TOWARDS MORE SENSIBLE ANTI-CIRCUMVENTION REGULATIONS

By Pamela Samuelson, University of California at Berkeley

I. INTRODUCTION

The circumvention of technical protection systems and the making of tools to enable such circumventions may seem to financial cryptographers a wholly natural and constructive set of activities. This community knows that it is impossible to make encryption systems more secure unless one tests how strong they are from time to time by trying to break them. However, now that other industries, notably entertainment industries, are relying on encryption technologies to protect information in digital form, it should not be surprising that these industries have a different perspective about circumvention and circumvention technologies. Copyright industry spokesmen are fond of likening the act of circumventing a technical protection system to "breaking and entering" a dwelling; they also liken the tools built to enable circumvention to "burglars' tools," the possession or sale of which has been outlawed in numerous states. The Digital Millennium Copyright Act (DMCA) anti-circumvention regulations, enacted by the U.S. Congress in October 1998, on which this paper will mainly focus, address the concerns of these industries that circumvention of technical protection systems substantially threatens the viability of copyright industries such that both the act of circumvention and the making of circumvention-enabling technologies need to be heavily regulated.

This paper will first review the circumstances that led to the adoption of the DMCA anti-circumvention regulations. It will then describe those regulations in some detail, and go on to discuss problematic aspects of the regulations. The paper will also suggest some ways in which the DMCA anti-circumvention regulations might be improved. Much as financial cryptographers might ardently wish for a repeal of these rules, this is realistically not going to happen. The best that the financial cryptography community can hope for is a narrowing of the regulations to do less damage to the evolution of sound cryptology than the current regulations may well do. Cryptologists from other nations need to pay attention to the DMCA regulations in part because the United States government has been working hard to persuade other nations to adopt equally strong, if not stronger, anti-circumvention regulations. With the assistance of the cryptology community, perhaps other nations will adopt more sensible anti-circumvention regulations. If so, these may help to serve as models to which U.S. law may eventually adapt.

II. ORIGINS OF ANTI-CIRCUMVENTION REGULATIONS

The Clinton Administration did not invent the concept of anti-circumvention regulations. Laws forbidding the manufacture, sale, and use of black-box decoder boxes for viewing encrypted cable television or satellite transmissions, for example, predate the DMCA. Hollywood had previously tried to get similar generalized anti-circumvention legislation, although Congress had always rejected such proposals. However, the Clinton Administration's so-called "White Paper" on "Intellectual Property and the National

Information Infrastructure" published in September 1995 strongly endorsed this legislation. The White Paper observed that copyright owners were investing in development and use of various kinds of technical measures to protect their works from piracy in digital networked environments. A ban on circumvention technologies was necessary, the White Paper argued, to induce copyright owners to make digital works available via the Internet. The report proposed to outlaw the manufacture and distribution of technologies, the primary purpose or effect of which was to bypass technical protection systems used by copyright owners to protect their works.

At about the same time, the Clinton Administration was proposing that a virtually identical anti-circumvention rule be included in a draft treaty on digital copyright issues scheduled for consideration at a diplomatic conference in December 1996 at the headquarters of the World Intellectual Property Organization (WIPO) in Geneva. Even though the draft treaty included a White Paper-like anti-circumvention rule, shortly before the diplomatic conference commenced, the Clinton Administration decided not to support the draft treaty proposal because there was such strong domestic opposition to the White Paper-like provision. U.S. negotiators to the WIPO diplomatic conference were under instructions to support a more neutral anti-circumvention rule which called upon nations to provide "adequate protection" and "effective remedies" to deal with circumvention of technical protection systems used by copyright owners to protect their works. The WIPO Copyright Treaty (WCT) adopted this approach to anti-circumvention regulation.

For well over a year after the diplomatic conference, the Clinton Administration's preferred legislation to implement the WCT was stalled in Congress. The principal opposition to the legislation came from telephone companies and online service providers (OSP) because the White Paper had taken the position that these institutions were and should be held strictly liable for infringing acts of their users, regardless of whether the companies knew of any infringement or not, or were able to control acts of infringement. In March of 1998, major copyright industry groups and telco-OSP groups agreed to add four "safe harbor" provisions to the DMCA so that telcos and OSPs could conduct business as usual and only be responsible for copyright infringement if they knew of infringing activities and did nothing about it.

Once the OSP compromise broke the legislative logjam, it was clear that the DMCA was going to be enacted. Although the anti-circumvention regulations continued to breed controversy, telcos and OSPs had spent virtually all of their political capital on the safe harbor provisions. Even major companies such as AT&T with encryption research groups likely to be adversely affected by broad anti-circumvention regulations did little or no lobbying on the anti-circumvention regulations after the OSP compromise. This left other opponents of broad anti-circumvention regulations in a relatively weak negotiating position. As the next section will show, the anti-circumvention regulations were eventually modified to accommodate certain socially desirable circumventions such as those done in the course of legitimate encryption research. However, the DMCA adopted the basic framework for regulating acts of circumvention and the making of circumvention tools that Hollywood and its allies in the Administration preferred. How

much significance courts will give to the limitations that Congress tried to build into the DMCA anti-circumvention regulations remains to be seen.

III. THE DMCA'S ANTI-CIRCUMVENTION REGULATIONS

There are two kinds of anti-circumvention rules in the DMCA. Section 1201(a)(1) (A) outlaws the act of circumventing "a technical measure that effectively controls access to a [copyrighted] work." Out of concern about the negative impact this rule might have on noninfringing uses of copyrighted works, Congress decided that this rule should not take effect in October 2000, that the impact of this rule on noninfringing uses of copyrighted works should be studied regularly by the Library of Congress, and that the rule should also be subject to seven very specific exceptions and several other more general limitations.

The second kind of anti-circumvention regulation in Section 1201 outlaws the manufacture and distribution of circumvention-enabling technologies (the "anti-device" provisions of the DMCA). Section 1201(a)(2) pertains to technologies that "effectively control access to [copyrighted] works," and 1201(b)(1) to technologies that "effectively protect[] a right of a copyright owner…in a work or a portion thereof." As to each, section 1201 states that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" if it has one or more of the following three characteristics: (1) if it is "primarily designed or produced for the purpose of circumventing [technical] protection," (2) if it has "only limited commercially significant purpose or use other than to circumvent [technical] protection," or (3) if it is "marketed by that person or another acting on its behalf with that person's knowledge for use in circumventing technical protection."

Section 1201(a)(1)(A) is subject to seven specific exceptions, three of which also contain exemptions from one or both of the anti-device rules. From the standpoint of the financial cryptography community, the most important exception applies to circumventions conducted in the course of legitimate encryption research. A second important privilege enables circumvention for purposes of computer security testing. A third allows circumvention of a technical protection system when necessary to achieve interoperability among computer programs. A fourth permits circumvention in the course of legitimate law enforcement and national security activities by governmental actors. The other three exceptions pertain to information privacy protection, parental control of access to harmful material by children, and certain acts by libraries.

The DMCA also contains some more general provisions that seem to limit the scope of the anti-circumvention regulations. One clarifies that software and hardware manufacturers are under no obligation to specially design their products to respond to particular technical protection measures. Another arguably preserves fair use as part of the DMCA. A third recognizes that some cases brought under the DMCA might raise First Amendment concerns and indicates Congressional intent that these regulations not be used to diminish free speech or press.

IV. PROBLEMS WITH THE DMCA ANTI-CIRCUMVENTION PROVISIONS

There are three principal problems with the DMCA's anti-circumvention regulations. First, several exceptions to section 1201's prohibitions are too narrowly drawn and ambiguous. Second, there is no general purpose exception to allow courts to exempt acts of circumvention (or the making of circumvention tools) which are clearly justifiable. Third, the DMCA anti-circumvention regulations are too copyright-centric. Each of these problems will be discussed in a subsection below.

A. OVERLY NARROW AND AMBIGUOUS EXCEPTIONS

Financial cryptographers will understandably be most concerned about the narrow scope of the encryption research exception in 1201(g). For one thing, this exception only applies if the cryptographer has asked (even if he or she has not received) permission from the copyright owner to engage in an act of circumvention before the circumvention is accomplished. Second, the statute emphasizes the need for a cryptographer to be an expert in order to qualify for this exemption even though some of the most brilliant minds in the field of cryptology lack formal training. Third, the statute permits a cryptanalyst to make tools to bypass access controls, but is silent on whether tools to bypass use or copy controls are permissible (that is, it contains an exception to one but not both of the anti-device rules). Fourth, it regulates the cryptologist's ability to disseminate the results of decryption (out of concern that dissemination might enable pirates to make illegal uses of the information). In addition, the statute makes it unlawful to bypass "effective technical protection measures" without clearly specifying what that term means. The computer security testing privilege of 1201(j) similarly applies only if the tester asks in advance and likewise allows making tools only to bypass access controls, not copy or use controls. Like 1201(g), it too regulates the tester's dissemination of the results of the testing.

Among the most curious things about four of the five remaining exceptions to 1201(a)(1)(A) is that each neglects to say whether it is okay to engage in tool-making if necessary to accomplish a privileged circumvention. It should be possible to argue that Congress must have intended to create at least an implied right to make a tool to engage in an act of privileged circumvention under 1201. However, it is far from clear that such an argument would succeed, especially given that some exceptions to 1201 explicitly include a tools privilege while others do not. Some courts may think this was a conscious Congressional decision.

Also unclear under the DMCA anti-circumvention regulations is whether fair use can be raised as a defense to section 1201 claims if the circumventor's use of a copyrighted work thereafter is fair and noninfringing, and whether if so, it is lawful to make a tool to accomplish a fair use circumvention. Hollywood's position is that there is no such thing as a fair use circumvention or fair use tool-making. The entertainment industry thinks that it has no obligation to make its work available in a form which would enable fair use to be made of it. It is hoping that courts will agree with it that fair use is only a defense to copyright infringement, not a "right" that users have, and that courts

will decide that fair use has no application in 1201 cases because 1201 is not a copyright infringement statute, but rather an independent right granted to copyright owners which is only limited by the seven exceptions in 1201(d)-(j). However, a number of copyright scholars make statutory and policy arguments in favor of fair use circumventions, and also argue that DMCA's anti-circumvention regulations would be unconstitutional if fair use did not apply to the anti-circumvention rules.

In addition, there is some uncertainty about the scope of the interoperability exception. Section 1201(f) embodies a negotiated compromise among affected industry groups that allows firms to circumvent technical measures if necessary to enable the circumventor to develop an interoperable computer program. Although the interoperability exception to 1201(a)(1)(A) contains an exception to both anti-device rules of the DMCA, it may be narrower than is socially desirable in a different respect.

To illustrate this point, consider the ruling so far in the high profile case brought by Universal City Studios against Eric Corley (aka Emmanuel Goldstein) and 2600 Magazine under the DMCA's anti-circumvention regulations. This suit challenges Corley's decision to post a computer program known as "DeCSS" on the website of the 2600 Magazine site and to link to other websites where DeCSS has been posted as violations of 1201(a)(2). The DeCSS program can be used to bypass the Content Scrambling System (CSS), a technical protection measure used to control access to DVD movies. Defense lawyers in the *Corley* case have argued that the case should be dismissed because the DeCSS program qualifies for the interoperability privilege of 1201(f). DeCSS was designed, they argue, to enable people to build software that would enable them to play legitimately purchased DVD movies on their platform of choice, namely, Linux computer systems.

In a preliminary ruling, the trial court rejected this defense on three grounds: first, because the defendants offered no evidence to support this contention; second, because the defendants themselves had not been trying to make an interoperable system, and hence, they didn't qualify for the privilege; and third, because 1201(f), in the court's view, only permitted circumvention for purposes of achieving program-to-program interoperability, whereas DeCSS, in its view, enabled program-to-data interoperability which 1201(f) did not cover.

In subsequent proceedings, declarations of several computing professionals have provided an evidentiary basis for the DeCSS interoperability defense. Given how hostile the trial judge was to this defense previously, it would be surprising for him to rule in Corley's favor on the 1201(f) defense in later rulings, but perhaps an appellate court will see things differently. The interoperability of digital data may, however, be quite as competitively important as interoperability among programs. The trial judge was correct, though, in observing that 1201 on its face only covers the latter and not the former. Whether circumvention should be permitted for other legitimate reverse engineering purposes, or only for interoperability purposes, is also worthy of consideration.

B. NEED FOR A GENERAL PURPOSE EXCEPTION

Given the complex specificity of the seven exceptions to 1201(a)(1)(A), it may be obvious why a general purpose "other legitimate purpose" circumvention exception should have been included in the DMCA. To comprehend why it was not, one must understand the intense political struggle during which these rules were framed and adopted. Hollywood initially wanted no exceptions to the anti-circumvention rules at all, although they were willing to accept an exception to enable law enforcement and national security officials to circumvent technical measures when necessary to do their jobs. The legislation proposed to Congress contained a law enforcement/national security exception.

After Hollywood and its allies compromised more than they'd expected over the OSP liability provisions of the DMCA, they were in no mood to compromise any further, especially not on the anti-circumvention regulations that then became their primary legislative objective. Copyright industry lobbyists deserve credit for the masterful job they did in persuading Congressional committees that broad anti-circumvention regulations were absolutely essential to prevent piracy on the Internet (even though the need was not, in fact, proven).

Congress did, however, pay some attention to critics of the anti-circumvention rules. When witnesses at legislative hearings could document with precision why a certain circumvention activity (such as encryption research) ought to be privileged, legislators would add another exception to 1201(a)(1)(A) to deal with it. Thus did the motley crew of exceptions become part of the DMCA. An unfortunate result of this process was, however, that Congress only created exceptions for those circumstances which it already understood to be a problem. It did not recognize the possibility that other legitimate reasons to circumvent technical protection measures might exist and add a general purpose exception to deal with them.

There are many legitimate reasons for circumventing technical measures that are not covered by existing exceptions to 1201. Suppose, for example, a firm received an encrypted digital object which it suspected contained a highly destructive computer virus or worm. The only way to find out if these suspicions were valid would be to circumvent the encryption to see what was inside. A strict interpretation of 1201 would make the act of circumvention illegal (because the virus inside very likely qualifies as an "original work of authorship" which copyright law would protect); a strict interpretation would also make it illegal to make a tool with which to circumvent the technical measure. Other examples would include the need of a firm to circumvent a technical measure to detect whether an infringing copy of a copyrighted work or child pornography was inside the encrypted object.

Congress should have added a general purpose "or other legitimate purposes" exception provision to section 1201 to deal with these kinds of legitimate circumventions. Without such a provision, courts will either have to contort the law or reach unjust results. A general purpose exception would add flexibility, adaptability, and fairness to the DMCA's anti-circumvention rules. In many other parts of copyright law—the fair

use doctrine, for example—Congress has trusted the courts to employ a situationally-based analysis to distinguish between legitimate and illegitimate activities. It should have done so with respect to the anti-circumvention rules as well.

C. COPYRIGHT-CENTRICITY OF DMCA ANTI-CIRCUMVENTION RULES

The DMCA anti-circumvention regulations were obviously designed to respond to concerns of copyright industry groups. The copyright-centric mindset of these industries helps to explain why they initially resisted any attempt to create exceptions allowing circumvention of technical protection measures for such legitimate purposes as encryption research and computer security testing: these industries simply didn't perceive that the regulations had implications for these and other legitimate activities. Congress eventually understood some of the harmful implications of overbroad DMCA proposals and adopted specific exceptions. This subsection will argue that Congress did not foresee other possible misapplications of the DMCA. It will also suggest that it is possible that if Congress had thought through anti-circumvention issues more carefully, it might have realized that in certain respects the DMCA's anti-circumvention regulations were too narrow.

The potential for unforeseen applications and possible misapplications of the DMCA anti-circumvention regulations becomes obvious once one recognizes that copyright industries are not the only entities using technical measures to protect digital information. Trade secret owners, privacy-seeking individuals, and others possessing confidential information (including the Department of Defense as to classified documents) also use technical protection measures, as do purveyors of electronic cash systems, to protect their legitimate interests in digital information. These parties may be as concerned as copyright owners about threatened losses arising from circumvention and circumvention technologies.

Initially, none of these parties might think of using the DMCA to challenge acts of circumvention or circumvention technologies, but consider this: Copyright law in the U.S. and elsewhere typically protects original works of authorship that have been fixed in some tangible medium of expression (e.g., printed on paper or stored on a ROM chip). Rights under copyright law subsist in protected works automatically by operation of law from the moment of their first fixation and last for at least 70 years in the U.S. and E.U. (and at least 50 years in most other nations).

Some of these non-copyright firms or individuals might be entitled to challenge circumventors under the DMCA. A person's electronic diary, for example, would almost certainly qualify as an original work of authorship; hence, the diarist could claim copyright in the diary. If she encrypted the diary, she could arguably use the DMCA to challenge any attempt to bypass an access control she used to protect her diary or letter (unless the circumventor was a law enforcement official able to qualify for the DMCA's special law enforcement exception) or anyone who made a tool to bypass it. The fact that privacy may be the paramount interest she really wants to protect through invocation of this law would not seem to bar her DMCA claim. Similarly, many trade secrets are likely

to be embodied in documents that evince the modicum of creativity that would enable them to be protected by copyright law. Even though firms that encrypt trade secrets may not really care about protecting the expression in documents embodying the secrets, it would appear that the DMCA's anti-circumvention regulations could, nevertheless, be used to challenge an act of circumvention or a circumvention technology that the trade secret owner might be worried about. No underlying copyright infringement or actual loss of copyrighted materials, after all, needs to be shown to establish a violation of 1201. In fact, it is unclear as yet whether a plaintiff needs to show any actual harm to win a claim under 1201. (In the *Corley* case, discussed above, Universal City Studios is arguing that harm should be presumed merely because of the availability of a circumvention tool.)

Purveyors of e-cash and government officials who have encrypted classified information may have a more difficult time bringing a DMCA challenge against a circumventor or the maker of a circumvention technology, even though the losses they face may be very serious indeed. Yet, even these parties might succeed under some circumstances. If encrypted cash included some program instructions, not just unoriginal data, and the program instructions were encrypted along with the data, the encryption would be protecting copyrighted material which then might allow the DMCA to be invoked. Although the U.S. government cannot claim copyright protection for government-authored works, it is possible that the government could raise a DMCA claim against a toolmaker if the government used the same encryption technique as a copyright owner and the tool that threatened its classified information also was capable of undoing the encrypted copyright material.

These examples raise at least two key questions: One is whether DMCA claims should be sustainable in what are really non-copyright cases. Regardless of one's perspective on the "should" question, some clever lawyer will surely figure out that the DMCA is broad enough to apply to at least some of these non-copyright situations. Here too, courts are likely to be faced on some occasions with situations in which circumventors have legitimate reasons to bypass technical measures as to which no applicable 1201 exception exists (e.g., as to e-cash, one might need to bypass the technical protection system to get access to audit trail information).

A second key question is whether it would have been better to think more holistically about circumvention and circumvention technologies and adopt a more general rule about them (including appropriate exceptions) so that the legitimacy of circumvention and circumvention technologies might be viewed more broadly, and not solely through the lens of a copyright industry-oriented law. It would make more sense to do this than to broaden the DMCA anti-circumvention rules to deal, for example, with the e-cash and classified information circumventions discussed above. How Congress would have dealt with anti-circumvention regulations if it had recognized the more general problem that circumvention and circumvention technologies present for the law cannot be fathomed, but is perhaps worth asking. Perhaps other countries will be wise enough to notice the more general nature of the challenges that circumvention and

circumvention technologies pose for the law and attempt a more holistic approach to regulating them.

V. CONCLUSION

As ugly and inelegant as anti-circumvention regulations may be to members of the financial cryptography community, these regulations will likely proliferate in national laws around the world. The reason is simple: an international copyright treaty requires signatory nations to provide "adequate protection" and "effective remedies" to protect copyright owners against circumvention of the technical protection measures they may use to protect their works against piracy. The U.S. DMCA anti-circumvention regulations are far from a minimalist implementation of the treaty. Cryptographers from nations that have not already adopted legislation to implement this treaty provision should become active in the legislative process to ensure that encryption research and computer security testing, among other legitimate activities, are not outlawed or unduly burdened by DMCA-like anti-circumvention regulations. U.S.-based cryptographers may need to become active legislatively as well to help Congress understand why certain changes need to be made to the DMCA, such as clarifying and broadening the encryption research and computer security testing exceptions and adopting a general "or other legitimate purpose" exception to the statute to make the law more balanced and effective.

Research support for this paper was provided by NSF Grant. No. SES 9979852. My thanks to Joan Feigenbaum and members of the Program Committee for Financial Cryptography 2000 for the opportunity to present the talk on which this paper was based.

SELECT BIBLIOGRAPHY

COMMITTEE ON INTELLECTUAL PROPERTY RIGHTS IN THE EMERGING INFORMATION INFRASTRUCTURE, NATIONAL RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE (2000) *available at* <http://www.nap.edu/books/0309064996/html/>.

Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998), § 1201 *available at* <http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR:>. [Anti-Circumvention Regulations]

Jane Ginsburg, From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law, COLUMBIA LAW SCHOOL PUBLIC LAW WORKING PAPER NO. 8 (2000) *available at* <http://papers.ssrn.com/paper.taf?ABSTRACT_ID=222493>.

Bruce Lehman, Patent and Trademark Office, REPORT OF WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS OF INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY RIGHTS AND THE NATIONAL INFORMATION INFRASTRUCTURE (Sept. 1995), *available at* <http://www.uspto.gov/web/offices/com/doc/ipnii/>. [White Paper]

David Nimmer, A Riff On Fair Use In The Digital Millennium Copyright Act, 148 U. PA. L. REV. 673 (2000).

Pamela Samuelson, Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised, 14 BERKELEY TECH. L. J. 519 (1999) available at <http://www.sims.berkeley.edu/~pam/papers/Samuelson_IP_dig_eco_htm.htm>.

WIPO Copyright Treaty, adopted by the Diplomatic Conference on Dec. 20, 1996, WIPO Doc. CRNR/DC/94 (Dec. 23, 1996) *available at* <http://www.wipo.org/eng/diplconf/distrib/94dc.htm>. [WIPO Copyright Treaty]