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).

has survived all pencil-and-paper attempts to break it could still fail in real use:[5]

- Theoretical analysis of a proposed security mechanism may fail to demonstrate that the mechanism has a flaw but fall short of proving that it is secure in a mathematically rigorous sense. The failure to prove that something doesn't work is not of course equivalent to a proof that it does work.
- Even if a proposal is proven to satisfy a formal security criterion, an implementer may make a mistake in a particular hardware or software implementation of that proposal. Fielded implementations, not abstract specifications, are what real customers will use, and hence implementations must be tested.
- Abstract, provable security criteria may be too costly for product vendors to develop. Developers of secure products make compromises that entail informed guesses about how their products will actually be used, how much money and cleverness will actually be put into attacking them, and with which other products they will interact. Experimentation is needed to test the accuracy of guesses.

A crucial part of experimental security R&D is circumvention (i.e., attack on hardware and software that is claimed to be secure). A research or development team builds a piece of hardware or software, claims that it protects the relevant digital assets, and then challenges the security community to refute its claim (e.g., through vendor challenges). An integral portion of the "security community" comprises nonprofessionals, who can be among the most effective circumventors.

Vigorous, expert attacks should be carried out under the same conditions in which the secure hardware or software will be used or, if those conditions are unknown or infeasible to simulate in the laboratory, under conditions that are as realistic as possible. If such attacks have not been carried out, the allegedly secure system should be regarded as untested and potential users should be as wary as they are of any untested product or service.

In addition to their methodological role in basic research in cryptology and security, experimental attacks on secure hardware and software play an important and growing role in commercial practice. Responsible vendors assemble and fund internal "tiger teams" that try to circumvent a security mechanism before a product relying on the mechanism enters the marketplace. If security is a critical feature of a product or service that a

[5]See *Computers at Risk: Safe Computing in the Information Age* (CSTB, 1991a) and *Trust in Cyberspace* (CSTB, 1999c) for additional discussion.

vendor has offered, prudent customers (a small minority of customers), before signing a large contract with that vendor, often demand the right to have their own security experts or third-party security consultants evaluate the product or service. Such an evaluation should include vigorous experimental attempts to circumvent the security mechanism. These evaluations may also be done by potential strategic partners and by industrial standards bodies, as well as by direct customers. Security consulting firms that routinely attempt circumvention to evaluate products include Network Associates, Counterpane Systems, and Cryptography Research, Inc.[6]

The evolution of the Sun Microsystems' Java programming system illustrates the importance of experimental circumvention to progress in the security R&D world. When Sun launched this innovative system, one of the most important claims it made was that server-supplied executable content could be run safely from any Java-enabled Web browser. Java programmers were supposed to be able to develop software that could be run on any hardware and software platform that supports the Java virtual machine (JVM) and the JVM was supposed to be secure enough to prevent any Java program that had been through its byte-code verifier from damaging the host machine on which it was running. Dean et al. (1996) were skeptical of this broad claim, performed some experimental attacks, and indeed managed to circumvent the JVM security mechanism. Sun Microsystems and Netscape shipped some quick fixes soon after those circumvention attempts succeeded and were publicized. Shortly thereafter, Dean (1997) wrote a more comprehensive analysis of the underlying problem, and Sun's subsequent Java Development Kit, version 1.1, adopted Dean's suggestions.[7]

Numerous examples of attacks, both theoretical and experimental, on proposed security mechanisms can be found in, for example, the proceedings of the International Association for Cryptologic Research (IACR) Crypto and Eurocrypt conferences, the Institute for Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy, the Association for Computing Machinery (ACM) Conference on Computer and Communications Security, the *Journal of Cryptology*, and several comprehensive books, including the one by Menezes et al. (1997). See Anderson (1993) for a thorough and highly readable account of failures in fielded

[6]Information is available at <http://www.nai.com>, <http://www.counterpane.com> and <http://www.cryptography.com>, respectively.

[7]This discussion should not be construed to mean that all of the security issues with Java have been resolved; it is included to serve as an example of the role that experimental circumvention plays in improving security.

automated teller machine security systems. Examples of actual attacks may be found in the Risks-Forum Digest.[8]

Although the security and cryptology community regards the right to "attack" technical protection services as a fundamental part of its work, crucial both to research and to commercial practice, it does not assert that those who are successful in breaking protection services have a right to steal intellectual property that those systems were deployed to protect. Although the pursuit of knowledge about the actual security of products and services that are advertised as secure is a respected and valued activity, the exploitation of that knowledge to commit crimes is not.

At this time, R&D security and cryptology community members are not required to be licensed or have any other special legal or administrative status by the government or by a professional society, to perform experimental circumvention. If a company, university, or government laboratory wants to hire a particular person to test the strength of technical protection services, it is free to evaluate that person's qualifications according to its own criteria; if a person wants to pursue these activities as an amateur, he or she is free to do so, as long as he or she does not do anything illegal. The people who do this sort of work, whether for a living or as a hobby, have a broad range of academic and professional backgrounds, and the field thrives on the multidisciplinary and unpredictable nature of the skills needed to be a good circumventor. For this reason, strong opposition exists in the security R&D community to the idea of developing a licensing process for circumvention activity and trying to use the process to strengthen copyright owners' control over the fate of their property. The effect of a licensing process might just be the opposite (i.e., in fact to weaken the protection for owners). The technical community feels strongly that there is no appropriate licensing body (i.e., there is no group of people well qualified to judge who is likely to be a competent and responsible circumventor) and that any licensing process likely to be developed would have the effect of stifling creativity and dissemination of circumvention results, ultimately degrading the state of the art of technical protection.[9]

---

[8]A discussion list of the ACM Committee on Computers and Public Policy, moderated by Peter G. Neumann, is available online at <http://catless.ncl.ac.uk/Risks/>. Also see *Computer Related Risks* (Neumann, 1995).

[9]The legal status of circumvention activity and the software and hardware tools developed by circumventors is an area in which analogies between intellectual property and some sorts of physical property break down. For example, one has to be a licensed locksmith to practice lock-picking or even to possess lock-picking tools. Otherwise, one is guilty of the crime of possession of burglary tools. There are many possible explanations for this difference in the status of tools that could be used to steal things. For example, it may be that there is an appropriate licensing body for locksmiths and that this licensing

Like other security research results, discoveries of technical flaws in IP protection services should be published in scientific journals and conference proceedings. These publication fora enforce quality control and objectivity, and the ethics of publishing circumvention results in these fora is noncontroversial in the security and cryptology R&D community. Publication in journals and conference proceedings is also inherently slow: At least 6 months, and sometimes as much as 2 years, passes between the submission of a paper and its appearance in print. During the interval between submission and publication, the circumventor can inform a vendor about the flaws in its system, and the vendor can take whatever steps he or she thinks are necessary before the flaws are reported in a paper.

In the 1990s, an alternative, more controversial publication strategy has emerged in the security and cryptology world: the popular media. Now that tens of millions of people are using the Internet and the World Wide Web, privacy, authenticity, anonymity, denial of service, and other security issues are of interest to the general public, and mainstream media report on them. Substantial coverage in the mainstream media, most notably in the *New York Times*, often catapults a researcher into stardom, with predictable consequences for job offers and promotion. This is quite unlike the traditional model of career advancement of researchers coming in proportion to one's standing in a meritocracy regulated by objective peer review. Because its career-enhancing potential is so huge, many security and cryptology researchers actively seek mainstream media coverage when they discover flaws in well-known products and services.

This form of publication is highly controversial in the security R&D community, with both benefits and drawbacks. The advantages of media coverage of results are considerable: Well-written popular articles can raise public awareness of the importance of computer security in general and IP protection in particular. Media coverage also forces vendors of flawed products to pay attention to the problem, denying them the option of hoping that customers won't discover that the tool may not be offering the advertised protection.

But the disadvantages are also considerable. Many popular articles are not well written and, through mistakes or exaggeration, give the impression that a product has been completely broken, when, in fact, the technical flaw that has been discovered is difficult to exploit and may not be practically important in the short run (even if it is potentially important in the long run and hence interesting to researchers). Widespread media coverage may also function as encouragement to criminals to exploit a newly discovered flaw. The security and cryptology community is

---

requirement does not have a chilling effect on lock development; if such is the case, then the two fields of endeavor really are not analogous, even if some of their potential effects are.

divided on the question of whether the pluses outnumber the minuses. Many in the community believe that each case must be considered separately, because no general code of ethics governs all of them.

Experimental circumvention often entails the development of hardware or software that breaks technical protection features of intellectual property (IP) management systems. The ethics governing distribution of these tools are similar to those governing their use: The developer may share his tools with other researchers so that his results can be reproduced and improved upon; he or she may not share them with pirates or anyone else whose goal is illegal appropriation of other people's property, rather than advancement of the state of the art of technical protection (or some other legal goal, including, of course, all legal circumventions defined in the DMCA).

Although most researchers may subscribe to the code of ethics described above, it is clear that there are others who do not. And once a particular circumvention technique becomes available on the Internet, its wide distribution occurs in a very short time span.[10]

DISCUSSION AND CONCLUSIONS

The general approach taken by the Digital Millennium Copyright Act (see addendum below) is to make circumvention illegal except under certain conditions. The legislative approach favored by the crypto and security community is to make *circumvention* legal, while making certain *uses* of circumvention illegal (including, of course, the theft of IP). The DMCA is a fairly good compromise for legislation that makes circumvention illegal except under certain conditions. The relevant sections do a reasonable job of carving out exemptions for the circumvention activities that the community now performs in the daily course of its work. However, there are issues that need to be addressed.

The essential and pervasive problem with the DMCA is that it is vague and uses crucial terms in ill-defined or misleading ways. As a consequence, a practicing circumventor, whether a researcher or criminal, is left without a clear definition of what a "technological protection mechanism" is or of what it means for one to be "effective." Although this may seem like an academic quibble, the example given in Callas et al. (1999) shows that, it is, on the contrary, a real-world concern. Some time ago

[10]For example, Microsoft launched the Windows Media Audio (WMA) format as an alternative to the popular MP3 technology. WMA files can be encoded to restrict playback to a single PC, time period, or number of plays. Almost instantly, cracking software that removes all playback restrictions began making its way around newsgroups and Internet Relay Chat sessions. See Sullivan and Gartner (1999).

there was a computer file system in which one could indicate that a particular file should not be copyable (i.e., there was a "don't copy" flag that could be set); the system's copy command would refuse to copy files on which this flag was set. Undoubtedly, a large fraction of computer users, when presented with a "cannot copy" error message, would conclude that there was no way for them to copy the file and would give up. Anyone with a rudimentary knowledge of computer programming, however, would know that it is trivial to write a program that opens a file, reads the file's contents, and writes them to another file. So is the "don't copy" flag an "effective technological protection measure" or not? Is the exercise of rudimentary programming knowledge that circumvents the flag always, sometimes, or never illegal under the DMCA?

There are several other examples of vague or inaccurate language in the law:

1. Circumvention activity is done by crypto and security R&D people in the course of research, development (of products and services), and consulting. Most of these activities are covered in 1201(g) ("Encryption Research") and 1201(j) ("Security Testing"). Roughly speaking, 1201(g) covers research, and 1201(j) covers development and consulting. However, this division of the material is artificial. It is inaccurate to associate the word encryption with research and the word security with development and consulting. All technical aspects of cryptology and security have to undergo research, development, and consulting. In particular, section 1201(j) should not concern itself only with "accessing a computer, computer system, or computer network." The discussion of "breaking out of the Java sandbox" above is a prime example of "security testing," but it is not an example of "accessing a computer, computer system, or computer network." The Java system security work was done by Professor Ed Felten and his students as a research project at Princeton, but Sun Microsystems could have justified the same project under the rubric of "security testing" before Java was released (and might regret that it didn't).

2. Section 1201(g)(2)(C) is too vague and will leave many well-intentioned crypto and security people unsure about what to do:

> . . . it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if . . .
>
> (C) the person made a good faith effort to obtain authorization before the circumvention . . . .

Important questions that are left unanswered include:

a. From whom is one supposed to obtain authorization? For example, suppose that a software vendor sells a digital library product, the owner of a valuable collection uses that product to control access to the collection, and a computer security expert wants to test the rights-management feature of the digital library product by attempting to get access to the collection without paying for it. Should he or she make a good-faith effort to get authorization from the software vendor, the collection owner, or both?

b. In the same example, suppose that one party grants authorization to circumvent but the other doesn't? Suppose it is the collection owner who has hired the computer security expert to test the product before deploying it; must they make a good-faith effort to get authorization from the vendor to test the product? If the vendor does not authorize the testing, may the collection owner and the security expert still test the product if they purchase it? Must they even seek authorization if the product is available and they buy it in the retail market?

c. Suppose that a request for authorization to circumvent simply goes unanswered. How long must a requester wait for an answer before he is considered to have made a good-faith effort?

3. Section 1201(g)(3)(B) is anathema to the multidisciplinary, extra-institutional culture of the crypto and security community and might inhibit some of that community's best work:

> (3) Factors in determining exemption.
>
> In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include . . .
>
> (B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology . . . .

Amateurs can be some of the best circumventors. Indeed, bugs in protection services are sometimes found by accident. Users may not even know that they are attempting to circumvent; they may simply do something that should work, see that it doesn't, and thus discover a flaw in the protection system. It would be against the interests of all concerned, including the content owners (who want flawed protection services to be fixed), to chill this type of unpredictable, nonprofessional circumvention activity.

4. It is unclear that the U.S. Copyright Office and the National Telecommunications and Information Administration of the U.S. Commerce Department can fulfill the responsibility conferred on them in Section 1201(g)(5):

> (5) Report to Congress—Not later than 1 year after the date of the enactment of this chapter, the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on—
>
> (A) encryption research and the development of encryption technology;
>
> (B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and
>
> (C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.
>
> The report shall include legislative recommendations, if any.

These bodies have little (if any) expertise in cryptology and few (if any) connections to the cryptologic research community.

Congress's implementation of the WIPO treaty provides a cautionary tale about the pitfalls of legislating in the high-tech arena. The extent that digital content distribution will prove to be important to the U.S. economy will not be known until major investments are made by distributors and major experiments are played out in the marketplace. Similarly, the importance of technological protection to the success of the content distribution business can only be determined in real-world competition. In the meantime, Congress has decided in advance that both are important and that the way to solve the problem raised by these important developments is to criminalize a set of activities that are valuable and standard in the high-tech community. The unintended consequences of criminalizing circumvention might ultimately prove to be more important than the problems that the DMCA set out to solve.

ADDENDUM: SECTION 103 OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

(a) In General.—Title 17, United States Code, is amended by adding at the end the following new chapter:

CHAPTER 12—COPYRIGHT PROTECTION AND MANAGEMENT SYSTEMS

Sec.
1201. Circumvention of copyright protection systems.
1202. Integrity of copyright management information.
1203. Civil remedies.
1204. Criminal offenses and penalties.
1205. Savings clause.

Sec. 1201. Circumvention of copyright protection systems

(a) Violations Regarding Circumvention of Technological Measures.—(1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected

[[Page 112 STAT. 2864]]

under this title. <<NOTE: Effective date.>> The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) <<NOTE: Reports. Regulations.>> During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding on the record for

NOTE: The material reprinted in this addendum was obtained from the Web site of the U.S. Copyright Office at <http://www.loc.gov/copyright/>. It is intended for use as a general reference, and not for legal research or other work requiring authenticated primary sources.

purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine—

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

(D) <<NOTE: Publication.>> The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

[[Page 112 STAT. 2865]]

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection—

(A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid,

bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional Violations.—(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection—

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

(c) Other Rights, Etc., Not Affected.—(1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

(2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

(3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

[[Page 112 STAT. 2866]]

(4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.

(d) Exemption for Nonprofit Libraries, Archives, and Educational Institutions.—(1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph—

(A) may not be retained longer than necessary to make such good faith determination; and

(B) may not be used for any other purpose.

(2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.

(3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1)—

(A) shall, for the first offense, be subject to the civil remedies under section 1203; and

(B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

(4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.

(5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be—

(A) open to the public; or

(B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(e) Law Enforcement, Intelligence, and Other Government Activities.—This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsec-

tion, the term 'information security' means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(f) Reverse Engineering.—(1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been

[[Page 112 STAT. 2867]]

readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.
(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.
(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.
(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

(g) Encryption Research.—
(1) Definitions.—For purposes of this subsection—

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(2) Permissible acts of encryption research.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the encryption research was disseminated, and if so, whether

[[Page 112 STAT. 2868]]

it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

(4) Use of technological means for research activities.—Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to—

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

(5) Report <<NOTE: Deadline.>> to Congress—Not later than 1 year after the date of the enactment of this chapter, the Register of Copy-

rights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on—

(A) encryption research and the development of encryption technology;

(B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and

(C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.

The report shall include legislative recommendations, if any.

(h) Exceptions Regarding Minors.—In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which—

(1) does not itself violate the provisions of this title; and

(2) has the sole purpose to prevent the access of minors to material on the Internet.

(i) Protection of Personally Identifying Information.—

(1) Circumvention permitted.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if—

(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;

[[Page 112 STAT. 2869]]

(B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

(C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and

(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

(2) Inapplicability to certain technological measures.—This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

(j) Security Testing.—
(1) Definition.—For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.
(2) Permissible acts of security testing.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.
(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.
(4) Use of technological means for security testing.—Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described

[[Page 112 STAT. 2870]]

in subsection (2), provided such technological means does not otherwise violate section (a)(2).