THE NEW U.S. ANTICIRCUMVENTION PROVISION: HEADING IN THE WRONG DIRECTION

by Jonathan Band and Taro Isshiki
Morrison & Foerster LLP
Washington, D.C.

On October 28, 1998, President Clinton signed into law the Digital Millennium Copyright Act (DMCA),[1] a complex law which makes major changes in U.S. copyright law to address the digital networked environment. Title I of the DMCA amends the Copyright Act to comply with the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty, adopted at the WIPO Diplomatic Conference in December 1996.

Both treaties require contracting parties to provide legal remedies against the circumvention of technological measures which protect authors' copyrights. To comply with this requirement, Congress added a new chapter, Chapter 12, to Title 17 of the United States Code. The new Chapter passed by Congress is much more balanced than the Administration's initial proposal, which was introduced in Congress in 1997. Nonetheless, the final provision still contains deep flaws which will hamper legitimate uses of technology and copyrighted works.

I. Section 1201's Prohibitions: The Administration's Proposal

After the 1996 WIPO diplomatic conference, the United States Patent and Trademark Office began formulating the Administration's proposal for implementing the WIPO treaties. The PTO's proposal was modified by the Office of the General Counsel of the Department of Commerce, which then submitted it to Congress in July, 1997. The Administration's proposal was promptly introduced in both chambers.[2] The basic framework for the Administration's Section 1201 endures in the legislation enacted by Congress.

Section 1201(a)(1) prohibits gaining unauthorized access to a work by circumventing a technological protection measure put in place by the copyright owner to control access to the copyrighted work, *e.g.*, encryption.[3] To facilitate enforcement of the copyright owner's ability to control access to his copyrighted work, Section 1201(a)(2) prohibits manufacturing or making available technologies, products and services used to

---

[1] Pub. L. No. 105-304.

[2] H.R. 2281, 105th Cong. (1997); S. 1121, 105th Cong. (1997).

[3] 17 U.S.C. § 1201(a)(1) (1998). To "circumvent a technological measure" means to "descramble a scrambled work, to decrypt an encrypted work, or otherwise avoid, bypass, remove, deactivate, or impair a technological protection measure." 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 process or treatment, with the authority of the copyright owner, to gain access to the work. 17 U.S.C. § 1201(a)(3) (1998).

defeat technological measures controlling access.[4] Similarly, Section 1201(b) prohibits the manufacture and distribution of the means of circumventing technological measures protecting the rights of a copyright owner, *e.g.*, measures which prevent reproduction. Thus, Section 1201 prohibits two categories of circumvention devices: those that circumvent access control technologies (Section 1201(a)(2)), and those that circumvent copy control technologies (Section 1201(b)).[5] Violation of Section 1201 leads to civil and criminal liability. A repeat offender can be imprisoned for 10 years and fined $1 million.

While the Administration was still formulating its proposal, the manufacturers of multiple purpose devices such as personal computers noted that a PC could be programmed to function as a circumvention device. To ensure that legitimate multipurpose devices could continue to be made and sold, the Administration limited the prohibition to devices that:

(1) are primarily designed or produced for the purpose of circumventing;

(2) have only a limited commercially significant purpose or use other than to circumvent; or

(3) are marketed for use in circumventing.

Even with this modification, the provision still contained a fundamental defect: it prohibited circumvention of access controls for lawful purposes, and it prohibited the manufacture and distribution of technologies which enabled circumvention for lawful purposes. To be sure, the Administration inserted a savings clause (now Section 1201(c)) which states that Section 1201 did not affect rights, remedies, limitations, or defenses to copyright infringement. A defense to copyright infringement, however, is *not* a defense to the independent prohibition on circumvention and circumvention devices established in Chapter 12.

The Administration made another modification which gave the appearance of addressing this issue. Section 1201(b) originally contained a provision parallel to Section 1201(a)(1) -- a prohibition on the act of circumventing a copy control. The Administration eliminated this provision in response to the library and education communities' concerns about the negative impact of the legislation on fair use. The Administration suggested that by eliminating the prohibition on the circumvention of copy controls, a library which engaged in such circumvention for purposes of archival copying permitted under 17 U.S.C. Section 108 would incur no liability. While this is technically correct, the Administration failed to note that so long as Section 1201(b) prohibited the manufacture of devices which could circumvent copy controls, the library had no way of engaging in the circumvention necessary to exercise its Section 108 privilege.

---

[4] 17 U.S.C. § 1201(a)(2), (b) (1998).

[5] Section 1201(b) also prohibits the manufacture of devices which circumvent technologies which protect the copyright owner's other rights under the Copyright Act, including the distribution and performance right.

Thus, the Section 1201 proposed by the Administration would have allowed the copyright owner to circumvent the panoply of exceptions and limitations on the copyright owners exclusive rights established by Congress and the courts over two hundred years. The copyright owner could surround her work with a technological protection, and thereby prevent purchasers from making fair use copies because the necessary devices would not be available. Moreover, under the regime established by Section 1201, the copyright owner could as a practical matter extend the term in the work indefinitely, because the uncircumventable technological protection would prevent reproduction once the term expired.

II. Introduction of Alternatives

Recognizing this basic defect, Senator John Ashcroft and Congressmen Rick Boucher and Tom Campbell introduced alternative legislation implementing the WIPO treaties.[6] The Ashcroft-Boucher-Campbell (ABC) approach read as follows: "No person, *for the purpose of facilitating or engaging in an act of infringement*, shall engage in conduct so as knowingly to remove, deactivate or otherwise circumvent the application or operation of any effective technological measure used by a copyright owner to preclude or limit reproduction of a work or a portion thereof."[7] Unlike the Administration's proposal, the ABC formulation focused only on the act of circumvention, not circumvention devices. Moreover, the ABC formulation targeted not all acts of circumvention, but just acts of circumvention which facilitated infringement. This would have permitted circumvention for non-infringing purposes.

The copyright content community rejected the ABC formulation as too difficult to enforce; it feared that if circumvention devices were available to consumers, consumers would engage in circumvention which would lead in turn to infringement. Accordingly, the content community urged Congress to proceed with the Administration's proposal banning devices.

Notwithstanding the absence of any evidence supporting the content community's concerns of rampant circumvention, Congress decided to follow the Administration's proposal. However, it soon became aware that the Administration's proposal, because of its breadth, prohibited many legitimate activities. Thus, as the bill advanced through Congress, numerous exceptions were grafted onto Section 1201. These exceptions have different thresholds for qualification, and apply to different subsections of Section 1201. The result is a confusing patchwork of prohibitions and exceptions which is sure to encourage litigation and impede innovation. By being overly solicitous of the content community's darkest fears of the Internet, Congress adopted an approach which restricts access to information and threatens technological development.

In Congress's defense, another dynamic was in operation with respect to Section 1201 in addition to over-solicitude to the content community: the grand compromise of the DMCA. Title I of the DMCA -- WIPO treaties implementation -- benefitted the content

---

[6] S. 1146, 105th Cong. (1997); H.R. 3048, 105th Cong. (1997).

[7] S. 1146, § 1201 (emphasis added).

community. Congress offset this benefit with a provision the content community did not want: Title II of the DMCA, which limited the copyright infringement liability of online service providers. In other words, Congress did not consider Section 1201 in isolation, as we are here. Rather, it considered Section 1201 in the context of a much broader piece of legislation, and it concluded that this broader legislation, taken as a whole, achieved a relatively balanced result.

III. Exceptions to Section 1201

Reverse Engineering. Section 1201(f) allows software developers to circumvent technological protection measures in a lawfully obtained computer program in order to identify the elements necessary to achieve interoperability of an independently created computer program with other programs. A person may engage in this circumvention only if the elements necessary to achieve interoperability are not readily available and the reverse engineering is otherwise permitted under the copyright law.[8] Furthermore, a person may develop and employ technological means to circumvent and make available to others the information or means for the purpose of achieving interoperability. In other words, Section 1201(f) provides an exception to all the prohibitions of Section 1201: Section 1201(a)(1)'s prohibition on the circumvention of access controls, Section 1201(a)(2)'s prohibition on the manufacture and distribution of devices which circumvent access controls, and Section 1201(b)'s prohibition on the manufacture and distribution of devices which circumvent copy controls.

This exception is notable in several respects. First, the language describing the acts of reverse engineering which justify circumvention comes directly from Article 6 of the European Union Software Directive. This may well be the first time language from an EU Directive has been incorporated verbatim into the U.S. Code. Incorporation of Article 6 language was no accident. Competing factions of the computer industry have long fought over the permissibility of software reverse engineering. The language of the Software Directive, adopted in 1991, resulted from a compromise between these factions. Accordingly, it was only logical to include this language, which both factions could accept, in the U.S. statute.[9]

Second, the exception represents the first Congressional recognition of the legitimacy of software reverse engineering. To be sure, Congress *did not* say that all software reverse engineering was permissible, or that all copying incidental to reverse engineering would always be a fair use. Rather, Congress simply indicated that it would permit circumvention when the underlying reverse engineering was not an infringement. But permitting circumvention when this condition was met indicates that Congress believed that the condition could be met; that is, that the copying incidental to reverse engineering could be a fair use. This signals Congress' basic agreement with the judicial rulings in *Sega Enters. Ltd. v. Accolade, Inc*., 977 F.2d 1510, 24 U.S.P.Q.2d 1561 (9th Cir. 1992) and its progeny.

---

[8] 17 U.S.C. § 1201(f) (1998).

[9] For a more detailed discussion of the history and meaning of the European Software Directive, *see* Jonathan Band and Masanobu Katoh, *Interfaces on Trial* (1995).

The Senate Judiciary Committee's report could not be clearer on this point. It states that this exception was "intended to allow legitimate software developers to continue engaging in certain activities for the purpose of achieving interoperability to the extent permitted by law prior to the enactment of this chapter."[10] The Committee evidently understood that if a dominant vendor placed on its program a technological measure that prevented reverse engineering, a legal prohibition on circumventing that technological protection could preclude other companies from obtaining the interface information necessary to operate in the dominant vendor's computing environment. Citing *Sega*, the Committee states that "[t]he objective is to ensure that the effect of current case law interpreting the Copyright Act is not changed by enactment of this legislation for certain acts of identification and analysis done in respect of computer programs."[11] The Committee concludes by noting that "[t]he purpose of this section is to foster competition and innovation in the computer and software industry."[12]

In this passage, the Senate Judiciary Committee asserts that *Sega v. Accolade* is good law. Although this is an obvious proposition to serious students of software copyright law, the PTO and the Office of the United States Trade Representative, as well as some software industry representatives, have argued that *Sega* is a minority view not entitled to much deference.[13] This provision of the DMCA should significantly undermine this argument.

Further, in this passage the Senate Judiciary Committee recognizes not only that *Sega* is good law, but also that it is good policy: Reverse engineering "foster[s] competition and innovation in the computer and software industry."[14]

Although Congress crafted a useful exception with respect to software reverse engineering for purposes of interoperability, circumvention (and circumvention devices) enabling reverse engineering for other purposes remains unlawful. Thus, a programmer appears prohibited from circumventing when he is engaged in error correction, Year 2000 remediation, or determining whether the target of the reverse engineering infringes his copyright. Congressman Dingell expressed serious concerns that this exception was too narrow, but did not succeed in broadening it.[15]

---

[10] S. Rep. 105-190 at 32 (1998)

[11] *Id.*

[12] *Id.*

[13] *See, e.g,* Jonathan Band, *Gunboat Diplomacy on the Pearl River: The Tortuous History of the Software Reverse Engineering Provisions of Hong Kong's New Copyright Bill,* Computer Lawyer, Feb. 1998, at 8.

[14] S. Rep. 105-190 at 32 (1998)

[15] "That provision is drafted narrowly to protect reverse engineering that is undertaken solely for the purpose of developing 'interoperable' products. While building 'interoperable' products may be a valuable exercise for software developers and producers of electronic games, many U.S. manufacturers use reverse engineering techniques to build a *better* mousetrap." Statement of the Honorable John D. Dingell regarding the markup of H.R. 2281 (June 17, 1998).

Encryption Research. Congress provided an encryption research exception intended to advance the state of knowledge in the field of encryption technology and to assist in the development of encryption products.[16] Congress recognized that "[t]he development of encryption science requires ongoing research and testing by scientists of existing encryption methods in order to build on those advances, thus promoting encryption technology generally."[17] This testing often involves efforts to circumvent the encryption -- so called "ethical hacking." Circumvention in the course of good faith encryption research may be allowed if the following conditions are met:[18]

(1) the researcher lawfully obtained the copyrighted work;

(2) circumvention is necessary for the encryption research;

(3) the researcher made a good faith effort to obtain authorization from the copyright owner before the circumvention; and

(4) circumvention is otherwise permissible under the applicable laws.

In addition to the above factors, Section 1201 directs the court to consider three other factors:[19]

(1) whether the information derived from the research was disseminated to advance the knowledge or development of encryption technology or to facilitate infringement;

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

(3) whether the researcher timely notifies the copyright owner with the findings and documentation of the research.

Furthermore, a person may develop and employ or provide to his collaborator technological means to circumvent for the sole purpose of performing acts of good faith encryption research. Unlike the reverse engineering exception, which applies to both access controls and copy controls (Sections 1201(a) and (b)), the encryption research exception applies only to access controls (Section 1201(a)).

Although the encryption research community was pleased that it obtained an exception to continue "ethical hacking," it remained concerned that the procedures and

---

[16] 17 U.S.C. § 1201(g) (1998).

[17] House of Representatives Committee on the Judiciary, 105th Cong., Section-By-Section Analysis of H.R. 2281 as Passed by the United States House of Representatives on August 4, 1998, at 16 (Comm. Print Sept. 1998).

[18] 17 U.S.C. § 1201(g)(2) (1998).

[19] 17 U.S.C. § 1201(g)(3) (1998).

limitations imposed by the exception would have a chilling effect on encryption research. Particularly disturbing was the ability to provide circumvention devices only to research collaborators as opposed to the general encryption research market. To address these concerns, the DMCA requires the Register of Copyrights and the Assistant Secretary of Commerce for Communications and Information to report jointly in a year on the effect of the subsection on encryption research, the adequacy of technological measures, and the protection of copyright owners against unauthorized access.

Security Testing. In addition to the encryption research exception, Section 1201 provides another exception for information security activities. The exception for security testing was added during the last days of the 105th Congress to resolve concerns related to the effect of the anti-circumvention provision on efforts to test "the security value and effectiveness of the technological measures" employed to protect "the integrity and security of computers, computer systems, or computer networks." In essence, sometimes the only way to test a computer system's security is to try to break in. The conference report analogizes this to a consumer "installing [a] lock on the front door and seeing if it can be picked."[20] The Conference Committee's report explains that "the conferees were concerned that section 1201(g)'s exclusive focus on encryption-related research does not encompass the entire range of legitimate information security activities. Not every technological means that is used to provide security relies on encryption technology, or does so to the exclusion of other methods."[21]

The security testing exception permits circumvention of access controls conducted in the course of security testing if it is otherwise legal under applicable law.[22] Security testing is defined as obtaining access, with the authorization of the owner or operator of the computer system, to a computer, computer system, or computer network, for the sole purpose of testing, investigating or correcting a potential or actual security flaw or vulnerability.[23] In determining if this exception is applicable, section 1201(j)(3) requires the court to consider whether the information derived from the security testing was used solely to promote the security measures and whether it was used or maintained so as not to facilitate infringement.[24] The conference report makes clear that the circumvention for purposes of security testing can be performed either by the system operator or by firms retained to perform such testing.[25] Section 1201(j)(4) also permits the development, production or distribution of technological means for the sole purpose of performing permitted acts of security testing.[26] Like the encryption research exception, the security

---

[20] H.R. Conf. Rep. No. 105-796, at 67 (1998).

[21] *Id.* at 66.

[22] 17 U.S.C. § 1201(j) (1998).

[23] 17 U.S.C. § 1201(j)(1) (1998).

[24] 17 U.S.C. § 1201(j)(3) (1998).

[25] H.R. Conf. Rep. No. 105-796, at 66-67 (1998).

[26] 17 U.S.C. § 1201(j)(4) (1998).

testing exception applies only to Section 1201(a) (access controls), and not 1201(b) (copy controls).

Law Enforcement and Intelligence Activities. Section 1201 permits circumvention, and the development of circumvention devices, for any lawfully authorized investigative, protective, or intelligence activity by a federal, state, or local government employee, or a person under contract to federal state, or local government.[27] This latter clause is particularly important because it allows the private sector to develop circumvention devices for use by government in law enforcement activities.

Protection of Minors. As the DMCA moved through Congress, concerns were raised that Section 1201 might prevent parents from effectively monitoring their children's use of the Internet. Accordingly, Section 1201(h) was added to allow the development of circumvention components which would permit a parent to access a restricted site visited by her child. Section 1201(h) is drafted so narrowly, however, that few product developers are likely to take advantage of it. Rather than giving a clear exception for such a component, Section 1201(h) merely permits a court to consider whether the component has this beneficial purpose when applying Section 1201. Section 1201(h), does not, however, instruct a court what to do once it does determine that this is the component's purpose. Moreover, Section 1201(h) applies only if the component is included in a product which does not itself violate the provisions of Title I.[28] In other words, a stand alone device intended to perform this function is not permitted. Finally, while Section 1201(h) appears to permit the manufacture of such a device, it arguably does not permit use of the component. This absurd result flows from the ambiguous manner in which the provision was drafted.

Protection of Personally Identifying Information. Section 1201(i) addresses personal privacy concerns by permitting circumvention for the limited purpose of identifying and disabling technological means such as a "cookie" which collects or disseminates personally identifying information reflecting the online activities of the user.[29] This exception applies only: if the user is not provided with 1) adequate notice that information is being collected and 2) the capability to prevent or restrict such collection or dissemination; and if the circumvention has no other effect on the ability of any person to gain access to any work.

This provision has serious flaws. First, a user may not circumvent to protect his privacy if the website notifies him that it has implanted a cookie. Thus, once the user receives the notice, he must choose whether to sacrifice his privacy or to refrain from proceeding further with his online activity. Second, while this provision permits acts of circumvention to protect privacy, it does not specifically permit the development and distribution of the means of effectuating that circumvention; it creates an exception to Section 1201(a)(1), but not Section 1201(a)(2). It is not clear how users are expected to

[27] 17 U.S.C. § 1201(e) (1998).

[28] 17 U.S.C. § 1201(h) (1998).

[29] 17 U.S.C. § 1201(i) (1998).

effectuate circumvention if developers are not permitted to manufacture and distribute circumvention devices.

Nonprofit Libraries, Archives, and Educational Institutions. Section 1201(d) provides an exemption for nonprofit libraries, archives, and educational institutions to gain access to a commercially exploited copyrighted work solely to make a good faith determination of whether to acquire such work.[30] A qualifying institution may gain access only when it cannot obtain a copy of an identical work by other means and access may not last longer than necessary. Such an entity is not allowed to use this exemption for commercial advantage or financial gain.

Here, too, the provision does not specifically permit the development and distribution of the devices necessary to effectuate the permitted circumvention. Even if the permission to develop the devices is implied, this exception is of little practical use. It is highly unlikely that a content provider will not make a work available to a potential customer, particularly large institutional customers such as libraries and schools. The library and educational associations did not request this exception; rather, it was "given" to them by the House Subcommittee on Courts and Intellectual Property so that the Subcommittee could claim that it responded to the concerns of libraries and schools.

Rulemaking. Congress understood that notwithstanding this list of specified exceptions, there may be still other legitimate reasons for circumventing technological protections. Accordingly, Congress suspended application of the prohibition on circumvention of access controls for two years, until the Librarian of Congress could conduct a rulemaking proceeding to determine whether additional exceptions were needed. The DMCA further requires the Librarian of Congress to conduct a similar rulemaking every three years thereafter. The Librarian's principal inquiry is whether the prohibition on circumvention will adversely affect the ability of users of copyrighted works to make noninfringing uses of the work.

Even though the prohibition on acts of circumvention are suspended for two years pending the rulemaking, the prohibition on the manufacture and distribution of devices which circumvent access controls and copy controls takes immediate effect. Moreover, under the rulemaking process the Librarian is authorized only to create additional exceptions to Section 1201(a)(1) -- the prohibition on circumvention of access controls. On the face of the statute, however, the Librarian does not appear authorized to create additional exceptions to the device prohibitions of Sections 1201(a)(2) and (b). Read literally, the statute allows the Librarian to permit the act of circumvention in additional situations, but not the devices necessary to perform the acts of circumvention. Hopefully Congress will correct this problem before Section 1201(a)(1) takes effect.

Indeed, Congress may soon be forced to amend the rule-making provision because it may well be unconstitutional. The Library of Congress is, of course, part of Congress, and thus it may not have the constitutional authority to issue regulations. (The constitutional structure of checks and balances would be frustrated if Congress could delegate rulemaking authority to its own entity.) It appears that the Justice Department

[30] 17 U.S.C. § 1201(d) (1998).

raised concerns about this issue, which the President attempted to cure in his statement upon signing the treaty. The President asserted that the Copyright Office is, for constitutional purposes, an executive branch entity. Thus, in his view, the Copyright Office can issue regulations. (Under Section 1201(a)(1)(c), however, the Copyright Office simply makes a recommendation to the Librarian of Congress, and the Librarian issues the rule.)

It remains to be seen whether the President's statement really fixes the problem. If it doesn't, the question then becomes whether this constitutional flaw can be separated from the rest of Section 1201, or if it poisons the entire provision.

This problem arose because of a jurisdictional squabble between the Commerce and Judiciary Committees in each chamber. The logical entities for a rulemaking of this sort would be the Patent and Trademark Office or the National Telecommunications and Information Administration. These agencies, however, reside in the Department of Commerce, and the Judiciary Committees in the House and Senate feared that granting the rulemaking authority to the Department of Commerce would lessen the Judiciary Committees' claim to primary jurisdiction over this issue. Placing the rulemaking under the Librarian of Congress avoids this jurisdictional problem.

IV. "No Mandate" and Other Provisions

Section 1201 contains a "no mandate" provision, which specifies that manufacturers of consumer electronics, telecommunications, and computing products are not required to design their products to respond to any particular technological protection measure.[31] This provision was essential to the consumer electronics and computer industries, which feared that Section 1201 otherwise might require VCRs and PCs to respond to inconsistent types of technological protection. The "no mandate" provision also makes clear that manufacturers will not have to retrofit VCR s and PCs already on the market to accommodate new forms of protection which may be incorporated in copyrighted material in the future.

Finally, Section 1201 contains a highly technical provision which specifically addresses the protection of analog television programming and prerecorded movies in relation to recording capabilities of ordinary consumer analog video cassette recorders. Section 1201 requires analog video cassette recorders to conform to the two forms of copy control technology that are in wide use in the market today — the automatic gain control technology and the colorstripe copy control technology.[32] This provision prohibits tampering with these analog copy control technologies to render them ineffective by redesigning of video recorders or by intervention of "black box" devices or "software hacks."

As an essential element of this provision, Congress included specific encoding rules to preserve long-standing consumer home taping practices. Copyright owners may use

[31] 17 U.S.C. § 1201(c)(3) (1998).

[32] 17 U.S.C. § 1201(k) (1998).

these technologies to prevent the making of a viewable copy of a pay-per-view program or a prerecorded tape, for example, but cannot limit the copying of traditional over-the-air broadcasts or basic and extended tiers of programming services, whether provided through cable or other wireline, satellite, or future over-the-air terrestrial systems. In addition, copyright owners may only utilize these technologies to prevent the making of a 'second generation' copy of an original transmission provided through a pay-television service

This provision becomes effective in eighteen months. Professional devices and Beta and 8mm VCRs, however, are exempt from its requirements.

V. The First Circumvention Case: *Sony Computer Entertainment v. Connectix*

The first circumvention case was filed in the federal court for the Northern District of California on January 27, 1999, just three months after President Clinton signed the DMCA into law. The complaint on its face fails to state a valid Section 1201 claim, which doubtless contributed to the court's rejection of the motion for a temporary restraining order on February 4, 1999.

Facts. The plaintiffs are the Japanese company Sony Computer Entertainment, Inc., and its U.S. subsidiary Sony Computer Entertainment America (collectively "SCEA"). The defendant is a privately held Silicon Valley company, Connectix. SCEA develops videogame CD-ROMs which run on its proprietary PlayStation. The PlayStation includes firmware embedded in ROM, which functions as the PlayStation's operating system (OS). The videogame CD-ROMs include software entitled "library code" which allows the videogame to run on the PlayStation. In addition to creating its own videogames, SCEA has licensed the library code to other videogame companies so that they can develop games compatible with the PlayStation.

Connectix developed a Virtual Game Station which allows the SCEA videogames to run on Apple computers, including the iMAC, the Macintosh, and the PowerBook. During the course of development, Connectix requested a license for the SCEA software, and requested technical assistance so that it could understand the operation of the PlayStation OS. SCEA refused the license and the assistance. Thereafter, Connectix reverse engineered both the PlayStation OS and the CD-ROM library code. Specifically, SCEA alleges that Connectix decompiled or disassembled the object code in the SCEA PlayStation and CD-ROM.

Additionally, SCEA contends that it embedded technological measures in the PlayStation and the videogames to prevent "counterfeit" games from running on the PlayStation. The Virtual Game Station does not contain the PlayStation's technological measures, and thus counterfeit games can run on it.

SCEA's Circumvention Claim. The SCEA complaint contains seven claims, including copyright infringement, trademark dilution, and circumvention of technolgical protection measures. Here we will focus on the circumvention claim, although it is worth

noting that the other claims appear to have little merit. The copyright claim, for example, centers on reverse engineering clearly permitted by the Ninth Circuit in *Sega v. Accolade*.

In its circumvention claim, SCEA contends that the Virtual Game Station's omission of the PlayStation's technological protection measures constitutes an unlawful circumvention of those measures. In the absence of those measures, counterfeit games can run on the Virtual Game Station. This claim does not make sense in several respects. First, from a purely logical (as opposed to legal) point of view, this claim is the opposite of the SCEA's copyright claim. There, SCEA in essence argues that Connectix copied too much. Here, SCEA is contending that Connectix copied too little -- that it "circumvented" the technological protection by failing to include it in the Virtual Game Station.

Second, currently there is no prohibition on the act of circumvention of access controls. The prohibition takes effect only after the Library of Congress completes its rulemaking in two years. Further, there is no prohibition on the act of circumventing copy controls. Accordingly, there is no prohibition on circumvention in effect for Connectix to violate.

To be sure, there is a prohibition on the manufacture of circumvention devices. But the Virtual Game Station itself does not circumvent anything. It simply operates regardless of whether the videogames contain SCEA's authentication signals. The "No Mandate" provision of Section 1201(c)(3) makes clear that this failure to behave in the same manner as the PlayStation does not violate the law; Section 1201(c)(3) provides that Section 1201 does not require a product to "provide for a response to any particular technological measure…." Indeed, the situation here is even more favorable to Connectix than the typical "No Mandate" situation. The Virtual Game Station is not ignoring a particular signal; rather, it is ignoring the *absence* of a particular signal.

Moreover, neither the Virtual Game Station nor any of its components is primarily designed or marketed to circumvent the technological protection measure. The vast majority of videogames on the market are legitimate, and the Virtual Game Station is primarily designed and marketed to run these legitimate games. Also, as noted above, no part of the Virtual Game Station is doing any circumvention. Thus, the Virtual Game Station does not fall within the device prohibition of Section 1201(a)(2) or (b).

Finally, Connectix asserted in its opposition to SCEA's TRO motion that its Virtual Game Station does in fact implement the PlayStation's technological measures, and cannot run the counterfeit videogames. Accordingly, the factual predicate is missing from SCEA's circumvention claim.

VI. An Assessment of Where We Ended Up

Without question, the exceptions and the "No Mandate" provision address many of the most serious problems with the technological protection measure proposed by the Administration and first introduced in Congress. Nonetheless, the provision still has significant shortcomings; it continues to prohibit some legitimate, socially useful activities such as circumvention for error correction. It remains to be seen whether the rulemaking produces additional exceptions which have the effect of permitting these socially useful

activities. In particular, will the rulemaking preserve fair use and the Copyright Act's other exceptions and limitations on authors' exclusive rights? Further, the existence of exceptions will not prevent the bringing of frivolous circumvention claims, such as SCEA's against Connectix. And legitimate, innovative companies like Connectix will still have to invest substantial resources in defending these frivolous claims.

Section 1201 may have another unintended consequence. Both Sections 1201(a)(2) and (b) prohibit the trafficking in circumvention devices. Will an Internet service provider which hosts a site which makes circumvention devices available be liable for "trafficking" in the devices, even if it had no knowledge of the presence of the devices on the site? The ISP probably would not face criminal liability if it had no knowledge; but it might well assume civil liability, because the Section 1201 does not contain a scienter requirement. Given that Title II of the DMCA provides safe harbors for ISPs from copyright liability, it would be ironic if Title I of the DMCA imposed additional liability on the ISPs. (The safe harbors of Title II apply only to copyright liability, not Section 1201 circumvention liability.)

Congress chose the approach of adopting an extremely broad prohibition, then granting an exception to any group powerful enough to lobby effectively for one. The breadth of the exception also turned on lobbying power; the security testing exception is more comprehensive than the privacy one because the banks and accounting firms pushing for the security testing exception had more political clout than the public interest groups concerned about privacy.

The critical mistake Congress made that resulted in this complex, inconsistent provision was its acceptance of the Administration's overly broad prohibition. The Administration's proposal was overly broad in three different ways. First, it regulated both devices and conduct, rather than just conduct. By regulating devices, Congress had to fashion exceptions for devices used in legitimate ways. Virtually any technology can be used for good or evil; the person operating the technology determines the role the technology plays. Section 1201's approach runs directly contrary to the Administration's stated philosophy vis-à-vis the Internet; it relies on heavy regulation rather than market driven solicitations.

Second, the Administration's proposal regulated circumvention, regardless of whether the circumvention actually facilitated infringement. By divorcing the act of circumvention from the act of infringement, Congress had to create exceptions for acts of circumvention which did not lead to infringement.

Third, the Administration's proposal addressed the circumvention of access control technologies *and* copy control technologies, rather than just the circumvention of copy control technologies. Because access control is so far removed from copyright protection, the prohibition implicated many legitimate activities. Had Congress dealt only with copy controls, the majority of the exceptions -- those for encryption research, security testing, protecting personal privacy, library purchasing, and monitoring children's use of the Internet -- would not have been needed.

Significantly, the treaties require none of the overbroad features. The treaties simply require that "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

The treaties say nothing about devices; they speak only of circumvention. The content community argues that a ban on devices is necessary to afford them "adequate legal protection" and "effective legal remedies," but this interpretation has no basis in the negotiating history of the treaties.

The treaties also say nothing about prohibiting circumvention in the absence of infringement. Indeed, the treaties could be read as prohibiting only circumvention which does in fact lead to infringement.

Finally, the treaties say nothing about controlling access to a work. Rather, the treaties speak of the exercise of their rights under the treaties or the Berne Convention, which do not include an exclusive right over access to the work.

In sum, Section 1201's problematic nature flows directly from the Administration and Congress going far beyond the requirements of the treaties. Conversely, the approach sponsored by Messrs. Ashcroft, Boucher, and Campbell went only as far as required by the treaties, and thus avoided the DMCA's inadvertent restriction on legitimate activities. When regulating new technologies such as the Internet, less is usually better.