Ass. Prof. Sonia K. Katyal

# The Dangers of Digital Rights Management in the United States

*Nearly twenty years ago, in a casual footnote at the end of an important essay, an American property scholar, Charles Donahue, drew a distinction between «property as a sword», and «property as a shield». Donahue's distinction symbolized an important difference between two facets of the institution – as well as the execution – of property rights; suggesting that property rights can be used for both defensive and offensive purposes in relationships with third parties.*

[Rz 1] Today, Donahue's distinction[1] offers us a rich metaphor for understanding the transformation that has taken place in the digital era, particularly with respect to the relationship between intellectual property and privacy in cyberspace. As is now clear, the Internet is no longer a smooth-functioning patchwork of anonymous communication between peers. Instead, lurking behind the façade of such potential connections lies an increasing and subtle host of opportunities for legal accountability and detection, particularly where the use (or misuse) of intellectual property is concerned. The result heralds an important shift in property rights in the digital era throughout the world: compared to real space, where property rights tended to serve as a shield from harm, intellectual property rights in cyberspace serve to form the basis for a host of potentially offensive strategies that have deleterious implications for privacy, anonymity, and freedom of expression.

[Rz 2] The purpose of my talk is to focus primarily on the phenomenon of digital rights management in the United States, and to suggest some possible areas for exploration internationally, particularly with respect to the protection of informational privacy. In recent years, strategies of copyright enforcement have rapidly multiplied, each strategy more invasive than the last. Today, the Recording Industry Association of America (RIAA) and other copyright owners maintain automated Web crawlers that regularly survey and record the Internet Protocol addresses of computers that trade files on peer-to-peer networks. Schools, responding to threats from the recording industry, have implemented programs that track and report the exchange of copyrighted files. A few have even decided to audit and actively monitor files traded by their students, at the RIAA's request. And in recent sessions in the United States, there were proposals before Congress that placed intellectual property owners in a virtually unrestrained position of authority over ordinary consumers and intermediaries.

[Rz 3] All of these different strategies share one thing in common: they rely on, invariably, private mechanisms of surveillance for their execution and control. And these techniques of surveillance – whether instituted by private entities, or public law enforcement – demonstrate copyright's increasingly tenuous relationship with information privacy. Recent developments in copyright law in the United States – in particular, the Digital Millennium Copyright Act – have invited intellectual property owners to create extrajudicial systems of monitoring and enforcement that detect, deter, and control acts of consumer infringement. As a result, intellectual property rights have been fundamentally altered – from a defensive shield into an offensively oriented type of weapon that can be used by intellectual property creators to record the activities of their consumers, and also to enforce particular standards of use and expression, proscribing activities that they deem unacceptable.

[Rz 4] The irony, of course, is that both areas of law are facing enormous challenges because of technology's ever-expanding pace of development. Yet, while both areas of law have enormously rich and well-developed areas of scholarly work and analysis, their interactions, particularly across the Internet, have been underappreciated by scholars. Today, however, they are on a collision course that cannot be overlooked much longer, sparked by two major developments in digital space: the rise of consumer surveillance, and the problem of rampant piracy.

[Rz 5] Today, the new piracy surveillance exposes the paradoxical nature of the Internet: it offers both the consumer and creator a seemingly endless capacity for human expression – a virtual marketplace of ideas – alongside an insurmountable array of capacities for surveillance. As a result, the Internet both enables and silences speech, often simultaneously.

[Rz 6] Piracy surveillance regimes take on three basic types, each displaying varying degrees of unilateral aggression: *monitoring*, which involves the use of automated systems to search for protected material; *digital rights*

*management*, which involves a host of actions taken in real space and cyberspace to limit certain uses of intellectual property; and *interference*, which involves a degree of preventative actions taken to prevent peer-to-peer file-sharing from occurring.

**Implications for Privacy and Free Speech**

[Rz 7] Piracy surveillance has inverted the relationship between privacy and property, subordinating the protection of privacy to the protection of property. This has occurred in two basic ways: first, piracy surveillance enables copyright owners to utilize a type of monitoring that demonstrably trespasses on a person's expectations of informational privacy and anonymity; and second, the use of piracy surveillance strategies, without conventional substantive and procedural due process constraints, has a harmful tendency to chill free expression in cyberspace.

[Rz 8] Throughout the world, it is widely recognized that informational privacy is a necessity for the development of the Internet, because data protection is necessary for the flourishment of trust and confidence in cyberspace. [2] Informational privacy is widely described as a right of the individual to «information self-determination.» [3]

[Rz 9] In the United States, there is no specific constitutional right to privacy, informational or otherwise. [4] Instead, the Supreme Court has developed a limited, «penumbral» conception of this right flowing from a variety of constitutional sources – the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments, and a host of later decisions that outline (and often complicate) the borders of this right. However, it is widely recognized that the United States' model for privacy protection is quite limited in terms of the role of the state – here, legal rules are narrowly targeted towards certain sectors, and tend to be thought of as an economic issue; here, privacy protection is normally thought to be an issue that involves consumers alone. [5] In contrast to this limited view of privacy in the United States, in Europe, we see a much more comprehensive approach to privacy protection. [6] Here, legislation strives to create a more complete set of rights and responsibilities – informational privacy is viewed as an issue of human rights, rather than a set of market-based considerations. [7]

[Rz 10] Finally, aside from these two largely divergent approaches between the United States and Europe, we also see a third set of considerations – those that are technical protections for privacy. As my colleagues Joel Reidenberg and Lawrence Lessig have pointed out, information privacy is also governed by a sort of «code», or a set of technical rules and engineering specifics that establish norms for protection of privacy. [8]

[Rz 11] On one hand, these methods of piracy surveillance allow intellectual property owners to ensure that their works are not being used for the purposes of piracy and counterfeiting. However, these private regimes of copyright enforcement carry some disadvantages, especially where privacy and data self-determination are involved.

[Rz 12] Digital Rights management forces individuals to disclose their identities, often for the purposes of marketing and consumer surveillance, instead of solely for protection against piracy. These have strong implications for privacy – both in the United States and internationally. As I argued earlier, the United States has a typically much more limited view of informational privacy protections, in stark contrast to Europe, which has a much more protective view of informational privacy as a basic human right.

[Rz 13] However, the technology of piracy surveillance knows no borders. In cyberspace, piracy surveillance enables ISPs to monitor and record the activities of their subscribers, thereby affecting the autonomy, anonymity, and privacy individuals enjoy in cyberspace. Moreover, there is some evidence that the technologies used to detect infringement can make mistakes, and it can be used for the purposes of censorship rather than copyright protection.

[Rz 14] Finally, piracy surveillance affects the audience's ability to access information without interference. And so, I would argue that we should be thoughtful, and somewhat critical – of the idea that digital rights management strategies can be successfully implemented throughout the world, particularly in Europe, which has a much stronger regime of protecting privacy than in the United States.

[Rz 15] In conclusion, this conflict between privacy and piracy is important not just because it showcases a new, overlooked mode of surveillance, but also because it demonstrates the need to resolve conflicts between them in ways that are reflective – and protective – of the relationship between modern technology and personal freedoms. I

conclude, therefore, by pointing out the need for greater public oversight over these private realms of surveillance, and suggest a number of ways in which we can envision a more protective sphere for individual autonomy in cyberspace.

---

Associate Professor of Law, Fordham University School of Law. Please note that this article is adapted from parts of two previous articles, *Privacy vs. Piracy*, 7 Yale Journal of Law and Technology 222 (2005); and *The New Surveillance*, 54 Case Western Law Review 297 (2004). For further exploration, please note that both articles can be downloaded without charge at http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=115375.

Résumé français de l´exposé de Prof. Sonia K. Katyal aux journées d´informatique juridique 2005 à Berne: Alain Clément, Le copyright aux USA: un exemple pour le reste du monde?, in: Jusletter 7. November 2005.

Deutsche Zusammenfassung des Referates von Prof. Sonia K. Katyal an der Tagung für Informatik und Recht 2005 in Bern: Maria Pia Portmann-Tinguely, Das US-Copyright für den Rest der Welt?, in: Jusletter 7. November 2005.

---

[1] Charles Donahue, Jr., *The Future of the Concept of Property Predicated From its Past*, *in* Property 28, 67-8 n.104 (J. Roland Pennock & John W. Chapman eds., 1980).
[2] Joel Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 Stan. L. Rev. 1315, 1325 (2000).
[3] Id.
[4] *See* U.S. Const. amend. I, III, IV, V, IX, XIV.
[5] Reidenberg, 52 Stan. L. Rev. at 1331.
[6] Reidenberg, 52 Stan. L. Rev. at 1330.
[7] Id.
[8] Reidenberg, 52 Stan. L. Rev. at 1331.

Rechtsgebiet: Informatikrecht
Erschienen in: Jusletter 7. November 2005
Zitiervorschlag: Sonia K. Katyal, The Dangers of Digital Rights Management in the United States, in: Jusletter 7. November 2005
Internetadresse: http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=4344