APPENDIX G

The Digital Millennium Copyright Act of 1998 and Circumvention of Technological Protection Measures

INTRODUCTION

The World Intellectual Property Organization (WIPO) treaty seeks to harmonize different countries' treatment of the ownership and protection of intellectual property, in order to enable the growth of global commerce in information goods and services. The Digital Millennium Copyright Act of 1998 (DMCA)[1] is the implementation of the WIPO treaty by the U.S. Congress.

As articulated in Chapter 6, many members of the committee believe that the DMCA, although well intentioned and well written in many respects, has some significant flaws with respect to its handling of technical protection mechanisms and circumvention. This appendix, endorsed by those committee members, describes those flaws and suggests ways in which the law's approach to circumvention could be improved.

Simply put, the DMCA makes it illegal, except in certain narrowly defined circumstances, to circumvent an "effective technical protection measure" used to protect a work. The DMCA seemingly makes it illegal (again, except in certain narrowly defined circumstances) to distribute software or other tools used in an act of circumvention, even if this particular act of circumvention is covered by one of the exceptions and, hence, is legal.

---

[1]Public Law 105-304. Relevant excerpts are found in the addendum to this appendix; the full text is available online at <http://frwebgate.access.gpo.gov/cgi-in/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105>.

Given that it is already illegal to infringe copyright, why did the U.S. Congress, in writing the DMCA, feel it necessary to criminalize "circumvention"?

It is a fundamental premise of the DMCA that, for the foreseeable future, the digital-content distribution business will be an important and growing part of the U.S. economy and that technological protection measures will be needed for the success of that business. The DMCA's anticircumvention provisions respond to the (presumed) economic importance of these developments by giving content owners a property right over the technological protection *mechanisms* they deploy, in addition to their existing rights over the *content* that these mechanisms protect. In the physical world, the theft of a tangible object is roughly analogous to copyright infringement; "breaking and entering" the room in which that object is stored is roughly analogous to circumvention. In the words of Callas et al. (1999), it is reasonable to assume that Congress's goal was "[t]o make it a more serious crime to infringe a work that the owner has actively tried to protect than to infringe one that the owner merely stated ownership of." Interpreted as an incentive for copyright owners to protect their own property, rather than to rely solely on the police and the courts, this is a perfectly understandable goal.

Unfortunately, it is far from clear that the DMCA's anticircumvention provisions will have primarily positive effects on content distributors and other interested parties. One problem is that circumvention is a bread-and-butter work practice in the cryptology and security research and development (R&D) community, yet this is precisely the technical community that content distributors are relying on to make effective technological protection measures. If this community is hindered in its ability to develop good products, is it wise to encourage owners to use these products?

It is of course possible that anticircumvention laws will be interpreted by distributors not as incentives to use effective protection measures but, rather, as incentives to do just the opposite—use insufficiently tested, possibly weak protection technology, and increase reliance on the police and the courts to punish people who hack around it. This would result in some cost shifting: Instead of owners and distributors paying for good technology to protect their property, the public at large would likely pay for a greater portion of this protection through the law-enforcement system, although some of the increased costs in enforcement may be borne by the antipiracy efforts of the various information industry associations.

This appendix begins by explaining how the cryptology and security R&D community works and what role circumvention plays in that work. The relevant sections of the DMCA are excerpted and some commentary given on their shortcomings, suggesting ways in which they could be

improved. Formal recommendations on this subject can be found in Chapter 6.

HOW THE CRYPTOLOGY AND SECURITY R&D COMMUNITIES WORK

Understanding the interaction of intellectual property and technical protection services requires an understanding of the research and development process in cryptology and security.[2] A distinguishing feature of these disciplines is that they proceed in an adversarial manner: One member of the R&D community proposes a protection mechanism; others attack the proposal and try to find its vulnerabilities. Using this approach, serious vulnerabilities can be discovered and corrected before the mechanism is fielded and relied on to protect valuable material.

Like most scientific and engineering communities, the security R&D community does both theoretical and experimental work. The theory of cryptology and security is substantial and still evolving, touching on some of the deepest and most challenging open questions in the foundations of computation.[3] A goal of this theory is to study concepts such as privacy, security, tamper resistance, integrity, and proof in a manner that is both mathematically rigorous and relevant to the construction of secure products and services.[4]

One purpose that this study serves is rigorous analysis of security mechanisms. When a technique for protecting digital assets is put forth, there are often follow-up papers demonstrating technical flaws that prevent it from living up to its claims. Sometimes, a purely theoretical analysis is sufficient to show that a proposed protection mechanism is flawed. For example, a follow-up theoretical paper may show that a mathematical assumption made in the original proposal is false or that the class of adversaries against which the proposed mechanism was shown to be "secure" is weaker than the classes of adversaries that exist in the real world.

If pencil-and-paper analysis fails to find flaws in a protection system, should the system be considered secure? No. Before a system is deployed and valuable digital assets are entrusted to it, it should be analyzed experimentally as well. There are several basic reasons that a system that

---

[2]In addition to providing the scientific and engineering foundation for IP management, these disciplines are also widely applicable in other domains, ranging from military system command and control to privacy protection for personal correspondence.

[3]Mathematically sophisticated readers should refer to, for example, Luby (1996) for an introduction to this theory.

[4]A survey and analysis of the policy and market aspects of cryptography may be found in *Cryptography's Role in Securing the Information Society* (CSTB, 1996).