compare In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003), *with* MGM v. Grokster, 380 F.3d 1154 (9th Cir. 2004), *cert. granted*, 125 S. Ct. 686 (Dec. 10, 2004).

[39] Paramount Pictures Corp. v. ReplayTV, 298 F. Supp. 2d 921 (C.D. Cal. 2004).

[40] *Id.*

[41] *See Grokster*, 380 F.3d 1154. The Supreme Court granted certiorari in *Grokster* on December 10, 2004, less than one month after Prof. Cohen delivered her remarks.

plaintiffs get fairly automatic disclosure if the papers are in order. If we look at the *John Doe* subpoenas issued in the P2P cases, the Southern District of New York's recent decision in *Sony Music Entertainment, Inc. v. Does 1-40* is a representative example.[42] The court begins by saying that P2P file-sharing is speech but it is not true speech, drawing on the Supreme Court's reasoning in the *Eldred* case.[43] After that, there is a balancing test, a test that has worked quite well in the context of corporate defamation suits. The court asks whether the discovery request is sufficiently specific, whether there is no other way to get the information, and whether there is a central need for the information to advance the litigated claim.[44] In the context of alleged defamation, this has been a balancing test with teeth. In the copyright infringement context, the three considerations are more easily satisfied, and since the court is not evaluating the merits of the copyright infringement claim there is no need to consider any defenses that the user might raise. The remaining question then concerns the targeted party's expectation of privacy. The *Sony Music Entertainment* court said that the expectation is minimal given, first, that this is not true speech and, second, that there is a "terms of service" agreement that says: "I will not use the ISP's services to commit infringement."[45] The court also reasoned that if you open up your computer to the world, you waive any privacy interest you might have.[46] The result of this reasoning is automatic disclosure of the information.

Turning to the indirect infringement context, the ReplayTV case is worth considering more closely. The district court overturned the magistrate's discovery order not based on any privacy interest that it found, but simply based upon its conclusion that the law did not impose on SonicBlue any requirement to create data that did not already exist, especially where it would be quite expensive to do so. The court actually noted that the information, if it did exist, would clearly be relevant to the dispute between the studios and ReplayTV.[47] The DirecTV lawsuits against the purchasers of smart card readers are in a similar vein. The one circuit-level decision on the validity of those lawsuits concluded that there is no civil liability under the Electronic Communications Privacy Act merely for possessing the equipment.[48] That ruling was based on the way the statute defines the violation; it was not based on any privacy interest. The statute confines the violation to the interception of a communication and does not encompass the possession of equipment that could be used to intercept. More importantly for our purposes, DirecTV's method of getting all of this information about smart card purchasers, which consisted of raids on the equipment manufacturers and seizure of their customer lists, went unquestioned. That is simply how you do discovery in this context.

---

[42] Sony Music Entm't v. Does 1–40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004).

[43] *See* Eldred v. Ashcroft, 537 U.S. 186, 221 (2003) ("The First Amendment securely protects the freedom to make—or decline to make—one's own speech; it bears less heavily when speakers assert the right to make other people's speeches.").

[44] *Sony Music Entm't*, 326 F. Supp. 2d at 564–65.

[45] *Id.*

[46] *Id.*

[47] Paramount Pictures Corp. v. ReplayTV, No. CV 01-9358 FMC (Ex), 2002 WL 32151632, at *2–*3 (C.D. Cal. May 30, 2002).

[48] DirecTV, Inc. v. Treworgy, 373 F.3d 1124, 1127 (11th Cir. 2004).

Then, of course, there is *Grokster*.[49] The Seventh Circuit was troubled that Aimster had enabled privacy via automatic encryption, but the court could not bring itself to say that encryption capability alone is bad, so it waffled and said that willful blindness will not save you from indirect infringement liability.[50] In *Grokster* the Ninth Circuit said lack of continuing control will save you.[51] If the Supreme Court chooses to grant cert., its decision could have implications for the kind of control required and the extent of blindness permitted.[52] To a very real degree, this is a question about what information is required to be kept. In *Grokster*, however, that issue has not really been framed as a privacy issue at all.

So what do we make of all of this? First, existing privacy protections provide process without substance (and, as Prof. Swire[53] and Ms. Deutsch[54] explained, there really is not that much process either).

Second, I am not terribly confident that the First Amendment is going to provide us with a useful tool to deal with this problem because we have a very profound national anxiety about situations in which privacy claims come into conflict with claims of illegal conduct. Just look at the cases about private possession of pornography. In 1969, the Supreme Court said, in *Stanley v. Georgia*, that the state cannot prosecute someone for private possession of obscenity because that is wholly inconsistent with the philosophy of the First Amendment—the state has no business in inquiring into what a man's library contains.[55] Four years later, the Court ruled that *Stanley* does not shield transportation of obscene materials for someone who intends to possess them for private use.[56] Then, in 1990. it said that private possession of child pornography also is not exempt because there is a compelling interest in protecting children.[57] This progression illustrates how, even when the First Amendment is involved, courts tend to waffle back and forth about exactly what privacy is guaranteed for someone who is engaging in conduct that is illegal. Currently we can see the same profound national anxiety playing out at the level of national security. If the privacy problem is framed as being just about the (nonexistent) privacy interests of P2P users and not more generally about what privacy users of copyrighted material enjoy, the First Amendment is not necessarily going to afford a particularly strong shield for people seeking to assert it in their own defense.

Finally, there is always a contract involved, and along with it the reasoning about how users have constructively waived their privacy rights by accepting "terms of service" agreements and by opening their computers up to other people for the purpose of sharing files. This reasoning eliminates whatever remaining claim to privacy might exist.

---

[49] MGM v. Grokster, 380 F.3d 1154 (9th Cir. 2004), *cert. granted*, 125 S. Ct. 686 (Dec. 10, 2004).

[50] *See In re* Aimster Copyright Litig., 334 F.3d 643, 650–51 (7th Cir. 2003).

[51] *See Grokster*, 380 F.3d at 1164–66.

[52] MGM v. Grokster, 125 S. Ct. 686 (Dec. 10, 2004) (granting petition for certiorari).

[53] *See supra* Part I.

[54] *See* Deutsch et al., *supra* note 31, Part III.

[55] Stanley v. Georgia, 394 U.S. 557 (1969).

[56] United States v. Orito, 413 U.S. 139 (1973).

[57] Osborne v. Ohio, 495 U.S. 103 (1990).

So the prognosis for user privacy does not look too good. However, I would like to suggest some tentative moves that might ultimately generate a more unified, affirmative conception of user privacy that extends beyond the P2P context.

If we think about user privacy in the context of intellectual consumption, we need to think about two kinds of breathing space for intellectual privacy, by which I mean intellectual consumption and exploration.[58] One is informational, and concerns the maintenance of records about what people read, see, hear and use. These records threaten to produce a chilling effect on intellectual exploration. We are starting to see some limited recognition that, even in the civil copyright context, some sort of informational privacy interest could be said to exist. There is § 1201(i) of the DMCA, which provides a limited privilege to circumvent technological protection measures to protect online privacy unless the content provider gives notice and an opportunity to opt out of data collection.[59] There is also a more general interest in regulating spyware, a term encompassing all technologies that collect information about computer users without their knowledge. In addition, we are starting to see some interesting research on designing privacy protections into DRM systems. A lot of this research is taking place in Europe, but some is being done here in the U.S. It could be that the European data protection directive will cause some of that research to be taken more seriously.

Once again, if we frame the user's privacy interest solely in terms of the informational privacy interest, when push comes to shove that interest is unlikely to be effective against a top-down design mandate that might be imposed on vendors, or against narrowly targeted discovery orders. Thus, I think we need to take more seriously a second type of breathing space that users of copyrighted material might assert for their intellectual consumption and exploration. This interest is spatial in nature, and it is an interest that is premised on the asserted legality of some uses of copyrighted material that take place within private spaces. Here again we see some interesting developments. State consumer protection lawsuits have been filed regarding malfunctioning DRM-protected CDs. We also see research on designing limited copy and use privileges into DRM systems, both in Europe and here in the U.S.. Some of this research may be driven by provisions of the European copyright directive that seem to require content providers to make good faith efforts to preserve privileges that users enjoy under their national copyright laws.[60] In the broadcast flag rulemaking, we see the FCC trying to ensure that equipment recognizing the broadcast flag will also allow use of material and copying material within what they call a personal digital networking environment.[61] However, the FCC does not seem to be imposing comparable requirements in the plug and play environment.

It is not clear yet what all of this will amount to. But these initiatives and others like them are where I think a lot of thought needs to be focused. I would be happy if we could resolve our more general anxiety about privacy versus illegality,

---

[58] *See generally* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003).

[59] *See* 17 U.S.C. § 1201(i) (2000).

[60] Council Directive 2001/29/EC, 2001 O.J. (L 167) 10, art. 6(4) (Directive of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society).

[61] Federal Communications Comm., *Digital Broadcast Content Protection: Notice of Proposed Rulemaking*, 68 Fed. Reg. 67,624 (Dec. 3, 2003).

but particularly in the current national security climate, I am not so optimistic that that is going to happen any time soon. Perhaps, however, there are other ways to address users' privacy concerns. Thank you.

III. DAVID E. SORKIN

PROF. SORKIN:[62] I want to pick up on some points that I think Prof. Cohen was making toward the end of her comments regarding incorporation of privacy into technology. Those of us who function at the intersection of law and technology see two very different worlds. In the law, when we are talking about privacy we look at procedural protections and sometimes, although usually not in this country, we talk about substantive legal protections. However, in the technology world, and in the internet world, it is all about self-help. It is all about finding your own way to get privacy, not relying on procedure or government.

What we often see are people who understand technology very well. These people tend to have a lot of resources available to them: time, money, as well as technical knowledge. They are able to get privacy and are able to make fair use of works and so on. Many other people are not so lucky. I think in one sense that is what is so threatening about Napster[63] and Grokster[64] and DirecTV's commercial skip feature and all these sorts of technologies that deliver that power to a much larger number of people. That is why I think the content industry tends to be trying to stop those threats. The industry does not really care too much about an obscure program written by a Norwegian teenager so long as people have to be able to install Linux to use it. I think we are seeing the development of some sort of digital divide in privacy. People who have resources and knowledge are able to buy privacy. Most people cannot do this. The same thing occurs with access to copyrighted works and of course the intersection of the two. I wonder if there are ways that we can bridge that digital divide without threatening copyright too much. Thank you.

---

[62] David E. Sorkin is Associate Professor of Law at The John Marshall Law School in Chicago, Illinois. Prior to joining the John Marshall faculty in 1991, Prof. Sorkin clerked for a state appellate judge in Indiana and taught at Indiana University School of Law–Indianapolis. Prof. Sorkin has written and spoken widely about internet policy, privacy, consumer protection issues and communication skills. In 1994, Prof. Sorkin created John Marshall's original website, and the following year he began teaching one of the first law school courses on cyberspace law. In 2001 and 2002, Prof. Sorkin taught courses in privacy and cyberlaw at Southern Cross University's Byron Bay Summer Law School in Australia. In 2002, Prof. Sorkin participated in conferences on internet governance and cyber liberties in Sydney, Australia; spoke about spam for the National Conference of State Legislatures in New Orleans; presented the keynote address at a conference on spam regulation held in Kyoto, Japan; and organized a program on spam at John Marshall. Prof. Sorkin's websites on Spam Laws and other topics are frequently cited as authorities. Prof. Sorkin teaches Consumer Law, Current Issues in Information Technology Law, Cyberspace Law, Information Law & Policy, Introduction to Information Technology Law, Lawyering Skills, and Transborder Data Flow.

[63] A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

[64] MGM v. Grokster, 380 F.3d 1154 (9th Cir. 2004), *cert. granted*, 125 S. Ct. 686 (Dec. 10, 2004).

IV. RESPONSE BY PROF. COHEN

PROF. COHEN:[65] I think that there are ways to bridge that divide. This relates to a problem that has been talked about a great deal already: the tendency to polarize this debate and say it is either all or nothing.[66] Recently I think there is more interest in exploring a variety of intermediate solutions that would be expressly designed to protect both copyright and the privacy interests of users. I mentioned efforts in the area of DRM design. Copyright has always been leaky. It has always been premised upon deliberately imperfect control of expression because of the public good that imperfect control fosters. There is an interesting socio-technical question concerning the extent to which this leakiness can be replicated using system design tools. There are also proposals like Prof. Fisher's for using a system of levies to generate compensation flowing to rights holders, while remaining more flexible in terms of some of the other aspects of copyright that are causing trouble; I am sure Prof. Fisher is going to tell you more about that.[67] I have not gotten a sense that the copyright industries have reacted in a wildly positive way to either of those proposals and I think that is unfortunate.

---

[65] *See* biographical information *supra* note 33.

[66] *See generally* Deutsch et al., *supra* note 31; Michael A. Geist et al., *Copyright & Privacy – Through the Technology Lens*, 4 J. MARSHALL REV. INTELL. PROP. L. 242 (2005).

[67] William W. Fisher, III, et al., *Copyright & Privacy – Through the Wide-Angle Lens*, 4 J. MARSHALL REV. INTELL. PROP. L. 285, Part II (2005).