Digital rights management (DRM) refers to the technologies and methods for controlling access to digital data and tracking their use. DRM supports mandatory access controls through cryptographic protocols and other protection measures. Producers of entertainment content, software and other forms of intellectual property use DRM technologies to limit the ability of both consumers and would-be thieves to copy and redistribute intellectual property. The next phase in the evolution of this technology should be the utilization of DRM in Web, e-commerce and database applications to protect consumer data from unauthorized use or redistribution.

Intellectual property rights holders perennially lobby for governments to mandate and regulate the adoption of DRM. For example, at the request of a Hollywood interest group, the FCC has repeatedly proposed limiting the ability of consumers to record television content at home and the ability of companies to produce digital video recorders by imposing a mandate called the “Broadcast Flag.” Governments, vendors, and rights holders should approach this matter carefully as government mandates limit the ability of innovators to introduce new technologies as well as the ability of consumers to purchase goods on the free market. In addition to being anti-market, mandates may be technically unwise. Mandating a potentially broken content-protection system would not be in the interests of any party.

Much of the commentary on DRM technologies from consumer and privacy-rights advocates focuses on threats such as the disclosure of consumer data or the erosion of fair-use rights. Although the risks associated with DRM are real, it is possible that consumer privacy could also benefit from DRM technologies. If DRM mandates appear to be inevitable, consumer and privacy rights advocates may want to calculate a shift in strategy. If it is reasonable to limit the ability of consumers to copy digital data by requiring manufacturers to embed DRM capabilities into new products, it may also be reasonable to implement DRM in Web, e-commerce and database applications so that the personal information of consumers can also receive protection.

At this time, most corporate privacy policies are all-or-nothing affairs that act to deprive consumers of any right to control personal information once remitted. To receive services one must typically agree to elaborate corporate policies that, in some cases, act to deprive consumers of any rights regarding privacy, product liability and merchantability of goods. Even when such
contracts border on the unconscionable, consumers feel forced to agree to the terms in order to receive services. Consumers should have the right to delegate privileges regarding their personal information more finely than currently possible when engaging in such contracts.

Through DRM technologies, consumers engaging in electronic commerce could grant vendors and suppliers a license to access and utilize certain aspects of the consumers’ data. This would enable a consumer to grant a read/write license to some creditors, perhaps as a function of a mortgage agreement, and provide a read-only license to a limited subset of the data for simple transactions such as shipping agreements and online orders. Such a license would empower consumers to prevent entities from misusing or reselling consumer information.

There are both positive and negative consequences to any technological change. Because producers need to protect themselves from intellectual property theft, DRM technologies appear to be here to stay. Instead of fighting against all change in this matter, privacy rights advocates should take a seat at the negotiating table and attempt to ensure that vendors implement DRM technology in a manner that protects and serves consumer privacy rights.

***

You can reach Robert Guess at <mailto:tcguesr@tcc.edu>.

***


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 Robert Guess & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.