

## **DRM and Privacy**

**Julie E. Cohen**

The future of online privacy is increasingly linked to the future of online copyright enforcement. In their push to control the proliferation of unauthorized copies, copyright owners and their technology partners are building into the technologies of digital rights management (DRM) a range of capabilities that implicate the privacy interests of users. The potential consequences of DRM for user privacy warrant far greater attention from policymakers and systems designers than they have received.

DRM initiatives may be envisioned as a series of concentric levels of control, each penetrating more deeply into the user's home electronic and computing environment.

At the simplest, DRM systems can impose direct restrictions on what individuals can do, in the privacy of their own homes, with copies of works they've paid for. The recent test marketing by several recording companies of copy-protected music CDs is perhaps the most publicized example; others include the Content Scrambling System (CSS) designed to prevent users from copying movies embedded in DVDs and software restrictions preventing the space-shifting, or device-shifting, of e-books.

At the next level of control, DRM systems can report back to the copyright owner of work on the activities of individual users. Such reporting may occur as part of a pay-per-use arrangement for access to the work or independently of payment terms; for example, the system might be designed to report attempts to make unauthorized copies or to determine which other software programs a user is running in conjunction with the DRM-protected program. DRM systems can also incorporate more broadly directed spyware. In 1999, RealNetworks distributed media player software that searched users' systems for information about their musical preferences, as well as about other software products that they had installed. At least one recent version of Netscape's SmartDownload software recorded every Web site visited by users who had installed both SmartDownload and Netscape's Communicator browser and transmitted that information to Netscape.

Each of these systems is relatively self-contained, encompassing only a particular type of content and requiring implementation in no more than a few complementary pieces of software or equipment. Each of the next two levels of DRM control seeks to embed direct enforcement and spyware functionality more globally by moving both functions deeper into the logical and physical layers of the user's electronic environment {1}. Microsoft's Palladium initiative seeks to embed standards for authenticating "trusted" programs and files at the operating-system level. The Trusted Computing Platform Alliance, a joint venture of Compaq, Hewlett-Packard, IBM, Intel, and Microsoft, is attempting to develop shared standards for implementing DRM controls in both software and hardware. An effort to develop DRM standards for high-definition television is also underway and some copyright interests are pushing for federal regulations mandating the adoption of a "broadcast flag" designed to identify copyright-protected content.

The capabilities of DRM systems implicate two different types of privacy interests in the circumstances of intellectual consumption.

Direct functionality restrictions intrude on the seclusion, or "private space," that long-established social practice reserves to the individual or family, and force changes in a set of

behaviors occurring within that space {4}. In so doing, they shift the baseline conditions of user autonomy to determine the circumstances of use and enjoyment of intellectual goods.

Spyware, in contrast, implicates privacy interests that are primarily informational. Information supplied by DRM technologies can be used to build a dossier about the user's informational preferences and patterns of use. This information in turn can be sold to data aggregators or obtained by the government and used for a variety of purposes. In Western cultures, information about intellectual activity has long been regarded as fundamentally private, both for reasons related to individual dignity and because of the powerful chilling effect that disclosure of intellectual preferences would produce. In the U.S., intellectual activity also lies close to the core of the interests protected by the First Amendment {3}. For this reason, several recent federal court decisions have set high standards for compelled production of this information in legal proceedings brought by the government.<sup>1</sup>

Whether these privacy interests are legally enforceable against private actors employing DRM systems, and to what extent, are much more difficult questions.

Although copyright law does not speak directly to the privacy interests of users of copyrighted works, it is implicitly protective of user privacy. The Copyright Act does not give copyright owners the exclusive right to control all uses of a copyrighted work or the right to conduct surveillance of users. It confers a much more limited set of rights and further truncates these rights with a series of express limitations. Two of these in particular – the first-sale doctrine and the fair-use doctrine – shield a range of actions users might take in private spaces, including time- and space-shifting and lending. Other informational products (such as wholly unoriginal databases) are not protected by copyright law at all.

However, copyright owners and other information providers argue that this baseline distribution of rights and limitations may be altered by contract, or “license,” the terms of which users are free to accept or reject. If this is right, then there is no reason the range of enforceable contractual restrictions could not include restrictions that diminish user privacy. But this position is far too simplistic.

Most people agree that many contractual restrictions on the use of copyrighted (or uncopyrighted) content are legitimate but also that some public policies should not be altered by contract. One example is the copyright rule that one is free to criticize or parody a copyrighted work; another is the general rule that one may not contract into a state of slavery. Do user privacy rights or some subset of them warrant similar protection?

In the U.S., the common law of privacy does not yet provide clear guidance as to the scope of privacy in the digital age. The tort of intrusion upon seclusion traditionally has focused on preventing physical and audiovisual invasions. No court has considered whether it similarly protects against the insertion of data sensors (such as spyware) or of devices that drastically restrict behavior but without reporting back. Arguably, both types of conduct threaten the interests that the tort is intended to protect {4}, but courts reasoning from precedent will need to be convinced to take that step. Moreover, in the context of DRM a court would also need to consider whether and to what extent these interests are or should be waivable.

---

<sup>1</sup> *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media Law Reporter 1599 (D.D.C. 1998); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002).

The fit between current judicial conceptions of privacy and informational privacy concerns is equally imperfect. The tort of “unauthorized appropriation of name or likeness” traditionally has focused on the improper use of pictorial images. So far, when asked to apply this tort to the digital “likenesses” generated by consumer-profiling activities, courts have resisted, though such resistance may diminish as profiling becomes more comprehensive and its harms more widely felt and acknowledged. Alternatively, based on the potential chilling effect of intellectual profiling, one could invoke the tort prohibiting disclosure of embarrassing private facts. This tort, though, has more often been applied to disclosure of sexual or intimate information; again, then, one would need to persuade courts to take a broader view of what is or should be considered “private.” Again, too, there is the omnipresent question of contractual waiver.

Federal privacy statutes protecting computers and electronic communications also are unhelpful in the context of DRM. The RealNetworks and Netscape products described earlier are now the subject of class actions alleging, respectively, violations of the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA). However, neither statute was designed to address this sort of overreaching. The CFAA prohibits only unauthorized access to computer systems, or access that exceeds the scope of authority.<sup>2</sup> The ECPA’s prohibitions against interception of electronic communications do not extend to interception that is consensual or that is undertaken by one of the parties to the communication.<sup>3</sup> Thus, it is hard to see how either statute would prohibit the implementation of DRM functions that have been disclosed and purportedly agreed upon.

The questions that law- and policymakers must confront, then, are whether the privacy invasions caused by DRM restrictions should be legally cognizable and, if so, whether such restrictions may legitimately be imposed under contract, regardless of their invasiveness. There are good reasons to conclude that the scope of privacy in intellectual consumption is a matter of considerable public policy importance and that the law should provide at least some inalienable privacy protection for users of intellectual goods.

As the above discussion of privacy tort theories suggests, courts already have the tools to recognize and extend to user a range of privacy interests better suited to the digital age. Responding to changing circumstances by redefining legally cognizable injury and responsibility is a central role of the courts. Many legal rules that we take for granted today simply did not exist 40 or 50 years ago. Consider, for example, the law of strict products liability, under which an injured consumer may recover damages directly from the manufacturer of a defective product, even if there is no privity of contract. And consider the law of sexual harassment, which recognizes that sex-based hazing in the workplace can amount to discrimination in violation of federal law. Given the unprecedented threats to intellectual privacy enabled by new technologies for digital distribution of intellectual goods, a similar process of redefinition makes sense here.

DRM developers and standards bodies also should be encouraged to address the privacy interests of users by incorporating privacy protections into their systems and standards. Stronger privacy protection is not necessarily incompatible with stronger copyright enforcement. DRM

---

<sup>2</sup> Computer Fraud and Abuse Act, 18 U.S.C. §1030.

<sup>3</sup> Electronic Communications Privacy Act, 18 U.S.C. §§ 2511, 2701.

*Communications of the ACM*, vol. 46, no. 4, 47-49 (Apr. 2003)

controls can be designed to be “leaky,” allowing users greater flexibility to access and use information goods within private spaces, and anonymization techniques can lessen at least some of the informational privacy concerns {2}.

In the emerging age of digital information, the proper balance between DRM and user privacy is an important subject for public debate. The time to begin this debate is now, while infrastructures and standards for DRM are still evolving.

### **References**

1. Benkler, Y. From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access. *Fed. Commun. Law J.* 52, no. 3 (May 2000): 561-579.
2. Burk, D. and Cohen, J. Fair use infrastructure for rights management systems. *Harvard J. Law & Tech.* 15, no. 1 (Fall 2001): 41-83.
3. Cohen, J. Copyright and the jurisprudence of self-help. *Berkeley Tech. Law J.* 13, no. 3 (Fall 1998): 1089-1143.
4. Cohen, J. A right to read anonymously: A closer look at “copyright management” in cyberspace. *Connecticut Law Rev.* 28, no. 4 (Summer 1996): 981-1039.

**JULIE E. COHEN** (jec @law.georgetown.edu) is a professor of law at the Georgetown University Law Center, Washington, D.C.