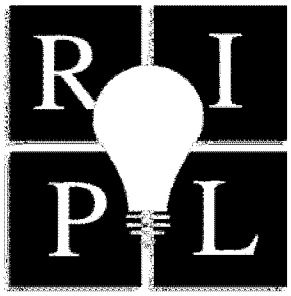
THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW



COPYRIGHT & PRIVACY – THROUGH THE TECHNOLOGY LENS

NOVEMBER 18, 2004

MICHAEL A. GEIST, DORIS ESTELLE LONG, LESLIE ANN REIS,
DAVID E. SORKIN AND FRED VON LOHMANN

ABSTRACT

How is new technology impacting on the more general question of privacy in cyberspace? Is the original notion of an expectation of anonymity on the internet still viable? Can technology pierce through the expectation of privacy even without judicial interference? Do individuals need protection from such technology? Is there technology available to protect the individual? Should these technological tools be regulated? Should the law differentiate between various types of alleged "illegal" behavior; e.g., IP infringement, defamation, possession of pornography and terrorism? Are there international standards that can assist in regulating the intersection between technology and privacy in cyberspace?

Cite as Michael A. Geist et al., *Copyright & Privacy – Through the Technology Lens*, 4 J. MARSHALL REV. INTELL. PROP. L. 242 (2005).

COPYRIGHT & PRIVACY – THROUGH THE TECHNOLOGY LENS*

NOVEMBER 18, 2004

MICHAEL A. GEIST, DORIS ESTELLE LONG, LESLIE ANN REIS,
DAVID E. SORKIN AND FRED VON LOHMANN

I. INTRODUCTION BY DAVID E. SORKIN

PROF. SORKIN:[1] Before we start I did just want to observe that I am fairly agnostic on the battle where the content owners, the record companies, the studios and the infringers on the other side. However, I am definitely rooting for the salmon against the grizzly bears.[2] Our first panelist is Fred von Lohmann from the Electronic Frontier Foundation ("EFF").

---

* 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] 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.

[2] *See* Sarah B. Deutsch, et al., *Copyright & Privacy – Through the Copyright Lens*, 4 J. MARSHALL REV. INTELL. PROP. L. 212, Part VIII (2005) (analogizing grizzly bears successfully catching salmon at a narrow point in a stream to ISPs and internet-access providers as the parties best-positioned to catch copyright infringers).

II. FRED VON LOHMANN

MR. VON LOHMANN:[3] In the interests of responding to the prompt of this panel, I am going to discuss the ways in which technology influences this debate. I am reminded of a time in the mid-nineties, before the World Wide Web had really taken hold, when a variety of legal theorists were saying there are a couple of things about the internet that you have to keep in mind. First of all, enforcement of any kind of intellectual property right on the Internet will be impossible, or certainly much more difficult than it is in the physical world. Secondly, so went the common wisdom, everyone on the Internet is anonymous. Or, as *The New Yorker* cartoon put it, in cyberspace, nobody knows you are a dog.[4]

The irony about those two once-commonly accepted wisdoms is that they were completely and utterly incorrect. It was, in fact, the technology folks who were familiar with how the internet works and actually had a hand in building it who arched their eyebrows immediately and said: "well . . . that is not really right." So it is with that lesson—a lesson of humility for all of us—that I want to paint a bit of the picture of the ways in which technology is critical to addressing this debate.

---

[3] Fred von Lohmann is a senior staff attorney with the Electronic Frontier Foundation ("EFF"), specializing in intellectual property issues. In that role, Mr. von Lohmann has represented programmers, technology innovators, and individuals in litigation against every major record label, movie studio and television network (as well as several cable TV networks and music publishers) in the United States. In addition to litigation, Mr. von Lohmann is involved in EFF's efforts to educate policy makers regarding the proper balance between intellectual property protection and the public interest in fair use, free expression and innovation.

The EFF matters in which he is involved include *MGM v. Grokster*, in which Mr. von Lohmann represents Streamcast Networks, developers of the Morpheus software application, in a lawsuit brought by twenty-eight entertainment companies alleging that Streamcast should be held liable for the activities of its end-users. Mr. von Lohmann argued this case on appeal before the Ninth Circuit Court of Appeals, leading to a groundbreaking ruling by the Court in August 2004 in favor of Streamcast and Grokster. Mr. von Lohmann was also involved in Broadcast Flag and Digital TV, working to represent the voice of consumers and innovators before the FCC and the BPDG in the debate over the "broadcast flag," Hollywood's scheme to sneak federally-mandated content protection technology into all digital television devices.

Mr. von Lohmann was named one 2004's one hundred most influential lawyers in California by the *Daily Journal*, a leading newspaper, and received a 2003 CLAY award (California Lawyer of the Year) from *California Lawyer* magazine. Mr. von Lohmann was also named one of the fifty Agenda Setters for 2003 by UK publication *Silicon.com*. Mr. von Lohmann has appeared on CNN, CNBC, ABC's *Good Morning America*, Fox News's *The O'Reilly Factor* and TechTV's *ScreenSavers*. Mr. von Lohmann has been widely quoted in a variety of publications, including *The New York Times, The Washington Post*, the *Los Angeles Times, Billboard, US News & World Report, CNET News, Wired News, TIME* magazine and a number of leading legal newspapers. Mr. von Lohmann's opinion pieces have appeared in the *Los Angeles Times* and the *San Jose Mercury News*. In addition, Mr. von Lohmann has published numerous EFF-related and other scholarly articles.

Before joining the EFF, Mr. von Lohmann was a visiting researcher with the Berkeley Center for Law and Technology, where his research focused on the impact of peer-to-peer ("P2P") technologies on the future of copyright. Prior to his research fellowship, Mr. von Lohmann was an attorney with the international law firm of Morrison & Foerster LLP, concentrating on transactions and counseling involving the internet and intellectual property. Mr. von Lohmann has also served as a law clerk to Chief Judge Thelton Henderson of the U.S. District Court for Northern California, and Judge Betty B. Fletcher, of the U.S. Ninth Circuit Court of Appeals. Mr. von Lohmann received both his undergraduate and law degrees from Stanford University.

[4] Peter Steiner, THE NEW YORKER, Jul. 5, 1993, at 61.

There is one theme I think that ought to recur in your minds all day today and that theme is the dynamic interaction between the technology and policy arenas. Whether policy-makers rely on courts, statutes or moral persuasion in an effort to regulate or control how technologies are being developed and used, all of these regulatory levers interact with the technology in a very interesting way. Namely, the technology changes. In fact, you have seen already in these digital copyright debates that the technology has not remained static. The peer-to-peer ("P2P") networks today do not operate the same way that Napster® did back in 1999. In addition, the P2P networks of tomorrow, or whatever other technologies may arise in their place, will not work the way that the technologies do today. The technology will respond to what policy-makers attempt to do. The question I think for all of us is: "how do we fashion a mechanism, a solution, that actually aligns the incentives of the stakeholders and the incentives of those who develop the technology?"

I will begin by talking about those who develop the technology. If you think the people that we are talking about here are the Microsofts or even for that matter the Kazaas of the world, you are mistaken. What the internet has made very clear is that new technologies can be developed by many players, many of whom are non-commercial, any of whom can be located anywhere on the planet. For example, most of the web servers run on the planet today use an open-source software package called Apache, developed and distributed by a loosely organized global collective of programmers, who are not in it for the money. If you try to find a corporate entity, a spot in the stream, to use the "grizzly bear and salmon" example provided earlier today,[5] you will find that there is no one spot in the stream in which you can impose easy pressure against the people who developed Apache.

We live in a dynamic system where the technology can and will change in response to efforts to control, regulate or change its course. This is not to say that technology is immune from, or entirely beyond the reach of, legal regimes and regulation. I think that fallacy is one that many technologists entertained in the mid-nineties. Many had the notion that they could simply ignore what lawmakers were up to because they would simply design around any regulation. Of course, that turned out not to be true, either. What I am trying to suggest is that these are interrelated systems. We must keep that in mind when we come up with solutions or proposals for solutions to copyright's "digital dilemma." Ask yourself: "well, how will the other side respond to that?"

I want to say a couple of words about how we got here and then a couple of words about where we are. Next, of course, to finish that chronology, I want to offer some suggestions about where we may be going.

In terms of how we got here, I think it is important to begin by recognizing the extent to which new internet technologies have fundamentally changed the way regular people interact with each other, their culture and the objects of that culture—whether they be music, film, books or games. Increasingly, you have a situation today where people online do a host of things that they previously experienced in a very different context. Many people have no idea that when they take their everyday interactions and move them on-line, the legal norms surrounding their privacy may dramatically change. People, of course, now conduct all manner of

---

[5] *See* source cited *supra* note 2 and accompanying text.

relationships, business and personal, using e-mail, instant messenger and things like that. These kinds of interactions before the internet were generally done face-to-face or over the phone.

Face-to-face interactions are rather unregulated in most senses. The telephone, in contrast, is a very different technology architecture, which has its own set of privacy rights and legal norms, both constitutional and statutory, developed over the course of many years.[6] Suddenly people have taken all of those face-to-face and telephonic interactions and put them on the new technology platform of the internet. They assume, I think, that they will enjoy the same privacy protections, both legally and technically guaranteed in the old context. They assume that their e-mails and online interactions are private.

They also bring their old expectations regarding copyright law. In the old world, when they handed a friend a cassette of their favorite songs, perhaps taped from the radio or their own record albums, they experienced that interaction as a private thing, as something noncommercial, as something they would not be punished for. I suspect that sensibility is carried over into the online environment for many who engage in P2P file sharing.

Thanks to the differences, both technical and legal, in the online context, today expectations and legal norms have diverged.

For example, sharing music online can now be much more easily discovered than sharing cassettes in the offline world. As Ms. Deutsch mentioned, there is now a growing industry dedicated to surveillance technologies on-line.[7] In this particular context, surveillance in the interests of enforcing copyright, you have a situation where your preconceived notions of how much privacy you used to have are changing underneath you. All the while, individuals, when they move their transactions into the internet context, have no idea that the legal norms have changed. Policymakers have been very slow to catch up and so we have an environment where many things are changing without traditional policymaking guidance being applied.

That is where we find ourselves now. I do not actually think that the rise in P2P file sharing represents the sudden rise of a new thieving class in America. I think what we have are established behaviors that have been in place in the offline world for a long time—behaviors around sharing, evangelizing the culture of your preference, talking about your favorite band, your favorite movie, loaning your friends phonographs, cassettes and then CDs, videotapes and then DVDs. We have a cultural expectation that it is good to be able to share and spread information about the books, movies and films that we care about. I think that is what has been carried on-line. I do not think the proliferation of P2P file-sharing represents a sudden massive upsurge in people who desire to shoplift or steal.

But bringing those established values surrounding the importance of sharing of cultural objects into the on-line context changes the equation in important ways. In addition, our policymakers and our laws are still struggling to catch up and find a new accommodation that makes sense of both what I think is the natural and good impulse to share and the economic reality that file-sharing is not the same as the home taping of the past. This need to accommodate consumer expectations and the

---

[6] *See generally* 18 U.S.C. §§ 2510–2522 (2000) (covering acts involving "Wire and Electronic Communications Interception and Interception of Oral Communications").

[7] *See* Deutsch et al., *supra* note 2, Part III.

copyright industries with new technologies is what copyright law has always struggled with.

So, to summarize, we got here because the architecture made things possible that were not possible before. Then we brought with us our preconceived legitimate expectations from the offline world, all the while without knowing or analyzing it while it was happening.

So where are we? I just want to say a few words about the recording industry's investigative efforts to give a context to the privacy concerns. Frankly, I think there is confusion on all sides of the spectrum. There are certainly those who believe that somehow the effort to enforce copyrights in the P2P context constitutes a complete and utter invasion of privacy of an unimagined magnitude. There are others, as I think you heard Mr. Oppenheim suggest, that argue there is no privacy interest here at all.[8]

In fact, if you look at the technology you realize that perhaps neither side is entirely correct. What the recording industry has done is hired investigators. There are now companies with names like BayTSP, Media Enforcer and the like, who basically pose as P2P users.[9] They run the same software or interoperable software that puts out queries into the P2P networks just as regular P2P users do. When they get responses from other users saying, yes, I have that Michael Jackson or Britney Spears track (or whatever track that investigator happens to be searching for on behalf of the owner of those copyrights), the investigator then records the offeror's IP address.

There was a time when copyright owners felt that was enough. That they needed no further investigation or evidence. The mere fact that someone responded to their query was enough to mark them as an infringer. I think the recording industry is learning a bitter lesson in Canada right now about the ways in which that level of evidence gathering is insufficient.[10] They have in the United States, at least it is my understanding, gone the next step and actually downloaded the tracks from the people who were purporting to offer them in order to verify that, in fact, it is the track they are looking for. So that is the way these IP addresses are gathered. *John Doe* lawsuits are then filed against these as-yet unidentified individuals. Subpoenas are issued to ISPs who are then asked to match that IP address with a particular named individual so that lawsuits may be filed.[11]

There are a couple of interesting things that stem from the technology to keep in mind. First, the recording industry's methods of investigation have, thus far, limited it to pursuing only "up-loaders," or people who are offering files to others. If you are not up-loading files, when the query from the investigator arrives, your computer will not respond. So the investigative methods being used today do not yield any

---

[8] *Id.*, Parts II, IX.

[9] *See generally* http://www.baytsp.com (last visited Mar. 13, 2005) (explanation of services); http://www.mediaenforcer.com (last visited Mar. 13, 2005) (explanation of services).

[10] BMG Can. Inc. v. Doe, [2004] 239 D.L.R. (4th) 726 (finding that recording industry evidence was inadequate to support the inference of infringement necessary to obtain the identities of P2P users).

[11] *See, e.g.*, MGM Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004), *cert. granted*, 125 S. Ct. 686 (Dec. 10, 2004); Pac. Bell Internet Servs. v. RIAA, No. C03-3560SI, 2003 U.S. Dist. LEXIS 21659, at *1 (N.D. Cal. Nov. 26, 2003); RIAA v. Verizon Internet Servs., 257 F. Supp. 2d 244, 264 (D.D.C. 2003).

information about the tens of millions of individuals who are solely downloading. These individuals are, in the parlance of the P2P networks, "leeches." They are downloading content but not contributing content to others. So, as far as I am aware, the recording industry's investigative methods are not invading or otherwise compromising the privacy of these P2P users.

Now, lest you think that is a great boon for the recording industry—that driving users to be "leechers," rather than "up-loaders," is somehow drying up the selection of content out there—nothing could be further from the truth. With hundreds of millions of P2P users scattered around the globe, even if most Americans were to stop uploading, there would be no shortage of every conceivable form of content from many, many sources around the world.

The second thing about the current investigation mechanism is that technologically it gives the record industry investigators an ability to find what they term "egregious infringers." This is basically a rhetorical device to say they are able to figure out how many other files that individual is sharing and to select for legal action only those who are sharing a large number (several hundred or more) of files. That is also a function of the technology, because current P2P file sharing applications will allow you to ask, once you have received a communication from another user: "what else are you sharing?" This is called the "browse host" feature in the P2P community. This feature, however, could easily change. In fact, there are some file-sharing applications that have already stopped offering that feature. One of the most popular new applications out there, BitTorrent, for example, does not yield that information.[12] It may well be that very soon the recording industry will have no idea how many files any individual is sharing, thereby making it impossible for them to limit their enforcement to "egregious infringers."

So that is the technological background. In light of that, I want to say a few words about where do we go from here in light of the technology. Technologies are dynamic. They will change in response to enforcement efforts and other regulatory measures adopted by policy-makers. If you adopt a regime that depends upon pitting the copyright and entertainment industries and perhaps law enforcement against the technology, its users and the natural inclination among people to share, you will find that the technology will take steps to try to make your life more difficult. We have already seen new technologies arise that offer enhanced anonymity for users of the networks in question. Freenet is perhaps the oldest file sharing network that had anonymity built into its very architecture—and mind you not solely to frustrate copyright owners. Tor is another Internet technology designed to secure a measure of privacy and anonymity for Internet users.[13] (Of course, anonymity has many uses and there is no reason to assume that anonymity is always intended only to frustrate copyright enforcement.)

You can be sure that the technology will begin changing under you in response to efforts to regulate it. Even if you think you can reach every technology company in America in order to prevent that development, you cannot reach every technology company on the planet. And why focus on companies? Napster® was created by a college student. BitTorrent, one of the most popular file sharing applications today, was written by a single unemployed software programmer working in his spare time.

---

[12] *See generally* http://www.bittorrent.com (explanation of services).

[13] *See* http://tor.eff.org (last visited Mar 13, 2005).

You may want to ask yourself if your proposed mechanism to resolve copyright's digital dilemma is one that will pit you against every computer programmer on the planet or, instead, align your incentives with the technologists of the future. That is the question which I think is not asked often enough by policy-makers considering alternatives to address the issue of copyright in the digital age.

You can ask all you like whether it is right or wrong. You can ask all you like who the victim is, whether or not we should be suing twelve-year-olds and their parents and grandparents. But I submit that in the long run, approaches focused on enforcement and deterrence are going to put us into a cycle that will imperil privacy, erode anonymity and proliferate the technologies of surveillance and censorship. All of these other social priorities will be jeopardized in the effort to try to stamp out what is going to be the natural rise of new technologies to meet an obvious demand. Thank you.

III. DORIS ESTELLE LONG

PROF. LONG:[14] I entitled my presentation for today "Is a Global Solution Possible to the Technology/Privacy Conundrum?" I think the title gives you a fairly good idea of the nature of my comments today. I am coming to this whole issue about technology, privacy and copyright from a slightly different perspective. That is the

---

[14] Doris Estelle Long is Professor of Law at The John Marshall Law School in Chicago, Illinois. Prior to joining the John Marshall faculty, Prof. Long was an attorney for over fourteen years with the Washington, D.C. law firms of Arent Fox Kinter Plotkin & Kahn, and Howrey and Simon where she specialized in the areas of intellectual property, unfair competition, entertainment, computer and commercial law. Prof. Long is a frequent lecturer in the areas of intellectual property law, e-commerce, culture and technology, and has presented papers at conferences in such diverse places as Havana, Cuba; Beijing, PRC; Moscow, Russia; Santo Domingo, Dominican Republic; Lima, Peru; Katmandu, Nepal; Rio de Janeiro, Brazil; Dakar, Senegal; Chiang Rai, Thailand; Taipei, Taiwan; Warsaw, Poland; Kiev, Ukraine; Chisinau, Moldova, Guinea, West Africa and New Delhi. Prof. Long has also been actively involved in training intellectual property enforcement officials in nations of the former Soviet Union under the auspices of the Federal Judicial Center and has served as a consultant on IPR protection issues and enforcement matters for foreign government agencies under the auspices of the U.S. Department Commercial Law Development Program of the U.S. State Department International Information Programs.

In 2000, Prof. Long was on leave from John Marshall and served as an attorney advisor in the Office of Legislative and International Affairs of the U.S. Patent and Trademark Office where she helped negotiate the IPR Enforcement Sections of the Jordan Free Trade Agreement (among others), participated in various bilateral consultations and had responsibility for international IP enforcement issues, including TRIPS compliance and WTO accessions. In 1998, Prof. Long served as a Fulbright Professor at Jiao Tung University in Shanghai where she taught International Intellectual Property Law and International Business Transactions. Prof. Long has also taught in Innsbruck, Austria and Leon, Nicaragua, and serves as a long-distance tutor for the World Intellectual Property Organization.

Prof. Long is the author of numerous books and articles in the area of intellectual property law, including a course book published by West on *International Intellectual Property Law*. At the J.D. level, Prof. Long teaches Copyright and Trademark Law, Intellectual Property in the Global Digital Environment, Unfair Competition and Trade Regulation Law, International Intellectual Property Law; and, at the LL.M. level, Prof. Long teaches International Trademark Law, International Copyright Law, Patent Law, Intellectual Property Law, Globalization and Internet Law and Free Speech in Cyberspace.

international perspective. I have to confess that some of my analysis is based on my own personal experiences.

I do a lot of work in intellectual property and rule-of-law capacity building in the Third World. As such, I am used to showing my identification to anybody who asks for it. I have been stamped, processed and databased by hotel clerks, train conductors, at border controls and almost anywhere else you can imagine. So I have a certain flexibility when it comes to certain types of privacy.

However, what really bothers me is that, as willing as I may be to show you my ID, I hate to have that information controlled, processed, sold and reappear in some other annoying form such as the allegedly compartmentalized banner ads that come at me when I am using the internet.[15] So one of the things I want to say, and one of my approaches to this issue is, as Mr. von Lohmann said, technology is global. Therefore, part of our solution has to be global.[16] I think that requires us to broaden the debate so that decisions can be made on a policy basis that goes beyond the significant, but fairly narrow platform of domestic concerns, and includes the global implications of such policies. In addition, as far as any balance that we are going to make between law, technology and copyright is concerned, it has to be done with an eye to inclusion of international concerns as well as domestic ones.

When you talk about privacy, remember that there are a lot of different definitions of privacy. Everything from the right to be left alone,[17] the right to avoid surveillance,[18] the right to have a private space either in my thoughts or my own physical entryway[19] can define privacy.[20] What I want to focus on is a relatively

---

[15] Although common usage continues to use an initial capital latter to describe "the Internet," such usage no longer seems appropriate given the internet's wide spread and long-standing use. Just as "the Telephone" has become "the telephone," so too, it is time to recognize that "the Internet" has become an accepted and longstanding communication form that no longer needs to be treated with the exclamatory reverence of an initial capital letter. Such special treatment, I believe, has been used in part to relieve international law of its responsibility to resolve the legal issues surrounding intellectual property and privacy on the internet. Capital letters subconsciously tell us all that the "Internet" is something new; so new that we cannot yet be expected to deal with the problems it poses. The time for such complacency, along with the initial capital letter, is long past.

[16] *See supra* Part II.

[17] This right to be left alone includes not merely the penumbra right of privacy recognized by the US Supreme Court in *Griswold v. Connecticut*, 318 U.S. 479, 483 (1965) and its diverse progeny, but includes the right of associational privacy, *see, e.g.*, NAACP v. Ala., 357 U.S. 449, 462 (1958) as well as the right to be left alone within those physical spaces over which one has the right to control physical intrusions, such as one's home, *see, e.g.*, Kyllo v. U.S., 533 U.S. 27, 31–33 (2001).

[18] This right includes, but is not bounded by, the rights against unauthorized search and seizure recognized under U.S. law. *See id.* In the context of the internet, it also includes the right to avoid the collection of personal information about one's web viewing or reading habits. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996); Jerry Kang, *Informational Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998). For examples of regulation of the right to control personal information, consider the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000) and the Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000).

[19] The recognition of some area of private space, whether physical or mental, is in part a subsection of the right to avoid surveillance and unwanted intrusions into personal spaces recognized by the prohibitions against unlawful search and seizure. *See* cases cited *supra* note 17 and accompanying text. There is, however, an additional mental freedom that is not necessarily bounded by physical spaces and which is the subject of increasing scholarly debate, particularly in

narrow question: the right to control the disclosure and use of personal identifying information and personal information.[21] You can define these terms broadly. My focus is not on the categorization, per se, of information. Instead, it is on what I perceive to be a more fundamental issue internationally—whether privacy is a purely individual right that then becomes something I can willie nillie give away or whether there is another aspect to privacy. I call it "collective," but I think it is more the social interest, where there are going to be certain aspects to privacy that even if you *do* want to sell it, we are not going to let you do it.[22] I think when we start talking about global privacy controls, we have to recognize that we are talking not just about an individual's interest in their own privacy. We are also talking about society's interest in where and when that privacy must be defended, even if the individual does not care about it.

When you talk about the global implications of privacy and think about the technology that comes into play here, the discussions cannot be focused solely on the actions of giant multinational corporations and associations, or companies located in the United States. The internet and the technology that we are dealing with comes from everywhere. If it comes from everywhere *a fortiori* you are not going to be able to deal with it in a rational or effective manner unless everybody is at the table. All of the parties' various concerns have to be raised so that you actually get some sort of a global solution. We know that the need for such a multinational solution is backed up by the nature of the internet itself. No one country creates technology.[23] No one country alone can effectively regulate that technology. When I talk about "global problems," I do not mean "problems" in the sense of something we have to correct. I mean problems in the sense that there are debates about the nature of the challenges and opportunities that may arise.

---

the area of access to digital works. *See generally* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29 (1994); Cohen, *supra* note 18.

[20] This short list is by no means intended to be inclusive of the various theories, bases or categories for privacy, particularly as those issues relate to technology. The types of privacy mentioned are merely examples of the types of issues that may be raised in either a domestic or international discussion of the scope of any recognized protection right or its limitations.

[21] As used here, the term "personal identifying information" is meant to include any information that can be used to identify an individual. Such information would include the traditional categories, such as name, address and social security numbers, as well as such newer methods of source identification as DNA and other biometric information. The term "personal information" theoretically would include this information, but is also intended to include other information which may not necessarily be self-identifying, such as unidentified or unaggregated medical information, or even the websites a person chose to visit last night or the movies someone watched last Saturday with friends.

[22] One example of such a social right is the right to control the disposition of one's own body. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 152–55. Although privacy-based concerns have granted each of us in the United States certain recognized rights over our bodies, *see id.*, there are laws in this country that say we cannot sell the use of our bodies for sexual purposes, *see, e.g.*, 18 U.S.C. § 2421 (criminalizing the act of crossing state lines to engage in prostitution or other sexual crimes). Similar limitations may be imposed on our ability to control or even sell our privacy rights.

[23] Consider some of the more prominent examples of technological development that have directly impacted the privacy/technology debate. ARPANET, which eventually evolved into the internet, was developed largely in the United States. DeCSS, which has proven to be the bane of the movie industry, was developed by Jon Johansen, a Norwegian. The so-called "Love Bug Virus" was created by Onel de Guzman, a Philipino.

Think about the internet itself. We have been focusing on P2P file sharing. However, there are a lot of business opportunities in P2P file sharing. There are a lot of e-Business models that are out there that necessitate that wherever you draw the lines between data collection, data mining and an individual's rights, you are going to have an impact across the globe on both major corporations who might use it as well as small and medium enterprises. We know that just as we have P2P file-trading, of course, across geographic boundaries, we have lawsuits all over dealing with the simple question of P2P file sharing and the rights to disclose information and the end user's identities.[24] This is a global problem. It is not just situated in one particular country and it really does need a global solution.

I have to say I agree with Mr. von Lohmann[25] when he says technology changes. I call myself a "techno-skeptic." Technology is great. Law can never catch up to technology. It is not possible. We have never been able to do it. We will never be able to do it. Nor would we want to. To illustrate this, think about the *Yahoo* case,[26] which is the Nazi paraphernalia case. I always think of that as a perfect example of even when you get the technology experts in the room, they disagree about what technology can and cannot do. The case was fascinating because you had various people testifying as to whether the technology would actually effectively allow you to block or not.[27]

If the experts in technology cannot describe the limits or the actual impacts of technology, then we cannot look to technology alone as a solution. I also think the perfect example of why technology does not solve all of your problems is evidenced in the anticircumvention provisions of the Digital Millennium Copyright Act ("DMCA").[28] Thank you very much for all of the efforts that were created to come up with a copy code which was circumvented by a nice little magic marker, so all I had

---

[24] *See Music industry wins approval of 871 subpoenas*, CNN.COM (Technology), July 19, 2003, *at* http://cnn.com/2003/TECH/internet/07/19/downloading.music.ap/index.html; *Fightback or death rattle?*, ECONOMIST.COM (The Economist Global Agenda), Apr. 2, 2004, *at* http://www.economist.com/agenda/displayStory.cfm?story_id=2552490; *Record Companies Sue Hundreds of File Sharers:* BMG v. Does 1–203, 10 No. 23 ANDREWS INTELL. PROP. LIT. R. 6 (Mar. 2, 2004); *UK music to sue online 'pirates,'* BBC NEWS (UK Ed.), Oct. 7, 2004, *at* http://news.bbc.co.uk/1/hi/entertainment/music/3722428.stm; John Leyden, *Japanese P2P founder arrested*, THE REGISTER (UK), May 10, 2004, *at* http://www.theregister.co.uk/2004/05/10/winny_founder_arrested.

[25] *See supra* Part II.

[26] *See* La Ligue Contre Le Racisme et L'Antisemitisme v. YAHOO! Inc., Superior Court of Paris, Nov. 20, 2000, obs. Judge Jean-Jecques Gomez, *unofficial English translation available at* http://www.gigalaw.com/library/france-yahoo-2000-11-20-lapres.html (last visited Mar. 13, 2005); *see also* Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 379 F.3d 1120 (9th Cir. 2004).

[27] *See* La Ligue Contre Le Racisme et L'Antisemitisme v. YAHOO! Inc., Superior Court of Paris, Nov. 20, 2000, obs. Judge Jean-Jecques Gomez. The disagreement between the experts is most clearly delineated in the decision of the French court, which ultimately reached the conclusion that blocking was technologically feasible, although complete blockage would be impossible to achieve. *Id.* The testimony, the decision and the ultimate result (a decision which proved unenforceable under US law, *Yahoo!*, 379 F.3d 1120) underscore the difficult relationship between law and technology in general. No resolution in this area has ever been perfect. In fact, to expect perfect compliance or perfect resolutions is to set up any potential solution for failure.

[28] *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.); 17 U.S.C. § 1201 (codifying the anticircumvention provisions of the DMCA).

to do was draw it around the edge and all of your wonderful technology was absolutely no good. So technology has its limits and we cannot rely on the so-called "experts" to either set the limits or solve any of what we perceive to be the so-called problems. I do not think the law can actually fix this by itself. I think we need to put them all together.

When you think about all of the debates around the borderless nature of cyberspace; when it first came into existence, it was touted as the wild frontier—the copyright-free zone.[29] As it turns out, it is not. Cyberspace does however, because of its very nature, pose problems for imposing hard goods' international guidelines to the internet. We have all kinds of international guidelines on protection. We have things like the World Intellectual Property Organization Copyright Treaty ("WCT") that talks about the application of copyright protections to the internet.[30] We have The Agreement on Trade Related Aspects of Intellectual Property Rights ("TRIPS") which talks about the need to have "effective enforcement" of intellectual property, including copyrights.[31] The problem with those treaties is that you cannot have the same type of enforcement regimes in the hard goods' world that you have on the internet. There is no physical border. If I am sending something across the internet, there are no customs who can seize it unless they want to examine every single piece of information that flows across their borders. It is possible, but it ruins the whole point of having the internet. While hard goods regimes do not solve our problems, they do give us some guidance. I am actually one of those people who thinks history is kind of helpful. One of my favorite books that I always recommend is a book by Standage, that talks about the "Victorian Internet": the telegraph.[32] When you think about the early stages of the telegraph and the early stages of the telephone, we had some of the same issues that came up. We had issues about service provider liability, privacy and who is responsible if the content is wrong or incorrect or bad.[33] So history does give us guidance. But once again, while I think we need to be informed about those previous issues, they does not give us the answer.

---

[29] *See, e.g.*, John Perry Barlow, *The Economy of Ideas*, WIRED, at 84 (Mar. 1994); Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19 (1996).

[30] WIPO Copyright Treaty, adopted Dec. 20, 1996, S. Treaty Doc. No. 105-17 (1997), 36 I.L.M. 65, 1997 WL 447232 (1997), *available at* http://www.wipo.int/treaties/en/ip/wct/trtdocs_ wo033.html (last visited Mar. 13, 2005) [hereinafter WTC]. The WCT is largely perceived as filling the gaps left by the Agreement on Trade Related Aspects of Intellectual Property Rights ("TRIPS"), *see infra* note 31, in dealing with the emerging problems of copyright use and protection on the internet. Among the more noteworthy developments contained in the WCT was the recognition that authors had the exclusive right to authorize the "making available" of their works on the internet, WCT, art. 6, and the requirements that signatory provide "effective legal remedies against the circumvention of effective technological measures" used in connection with the exercise of copyright, WCT, art. 11.

[31] Agreement on Trade-Related Aspects of Intellectual-Property Rights, Apr. 15, 1994, 33 I.L.M. 81, *available at* http://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm (last visited Mar. 13, 2005). Part III of TRIPS, in particular, Articles 41 to 61, require effective enforcement of intellectual property rights, including civil, criminal and border control measures. Although TRIPS was largely negotiated prior to the emergence of the internet as a communications media for the masses, its provisions are considered content neutral and, therefore, fully applicable to copyright enforcement on the internet.

[32] TOM STANDAGE, THE VICTORIAN INTERNET: THE REMARKABLE STORY OF THE TELEGRAPH AND THE NINETEENTH CENTURY'S ON-LINE PIONEERS (Walker Publishing Co. 1998).

[33] *Id.*

One of the problems that we have in talking about privacy on a global scale is that definitions of privacy, of what my expectation is and what I anticipate should belong to me as an individual, change based on social, political and cultural norms. In fact, even I would suggest technology has changed some of our assumptions. I think back to when I first started in the practice of law, back in the dark ages, it became very apparent that if you picked up the office telephone and used it, you did not have the same privacy you had if you used your telephone at home. This was because it was your employer's piece of equipment. If you really thought nobody was listening in from time to time, you were naïve. That does not mean that we all have to be paranoid. But it does mean that technology has changed our expectations.

A good example of how culture distinguishes between our expectations of privacy is to take a look at the United States' treatment of what you can do on a commercial basis with personal information and the European Union's ("EU's") treatment. When you look at the database directive on data processing and privacy, it becomes very clear.[34] There is no question that the EU Directive imposes far more stringent protections for the collection and use of certain types of personal information that our laws do in the United States.[35] In addition, when you talk to people from the EU they are appalled at the things that we in the United States think are okay to collect and sell. " What the heck, I gave my consent." The people from the EU sit there and say that you are not supposed to be allowed to do that. So we see that culture comes into it. In fact, culture informs the debate. As such, we will again be faced with international standards that will only be harmonized and not uniform and it may make for difficulties.[36]

If we cannot all agree on the definition of privacy, maybe we can all agree on what you should not have privacy for. I listed a couple of places where you can look through them, and you can, based on that list, decide which ones you should give greater or lesser privacy for or for which we impose greater procedures. Among the types of conduct for which we might as a global society decide to give greater or lesser degrees of privacy are solicitation to commit murder, public riot, defamation, obscenity, and copyright infringement.[37] We would probably all agree that solicitation to commit murder ought to be right up there as an instance where you do not have a lot of privacy rights. What is the definition of "solicitation to commit murder?" Does the publication of a book called "Hit Man," which describes how to commit murder qualify as something for which you lose privacy?[38] So even as we

---

[34] Council Directive 95/46/EC, 1995 O. J. (L 281) 31.

[35] *See generally* CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ON-LINE BUSINESS (Oxford University Press 2003).

[36] *See generally* Doris Estelle Long, *"Globalization": A Future Trend or a Satisfying Mirage?,* 49 J. COPYRIGHT SOCIETY 313 (2001) (examining the problems that harmonized, as opposed to "uniform," standards may cause, particularly in the arena of creating predictable enforcement paradigms).

[37] All of these activities have formed a basis for exclusions from identity protection around the world. *See generally* Doris Estelle Long, *Crossing the Pond: International ISP's and the Barrier Reef of Strict Liability, in* PROCEEDINGS OF THE AM. INTELL. PROP. L. ASSOC. ANNUAL SPRING MEETING (Am. Intell. Prop. L. Assoc., Dallas, TX., May 2004).

[38] REX FERAL, HIT MAN: A TECHNICAL MANUAL FOR INDEPENDENT CONTRACTORS (Paladin Pr. 1983); *see also* Rice v. Paladin Enters., 128 F.3d 233 (4th Cir. 1997) (finding genuine issues of fact existed as to whether publisher of a book that assisted murderer could be held liable in wrongful death action).

look at categories where we might be able to say, okay, lesser standard of individual privacy, greater rights to have procedural protections in place to allow disclosure, we will not all agree on what those definitions are internationally.

If you look at ISP liability rules, they give you a good sense of how difficult it is to agree on a single international standard. Look at the categories for which ISPs are not safe harbored. Based on the activities of their end-users, you find Australia prohibits activities where it is unsuitable for minors.[39] Look at Singapore's regulations where if the activity is objectionable on the grounds of public order and national harmony, the ISP is liable.[40] In China, there are regulations that if it endangers national security and disturbs the social order, the ISP is liable.[41] We cannot agree and I do not think we ever will completely agree internationally on what types of activities are not considered private.

If you look at it from the point of view of end-user information, we do not have agreements on the standards to be applied. When you look at the free trade agreements the United States has entered into with Singapore and various countries,[42] they basically adopt the language of the DMCA.[43] They say you have to have expeditious disclosure.[44] They also contains that marvelously obscure language that does not make it clear what happens to conduits.[45] That ambiguity has been

---

[39] Australian Censorship Act of 1996 (WA), *available at* http://libertus.net/censor (last visited Mar. 13, 2005).

[40] Broadcasting Act of 1996, ch. 28, § 9, cl. 2, ¶ 13(b)(i) (Singapore ISP Class Licensing Regulations), *available at* http://www.mda.gov.sg/wms.file/mobj/mobj.487.ClassLicence.pdf (last visited Mar. 13, 2005).

[41] Chinese Internet Domain Name Regulations, ch. 4, art. 19, § 2 (Sept. 30, 2002), *available at* http://www.chinaepulse.com (last visited Mar. 13, 2005).

[42] In addition to the Free Trade Agreement between the United States and Singapore, the U.S. has either entered into or is in the process of negotiating free trade agreements with a broad range of trading partners and potential trading partners, including the Andean Community (Columbia, Peru, Ecuador, Bolivia); Australia; Bahrain; CAFTA (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua); Chile; Morocco; and the South African Customs Union (Botswana, Lesotho, Namibia, South Africa, Swaziland).

[43] *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.); *see also* 17 U.S.C. § 1309 (2000). Among the provisions that have been incorporated into the Singapore Free Trade Agreement are the safe harbor provisions of § 512 of the US Copyright Act, 17 U.S.C. § 512(b), the notice and take-down requirements for hosting and caching sites, *id.* § 512(c), and a modified subpoena process requiring the expedited disclosure of end user information in cases of potential infringement, *id.* § 512(h). The analogues for these requirements are found in Chapter 22.16 of the Singapore Free Trade Agreement ("FTA"). These provisions have been mirrored in other FTAs. *See supra* text accompanying note 42.

[44] *See, e.g.*, Singapore Free Trade Agreement, ch. 22.16(a) [hereinafter Singapore FTA].

[45] In particular, Chapter 22.16(A) of the Singapore FTA requires administrative or judicial procedures that enable copyright owners to obtain "expeditious" disclosure of end user "information." To qualify for such disclosure the copyright owner must have previously given "effective notification of claimed infringement." *Id.* The "information" must be in the "possession" of the ISP and must "identify" the alleged infringer. *Id.* There is no affirmative obligation to recreate end-user information. *See supra* text accompanying note 43. The language regarding the duty to disclose end-user information is tied to the provision of "effective notice" of infringement. Under the language of Chapter 22.16, safe-harbor acts of storage (hosting) and linking are specifically premised on expeditious removal of or disabling access to infringing material upon gaining actual knowledge or awareness of infringement, including "effective notice." Singapore FTA, ch.

adopted directly into what is at least a bilateral standard. Due to the number of countries that are entering into free trade agreements with the United States, and the similarity of the language in these agreements,[46] this becomes potentially an international standard. If you look at the EU, with much higher protection in their database directive on privacy, you need a higher level of proof to obtain such identifying information. Look at some of the U.K. cases, like the *Ashworth* case (which is not an internet case).[47] *Ashworth* requires an overwhelming likelihood that a specific wrongdoing must have been committed.[48] I think we are seeing in the United States greater recognition that if we impose requirements for end-user disclosure of identity we are going to make sure the standards for securing such disclosure are higher.[49] At least we have some sort of international standard that is gradually growing so that if you are going to be required to disclose identifying information regarding the end-user we do recognize there is some privacy concern we are going to have to balance.

One of the problems about trying to set any sort of standard right now on an international basis is that I am very nervous about setting law before we understand technology. I am very nervous about setting policy before we really understand the ramifications of it. Now, admittedly we always have that problem. Think back to when they created the camera. All of a sudden the debate became "well, if you are photographing reality, is it copyright protectable?"[50] One of the things I am concerned about is when you look at some of the early efforts to deal with the technology issue, like the DMCA's anti-circumvention provisions,[51] and where some of those electronic fences were placed; they were placed before we fully understood

---

22.16(v)(B). The act of caching similarly requires expeditious removal of or disabling access to infringing material upon receipt of effective notification. *Id.*, ch. 22.16(iv)(D). Conduit activities impose no such obligation. Yet, the obligation to establish administrative or judicial proceedings to require the disclosure of end-user identification is tied to the receipt of "effective notification of claimed infringement." *Id.* This failure to require conduit ISPs to comply with removal notifications in the DMCA led the D.C. Circuit Court of Appeals to refuse to apply the expedited subpoena process of § 512(h) to conduit ISPs. *See* RIAA v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 347 (2004). Although treaty language is not generally the same as a statute, and is not subject to the same rules of interpretation, there is a strong likelihood that this lack of clarity may be relied upon to avoid requiring identity disclosures based solely on conduit activity.

[46] *See generally supra* text accompanying note 42.

[47] Ashworth Hosp. Auth. v. MGN Ltd., 1 W.L.R. 2033 (H.L. 2002) (U.K.) (involving the identification of a journalist's source).

[48] *Id.* In *Ashworth,* the court granted the request for disclosure on the grounds that there was an "overwhelming likelihood" that a specific wrongdoing had been committed. *Id.*; *see also* Totalise Plc v. Motley Fool Ltd, 1 W.L.R. 1233 (Eng. C.A. 2002), *available at* WL, 2001 WL 1479825 (indicating that the party seeking the disclosure of the identity of an alleged defamer who utilized the internet should be required to pay the costs since any voluntary disclosure would be a breach of the Data Protection Act of 1998); Long, *supra* note 37.

[49] *See* Elektra Entm't Group Inc. v. Does 1–6, No. 04-1241, 2004 U.S. Dist. LEXIS 22673 (E.D. Pa. Oct. 12, 2004).

[50] *See, e.g.*, Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53 (1884).

[51] *See, e.g.*, 17 U.S.C. § 1201 (2000).

what the nature of the uses was going to be. Look at § 512(h).[52] Nobody anticipated at that time we were going to have to actually deal with conduits as the problem.[53] They were focused on warez sites, not P2P file trading. Look at the *Grokster* case.[54] While the issue about the balance between technology, substantially non-infringing uses and P2P is important, if we get a decision where certiorari is granted before we have a true conflict and a chance to really think about it in a rational manner, we will not fully understand what the implications of that hasty decision may prove to be.[55] I have to say, and it is not just because I am in Illinois, but I kind of like the approach that Judge Posner is trying to take to that issue in *Aimster*.[56] I would like the idea of trying to put some sort of economics in it. In *Aimster*, Posner suggested taking a cost/benefit risk analysis into consideration in determining what activities qualify as substantially non-infringing uses under the *Sony* test.[57] I would also hate to see that disappear in a rash decision before the courts and Congress have had a chance to consider the issue and craft a more fully articulated policy decision whose implications are fully understood. In addition, I hate to point the finger at consumers, but we are not as savvy as we are supposed to be. We do not completely appreciate how much of our privacy we are trading away and to a certain extent I think this is where some international education is probably required.

Think about all of the recent articles that you have read talking about innovation. I have a cell phone. The new innovation is not better service; it is not a clearer signal; it is, look, I have a cell phone where I can take a picture! I am not sure that we are getting the technology we deserve to deal with some of these privacy issues. I am also concerned that consumers tradeoff their rights without knowing what they are trading. More importantly, to a certain extent, consumers do not have the rights to trade.

Among the potential solutions, and these are just thoughts to throw out there, are consumer education awareness, greater consumer protection through notice and labeling, fair information use standards, including data mining prohibitions and "propertization" of personal information. When you look at these possible solutions I do not think any one of them will work on an international level. We need a combination of approaches to try and deal with the idea of privacy and technology and at least we need to start the debate. I think there needs to be more awareness by consumers and, in part, I think that requires that we have more protection of consumers. At a minimum: label things when you start selling me disks that will not play on the equipment that I currently have. Beyond that, I do not think you want just labeling. Removing any ability to exercise fair use simply by placing a label on material is not a solution.

---

[52] *Id.* § 512(h). This provision established an expedited subpoena process for the disclosure of end-user identities and has been the subject of heated debate over the application of these procedures to ISPs involved in conduit activities. *Id.*

[53] *Id.*

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

[55] The Supreme Court granted certiorari in the *Grokster* case less than one month after Prof. Long delivered these remarks. *See* MGM Studios, Inc., v. Grokster, Ltd., 125 S. Ct. 686 (Dec. 10, 2004). The oral arguments before the Supreme Court are scheduled for March 29, 2005.

[56] *In re* Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003).

[57] *Id.* at 653–54.

I do not think I ought to be able to always give away my privacy rights. I think we have to look at some other alternatives. When you talk about fair information use standards, which includes not just data-mining prohibitions but also substantive requirements that deal with the collection of information, look at the Organization for Economic Co-operation and Development ("OECD") which back in 1980 was already talking about how to deal with these problems.[58] We need to pull that forward, put it back on the table and start more discussions about it.

Finally, since we are going to talk about intellectual property, let's talk about something new—databases, the organization of personal information. If my right to privacy is not completely appreciated unless there is a property right attached to it, then maybe what we do is start informing consumers that they have a property right in their information. I do not think that solves the problem. I think it raises a whole lot of interesting questions because you have all seen that when we have property, we can place all kinds of fair uses and easements on it. I think all of these are issues where we need to talk on an international level about how we solve the problem. In the future, the technology is going to keep forging ahead. The international implications are going to keep getting broader and broader and the issues will remain unresolved until we actually sit down and deal with it. The solution is a good one if it says that we are not in enemy camps. We need to meet in a middle ground and we need to start putting it on the table in front of large multinational organizations. If we simply rely on bilateral treaties, we are not going to get the type of protection that privacy might need because the right voices are not being heard. Thank you.

IV. MICHAEL A. GEIST

DR. GEIST:[59] I thought I heard in Mr. Oppenheim's rebuttal at the end of our last panel a comment that suggested that we actually need to have a debate about whether P2P enjoys privacy protection.[60] I have to say that in Canada we do not have that debate anymore.

It is fairly clear in Canada that privacy is protected in P2P as it is protected everywhere. We have national privacy legislation.

---

[58] *See, e.g.*, Organisation of Economic Co-operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Paris, Sept. 23, 1980.

[59] Michael A. Geist is the Canada Research Chair of Internet and E-commerce Law at the University of Ottawa. Dr. Geist obtained his Bachelor of Laws (LL.B.) degree from Osgoode Hall Law School in Toronto, Master of Laws (LL.M.) degrees from Cambridge University in the United Kingdom and Columbia Law School in New York, New York and a Doctorate of Law (J.S.D.) from Columbia Law School. Dr. Geist has written numerous academic articles and government reports on the internet and law. Dr. Geist is a member of Canada's National Task Force on Spam. Dr. Geist is also a columnist on law and technology for the *Toronto Star* and the *Ottawa Citizen*, and is the author of the textbook *Internet Law in Canada* which is now in its third edition. Dr. Geist is the editor of the Canadian Privacy Law Review and the creator of http://www.privacyinfo.ca, one of Canada's leading privacy websites. In 2003, Dr. Geist received Canarie's IWAY Public Leadership Award for his contribution to the development of the internet in Canada and was named one of Canada's Top 40 Under 40. More information can be obtained at http://www.michaelgeist.ca.

[60] *See* Deutsch et al., *supra* note 2, Part IX.

I want to talk a bit about what the impact that that privacy legislation has had on a couple of copyright cases as well as some of the Privacy Commissioner's findings that focus on technology issues.[61] I will start, actually, by saying that it may come as a surprise for you to hear that I actually think Canada's privacy legislation is woefully inadequate and ineffective.

I write a column in Canada on technology law issues. I have written a number of pieces fairly recently talking about some of the ineffectiveness of Canada's privacy legislation yet I still think it has had a significant impact on the areas that we are talking about. To understand why, I started thinking about football.

In Ottawa this weekend we are having our Grey Cup. The Grey Cup is sort of the Canadian equivalent of the Super Bowl in the sense that it is the national championship of Canadian professional football. Typically the games are played under snowy conditions. I am actually going to the game and have seats that are covered, so I am hoping that it snows. It is a quintessentially Canadian game. The local Ottawa team, the Ottawa Renegades are not playing but they are in fact the host team. I raise all of this because about ten months ago I received an unsolicited commercial e-mail from the Ottawa Renegades inviting me to purchase season tickets. I got in contact with them and asked how they obtained my e-mail address. I indicated that I would rather not hear from them again and asked them to please stop sending me these e-mails. They agreed. Then two weeks later they sent me another one. So I thought this provided a fine opportunity to see how well our new privacy laws in Canada worked and launched a complaint against the Renegades. I have been told that I won the decision and am told that a well-founded finding is forthcoming.[62] When talking about this with a number of people they say, "so what?" I must say that sometimes I have a hard time answering that question. I will be in the possession of a well founded finding from the Privacy Commissioner saying I opted out and the opt-out was not respected. Perhaps my personal information and my e-mail address was collected contrary to Canada's privacy law, but it does not go any further than that. You see, the decision that will be posted by the Privacy Commissioner will not mention me certainly, but it will also not mention the Renegades, although that may be coming to a newspaper article near you.[63]

The thing about this is that our laws do not name the complainants nor do they name the people who are the targets. In addition, there has yet to be any significant enforcement actions. I do not think the Privacy Commissioner, is about to go to federal court over this case because the Ottawa Renegades have done something so severely wrong that in fact they ought to compensate me in some way. There are limited reporting requirements. In fact, The Commissioner will, I suspect, release this finding because it raises some new issues. However, there are many other

---

[61] The Privacy Commissioner is a Canadian officer of Parliament whose role is to promote awareness of privacy related issues, conduct investigations into breaches of privacy in both the pubic and private sector and resolve conflicts over the use and dissemination of private information.

[62] Letter from the Office of the Privacy Commissioner of Canada to Michael Geist, File Nos. 6100-00780, 6100-00781, (Dec. 01, 2004), *available at* http://www.mgblog.com/resc/GeistPCCSpam decision.pdf.

[63] Indeed, Dr. Geist published such an article shortly after making these remarks. Michael Geist, *2004's Tech Rulings Shaping Lives, Business Banner Year for Digital Decisions,* THE TORONTO STAR, Dec. 20, 2004, at C01 (setting forth the developments in Canadian technology law over the last year, literally from A–Z).

findings that are resolved and are not released at all. It is not that this is going to stop spam. Those sending spam are not going to look at this one decision, and exclaim, "I get it, I should not be doing this anymore!" and just stop. I think there are other kinds of organizations who would not think of themselves as spammers at all, yet they clog my e-mail box. So perhaps this decision will make them think a little harder about the kinds of things that they do and gauge on what side of the envelope their marketing practices fall. That is in many ways what we have seen happening in the copyright realm where, not withstanding the fact there is no specific privacy provisions within our copyright act, our national privacy legislation has had a real impact.

Privacy is now a stakeholder in the copyright debate. It is not the stakeholder that sits around the table and tries to lobby government officials about what should be done. It is sometimes brought up by public interest groups, but they are dealing with all kinds of issues and privacy sometimes even takes a backseat there. Once you get judges and others looking at the issues, however, privacy is suddenly very much at the table. If you read the *BMG v. Doe*[64] case as well as the SOCAN v. CAIP Supreme Court case,[65] you will find that the court is very aware of the culture of privacy that we now have in Canada. In fact privacy's importance is to be factored into the court's analysis as far as copyright and also within technology more generally. Let me give you three quotes that came from the justices in the *BMG* case. One was "protection of privacy is of the utmost importance to Canadian society."[66] Another, "parliament has also recognized the need to protect privacy by enacting PIPEDA," the Personal Information Protection and Electronic Documents Act.[67] Then, finally, "PIPEDA requires the court to balance privacy rights against the rights of other individuals and the public interest."[68] These issues were raised by the intervener I mentioned in my last presentation, the Canadian Internet Policy and Public Interest Clinic ("CIPPIC").[69] However, there were certainly those that argued this was not going to be an issue at all. There is in fact an exception to Canada's privacy legislation where we look at potential civil or criminal liability. Yet this judge made it clear that he was going to consider the privacy grounds and state very clearly that Parliament, in reflecting Canadian society's views, sees the privacy issue as a fundamentally important one. The way that played out is quite interesting and it picks up a little bit on what Prof. Palfrey had to say as part of his presentation.[70] Prof. Palfrey talked about the ways in which they have tried to strike some of the balances or the way the balance might be appropriately struck.[71]

The judge I mentioned earlier tried to do the same kind of thing. One way in which Prof. Palfrey did this relates to what he showed us regarding the style of cause and the parties. This would not happen in Canada, since this judge said he would not release the names of the parties to the general public.[72] The judge argued that

---

[64] BMG Can. Inc. v. Doe, [2004] 239 D.L.R. (4th) 726.
[65] SOCAN v. Can. Ass'n of Internet Providers, [2004] 240 D.L.R. (4th) 193.
[66] *BMG,* 239 D.L.R. (4th) at 736.
[67] *Id.* at 738.
[68] *Id.* at 740.
[69] *See* Deutsch et al., *supra* note 2, Part VI.
[70] *See id.*, Part V.
[71] *See id.*
[72] *BMG,* 239 D.L.R. (4th) at 744; *see also* Deutsch et al., *supra* note 2, Part V.

one of the things that was essential in balancing privacy as against some of these copyright interests was to develop what he describes as a public interest test. Public interest on the one hand to enforce copyright law while, at the same time, ensuring the privacy of the particular individuals who are to be most affected. The judge talked about a number of things. First, the information to be disclosed ought to be reliable.[73] One of the things he was deeply troubled with was that the information that was provided to the court as evidence of infringement was somewhat stale and dated—it was a couple months old.[74] He questioned the reliability of that evidence.[75] With respect to the balancing test, with copyright on the one hand and privacy on the other, he was really concerned about this.[76] Is this old information that is going to impact someone so directly that he ought not to use it? The judge also talked about restricting disclosure to the minimum required.[77] This minimum arises in a couple of ways. The first way is a limited use so that it could only be used by the parties if the judge were to issue this order for the purposes of proceeding with the suit.[78] That reflects one of the fundamental principles you would find in the privacy legislation as a whole. Limits would be set on what the party who obtained the information in the first place, could do with it. The judge also argued that the Kazaa pseudonyms were actually sufficient to pursue the case.[79] He argued that from a public perspective the only thing that would be provided was something that was already in a public domain.[80] For instance "geekboy@kazaa.com" was one of the pseudonyms, and that pseudonym could continue to be used in the style of cause.[81] The actual names of the parties, the information that was needed to proceed forward with the case, would be contained in an annex that would be kept under confidential seal.[82] In fact, it would not be made publicly available.[83] We had here a judge that was trying to strike that balance and sought to identify a number of ways to do it.

We had this issue rise to the surface again in the Canadian context in the Tariff 22 case this past summer.[84] This is the case where the style of cause there is *SOCAN v. CAIP*, the Canadian Association of Internet Providers.[85] The case had to do with a proposed tariff dealing with music streaming or downloading from a website.[86] One of the questions that the court had to deal with was where a transmission would occur.[87] Was it from the host server or perhaps where it was received. In addition, in a dissenting opinion written by Canadian Supreme Court Justice LeBel that ought not to be ignored, Judge LeBel raised the privacy concerns with a test that focused on

---

[73] *BMG*, 239 D.L.R. (4th) at 736–37.
[74] *Id.* at 742.
[75] *Id.*
[76] *Id.* at 743–44.
[77] *Id.* at 745.
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.* at 737, 745.
[82] *Id.*
[83] *Id.*
[84] SOCAN v. Can. Ass'n of Internet Providers, [2004] 240 D.L.R. (4th) 193.
[85] *Id.*
[86] *Id.* at 203.
[87] *Id.* at 213.

where the transmission was received.[88] This judge actually argued that we ought to use the place of the server test.[89] One of this judge's prime motivations in doing so, although the rest of the court did not agree, was that he did not want to start delving into the internet practices of individual users. This judge thought it would be a core part of trying to identify where something was downloaded as opposed to the location of the host server which would not implicate those concerns at all.[90]

A couple of quotes from Canadian Supreme Court Justice LeBel: "My second concern relates to privacy issues. Insofar as is, possible this court should adopt an interpretation of section 3(1)(f) that respects end users' privacy interests, and should eschew an interpretation that would encourage the monitoring or collection of personal data gleaned from Internet-related activity within the home."[91] Further, Judge LeBel continues, "[p]rivacy interests of individuals will be directly implicated where owners of copyrighted works or their collective societies attempt to retrieve data from Internet Service Providers about an end user's downloading of copyrighted works. We should therefore be wary of adopting a test that may encourage such monitoring."[92] This was a dissent and there are some that say this is just one judge and that it does not necessarily reflect the view of the Court. What I think is noteworthy here is that if you take a look back at the briefs and then back at the argument, nobody raised this issue. This was a judge that took a look at the impact that this technology would have and said: "you know what—I must infuse a privacy analysis as part of this test even if the parties themselves chose not to do so." I suspect that there may well be judges that agreed with Justice LeBel but in this particular instance chose not to address the issue, in part, because it was not argued. Judges do not often delve into issues when they are not argued before the court. The Supreme Court will have an opportunity to deal with this some time in the future but the impact of privacy on this issue, even when not argued, is symptomatic of what happens when you infuse the culture of privacy into a country, as we have in Canada, and make privacy a stakeholder.

That does not mean necessarily that we are always going adopt an approach to absolutely protect privacy at all costs. Our Privacy Commissioner has issued a couple of findings over the last month or so about some interesting future technologies: one dealing with biometrics[93] and another dealing with webcam surveillance in the workplace.[94] In the biometrics case, the Privacy Commissioner found that it was an appropriate use of the technology. The technology that was

---

[88] *Id.* at 242.

[89] *Id.* at 242–43.

[90] *Id.* at 239–40.

[91] *Id.* at 242.

[92] *Id.* at 243.

[93] Office of the Privacy Commissioner of Canada, Commissioner's Findings, Summaries of findings under the Personal Information Protection and Electronic Documents Act, *PIPEDA Case Summary #281: Organization uses biometrics for authentication purposes* (2004), *available at* http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp (last visited Mar. 13, 2005); *see also In re* Cascadia Terminal & Grain Workers' Union, Local 333, 2004 C.L.A.S.J. 4301 (2004), *available at* LEXIS, 2004 C.L.A.S.J. LEXIS 111.

[94] Office of the Privacy Commissioner of Canada, Commissioner's Findings, Summaries of findings under the Personal Information Protection and Electronic Documents Act, *PIPEDA Case Summary #279: Surveillance of employees at work* (2004), *available at* http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_e.asp (last visited Mar. 13, 2005).

going to be used was a voice print and the company was able to successfully argue that this was an effective approach to deal with absenteeism from the workplace. On the other hand in a webcam surveillance case in which an ISP was posting webcams throughout the building to monitor their employees, The Commissioner found it was not an appropriate use of the technology. What I think is critical here is that we are seeing, at least in Canada in the short time that we are now experimenting with the private sector, national privacy legislation that does have a direct impact on the way technology is implemented. However, the copyright analysis tells us that there are a couple of ways to deal with the privacy issue within copyright. One is, of course, to be quite explicit about it. Build in tests and requirements and standards within laws to make sure we have an appropriate level of privacy protection. There is another way. Ensure that privacy is, in fact, the stakeholder by creating a culture of privacy. A national privacy law can do that. What you find is that any law regardless of whether or not it has included some of these privacy provisions, actually is interpreted in a context by which privacy itself is very much a critical consideration. Thank you.

V. LESLIE ANN REIS

PROF. REIS:[95] What I would really like to do is put a couple of ideas on the table for the panelists to discuss, time permitting, and to discuss these notions in both how the technology impacts the particular concept or practice and also how to regulate or find the appropriate balance of interests.

---

[95] Leslie Ann Reis is Adjunct Professor of Law and Director of the Center for Information Technology and Privacy Law at The John Marshall Law School in Chicago, Illinois. Prior to becoming an attorney, Prof. Reis worked for more than fifteen years as a broadcast journalist. Prof. Reis is the recipient of numerous awards including a Chicago Area Emmy Award for outstanding achievement in editing. Prof. Reis continues to serve as a consultant for media organizations.

In addition to her academic and administrative duties, Prof. Reis is currently serving as a member of the federal Information Security and Privacy Advisory Board, whose mission is to advise Congress and the U.S. Department of Commerce about issues affecting the security and privacy of information in government computer and telecommunications systems.

In 1996–1997, Prof. Reis was awarded a legal fellowship with the Reporters Committee for Freedom of the Press where she wrote extensively on media, information and technology issues for the Committee's various publications. Prof. Reis co-authored an *amicus curiae* brief to the U.S. Supreme Court in the internet indecency case, *Reno v. ACLU*. Prof. Reis's comments opposing the World Intellectual Property Organization's proposed copyright protection for databases were published in the *Government Information Quarterly*. Prof. Reis has practiced civil rights law in Chicago and is a past Director of the American Judicature Society's Center for Judicial Independence.

Prof. Reis joined the John Marshall faculty in 1997 and currently teaches courses in information law and policy, First Amendment, free speech and privacy rights. Prof. Reis also supervises John Marshall's *Journal of Computer and Information Law*.

Prof. Reis's publications include *The Rodney King Beating – Beyond Fair Use: A Broadcaster's Right to Use Copyrighted Material as Part of a Newscast*, 13 JOHN MARSHALL J. COMPUTER & INFO. L. 269 (1995), *Tapping Officials' Secrets: the Door to Open Government* (1997) (Editor & Contributing Author), *Can We Tape: A Practical Guide to Taping Conversations in the 50 States and D.C.* (1996) (Contributing Author) and *E-FOIA: Introduction to the New & Improved Freedom of Information Act* (1996).

The first idea that came to mind involved a technology that was only briefly touched upon by a couple of our speakers and that is data-mining. In particular, I would like to talk a little bit about the notions of data-mining by government entities. In addition, if there is some time, I would like to touch upon the notion of using technology to either protect or defeat anonymity or anonymous speech and how all of that ties into some of the recent cases, including *Elektra*.[96]

Dr. Geist brought up the question of how did the Renegades get your info.[97] What I really want to talk about, or at least have the panelists address, is not just the use of data-mining technologies in the private sector but, more importantly, the issue of how the data-mining technologies, and again, older technologies and new uses are used by the government. We are obviously very familiar with a number of programs and proposals under consideration under the guise of both national security and creating efficient government under the e-Government Act.[98] The notion of using data-mining technologies to provide an enhanced government to citizen services, in particular, the use or the mining of information collected and maintained by the private sector. This information as Prof. Long briefly mentioned, may fall outside the concepts or the confines of fair information practices.[99] These notions are sometimes adopted by private sector entities, but not always. Certainly information collected and maintained by the private sector falls outside of the protections offered by the Privacy Act of 1974.[100] So I would really love to hear the panelist's views and approaches on how the technology impacts this and what kind of regulatory mechanisms might be appropriate. Mr. von Lohmann, do you want to take the first shot at it?

VI. RESPONSES TO PROF. REIS

MR. VON LOHMANN (responding):[101] I am going to pass on that question. The EFF is increasingly involved in examining the interplay between private database collection and government database collection, but I am not the person with that expertise. Lee Tien, my colleague, has done a great deal of work in this area and we have a great deal of information on our website addressing it.[102] "Total Information Awareness" is the moniker under which this idea was originally floated by the government, and many of its proposals continue to be part of the policy debate. Moreover, I will note that I now live in a state, California, where everyone who is arrested will have their DNA taken and put into a state-administered database, so I do appreciate the issue. However, I will leave it to my expert colleagues to provide the substance.

---

[96] Elektra Entm't Group Inc. v. Does 1–6, No. 04-1241, 2004 U.S. Dist. LEXIS 22673 (E.D. Pa. Oct. 12, 2004).

[97] *See supra* Part IV.

[98] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2932–39 (codified as amended in scattered sections of 5, 10, 13, 31, 40, 41, 44 U.S.C.).

[99] *See supra* Part III.

[100] Privacy Act of 1974, 5 U.S.C. § 552a (2000).

[101] *See* biographical information *supra* note 3.

[102] *See* http://www.eff.org/privacy (last visited Mar. 13, 2005).

PROF. LONG (responding):[103] I think my concern with the issue of "Total Information Awareness" in whatever guise in may take, and I have to admit I was one of these people because as I said I travel internationally who did not fully appreciate this issue until having lengthy discussions with my colleagues sitting with me at the table, is that there is something wrong with collecting personal identifying information for legitimate government purposes. While I do not mind showing you my ID or providing this information, I mind very much what you are going to be doing with it. My concern is that while we think about the "Big Brother is watching you" standard, we forget that Big Brother is also actively involved in commercial enterprises. I can see information being taken under the guise of being the U.S. government, essentially data-mining information, and using it to sell me new posters from the U.S. Postal Service. As a result, I would not only get tickets for the Renegades game, but the U.S. government would now use personal information in order to sell me stuff that they sell out of their commercial branches. I do not think there is any regulations for this, and there needs to be.

DR. GEIST (responding):[104] I am actually more concerned with the public sector side of the equation than I am with the private sector side, although there was an article in the New York Times earlier this week that talked about the size of Wal-Mart's database, and its ability to mine that.[105] I believe they indicated that it was larger than the internet itself, something like 435 million terabytes—or some astronomical number that is literally larger than the internet.[106] There certainly are some private sector groups that have the power to mine an incredible amount of information. In Canada, the debate right now around privacy has to do with public sector information, in particular, data that is out-sourced outside of the country. In addition, there are concerns in Canada in the context of whether the USA Patriot Act[107] or other legislation might well be used by U.S. law enforcement to compel an organization, whether in the United States or even in Canada subject to US personal jurisdiction, to disclose that information in violation of Canadian privacy law.

Now, the B.C. government recently enacted new legislation to actually put up a digital firewall between B.C. and the United States and the rest of the world to try and stop some of this data from flowing out. This set some significant restrictions on what organizations can do with public sector data. In addition, we are talking about two thousand or so different public sector entities. The problem is when you start talking to the outsourcers, the organizations that engage in these kinds of things, they do not have much of a separation in terms of the data warehouses between Canada and the United States. Canada is just the fifty-first state as far as they are concerned. The ability to actually stop data from flowing from Canada into the United States is not as simple as putting a new field in a database. It means either providing a service or not.

---

[103] *See* biographical information *supra* note 14.

[104] *See* biographical information *supra* note 59.

[105] Constance L. Hays, *What They Know About You*, N.Y. TIMES, Nov. 14, 2004, § 3, at 1.

[106] *Id.* (stating that the Wal-Mart database contains 460 terabytes of data).

[107] *See* USA Patriot Act, Pub. L. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8, 15, 18, 22, 31, 42, 49, 50 U.S.C.).

Yesterday one of our federal politicians, Reginald Alcock said he wants to pull all of the Privacy Commissioners from across the country to try to develop a coordinated approach on this particular issue. There is no obvious solution. Canada alone does not just face it—everybody faces it. It is not immediately obvious how you can, on the one hand, ensure there is an effective level of protection of the data and at the same time enjoy the kinds of efficiencies that many would think are essential to provide the sorts of services that we have come to rely upon.

VII. CONCLUDING REMARKS BY PROF. REIS

PROF. REIS:[108] Unfortunately in the interest of time, we will not get to the anonymity issue and perhaps off-line or off-panel we can talk a little bit about that. I just wanted to make one comment, and that is, leave it to the Canadians to come up with the most cogent, clean, decipherable analysis of at least § 215 of the Patriot Act that Dr. Geist was one of the co-authors on.[109] If you have an opportunity to take a look at that in terms of the data-mining and of course the outsourcing issue, its a very, very good document and I am disappointed we did not get more time to talk about that. Thank you.

---

[108] *See* biographical information *supra* note 95.

[109] *See* Michael Geist & Milana Homsi, *The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?,* 6–12 (July 2004) *at* http://www.mgblog.com/resc/Geisthomsipatriotact.pdf; *see also* USA Patriot Act, Pub. L. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8, 15, 18, 22, 31, 42, 49, 50 U.S.C.).