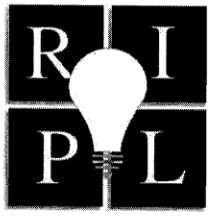
THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW



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?

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.