

April 1, 2007

Yoram HaCohen
Head of the Law, Information and Technology Authority
Ministry of Justice
Hasholsha Street 3, Post Office Box 9288
Tel Aviv 61092, Israel

Re: February 19, 2007 Request for Comments on the Possible Creation of DRM Legislation

Dear Mr. HaCohen:

The undersigned organizations, representing a broad spectrum of technology companies, libraries, and consumers in the United States, appreciate this opportunity to respond to your Request for Comments, dated February 19, on the possible creation of DRM legislation. The undersigned organizations have participated in the deliberative processes leading to the World Intellectual Property Organization (WIPO) Copyright Treaty, the U.S. Digital Millennium Copyright Act, and much of the litigation that has followed. Based on these experiences, the undersigned organizations respectfully offer recommendations described below.

Generally, we submit that anticircumvention rules are controversial, and are not advisable. Their objectives may instead be adequately addressed through other means, including traditional secondary liability. If policymakers nevertheless elect to institute such a regime, the regime must be narrowly tailored, providing a general exception to the circumvention ban for all acts of circumvention that do not directly result in infringement. In addition, the rule should contain specific safeguards designed to protect competition, innovation, and end-user rights, and a means by which those safeguards may be expediently broadened as circumstances require.

1. Anticircumvention Goals Can Be Satisfied by Means Other Than Broad Bans, Such as Secondary Liability.

“Anticircumvention” is generally understood to describe a copyright-like legal framework that forbids the disabling or evasion of technology that protects copyrights. Some form of circumvention prohibition (*i.e.*, protection for “technological protection measures” or TPMs)¹ is required by Article 11 of the WIPO Copyright Treaty (WCT) and Article 18 of the WIPO Performances and Phonograms Treaty (WPPT).

The United States, like many other signatories of the WCT, crafted independent legislation to implement this obligation. The U.S. anticircumvention rule was codified by the Digital Millennium Copyright Act.² U.S. practice subsequent to the DMCA’s enactment has

¹ “Technological protection measures” is a term of art used frequently in the U.S. legal context to refer to technologies such as “digital rights management” (DRM).

² Pub. L. No. 104-304, 112 Stat. 2860 (1998) (codified in various sections of U.S. Code, Title 17).

been to require very similar provisions in free trade agreements. U.S. free trade agreements' text on this subject is very specific, particularly in comparison to multilateral instruments, which lack specificity as to how anticircumvention should be implemented.

The U.S. experience with the DMCA illustrates that overbroad legal protection for technological protection measures can have serious unintended consequences beyond areas governed by copyright law, including on the technology sector and on educational and research activities. Given that experimentation with anticircumvention has thus far proved troublesome, policymakers should consider the narrowest possible implementation. Undoubtedly, multiple narrower models for implementing an anticircumvention rule exist.³

One possibility is to ban only acts of circumvention, rather than tools that can be used to circumvent. Article 11 of the WCT only prohibits the circumvention of effective technological measures, not the technology by which circumvention is achieved. In fact, the text as proposed to the Diplomatic Conference in 1996 had originally focused exclusively on such tools, referred to "protection-defeating devices."⁴ As history reflects, the Diplomatic Conference rejected such a prohibition, opting for the blander, less restrictive language in Article 11.

Alternatively, where secondary liability exists in statute or common law, "adequate legal protection and effective legal remedies against the circumvention of effective technological measures" may be provided by traditional secondary liability instead of *sui generis* prohibitions like the DMCA.⁵ Under U.S. practice, secondary liability theories traditionally impose liability where a party had the right and ability to supervise the infringing activity and an obvious and direct financial interest in the exploitation of copyrighted materials (vicarious liability),⁶ or where a party intentionally induces direct infringement through purposeful, culpable expression and conduct (contributory infringement).⁷ These are activities which anticircumvention rules intend to deter, but would be more efficiently addressed through secondary liability. Secondary liability is also useful because in cases in which secondary liability is not implicated, the given use is not one connected with the normal exercise of authors' rights. To prohibit such uses is inappropriate, yet circumvention bans have a demonstrable history of doing precisely that.

Thus, when national law provides for secondary liability, a specific anticircumvention law is redundant or over inclusive. Any product, service, or activity that would enable circumvention of effective technological measures could easily be addressed via a carefully tailored secondary liability regime that gives due recognition and protection to legitimate articles of commerce, entrepreneurship, and the public interest, without resorting to anticircumvention

³ Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, nn. 324-29 and accompanying text, available at <<http://www.ischool.berkeley.edu/~pam/papers/l&e%20reveng3.pdf>>.

⁴ Records of the Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, Geneva 1996, Vol. 1 (WIPO 1999), at 14-15.

⁵ See, e.g., Pamela Samuelson, Big Media Beaten Back, *Wired* (vol. 5.03) at 64, March 1997, available at http://www.wired.com/wired/5.03/netizen_pr.html (arguing that existing U.S. law, including secondary liability, satisfied WIPO treaty obligations).

⁶ See, e.g., *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304 (2d Cir. 1963).

⁷ See *MGM Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764 (2005) (citing *Gershwin Pub. Corp. v. Columbia Artists Mgmt, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971)).

rules. Accordingly, we recommend a specific circumvention ban only if secondary liability practice is deemed insufficient.

2. Any Anticircumvention Law Should Be Narrowly Tailored.

When enacting the DMCA, the U.S. Congress exceeded what was necessary to conform American law to WIPO obligations.⁸ The DMCA contains three separate bans, addressing both ‘access controls’ and ‘copy controls.’ It bans (1) the act of circumventing a technological protection measure that controls access to a copyrighted work;⁹ (2) the manufacture, importation, distribution, or trafficking in tools, technologies and devices that can circumvent TPMs that control access to copyrighted works;¹⁰ and (3) the manufacture, importation, distribution, or trafficking in tools, technologies and devices are primarily designed or produced for the purpose of circumventing TPMs that protect the right of a copyright owner.¹¹

Article 11 of the WIPO Copyright Treaty, by contrast, merely requires protection for technological measures used in connection with “exercise of... rights... *and* that restrict acts... which are not authorized by the authors concerned or permitted by law.” (Emphasis supplied.)

Subsequent case law has indicated that DMCA violations must have a nexus to infringement,¹² consistent with Article 11. Nevertheless, the results of the elaborate U.S. system have been negative. The effect has been to threaten end-users and consumer rights, suppressing lawful uses that would benefit the public. Numerous organizations ranging from civil liberties advocates to conservative think tanks have criticized the DMCA’s anticompetitive and anti-consumer effects.¹³ Therefore, if an anticircumvention regime is deemed necessary, it should be narrowly tailored, and limited to uses that lead to infringement.

Various elements can help achieve a narrow rule. For example, one element that would mitigate the over-breadth of a circumvention ban is an “actual” or “subjective” knowledge requirement. Requiring proof that violations were committed with actual knowledge that the act was unlawful would avoid the risk that liability could accrue for accidental or unknowing

⁸ Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 Berkeley Tech. L. J. 519, 521, 531-32 (1999) (explaining that existing U.S. law satisfied WIPO anticircumvention obligations) (available at <http://www.ischool.berkeley.edu/~pam/papers/Samuelson_IP_dig_eco_htm.htm>); see also *WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 before the House Subcomm. on Courts and Intellectual Prop.*, 105th Cong., 1st sess. (Sept. 16, 1997) at 62 (testimony of Asst. Sec. of Commerce and Commissioner of Patents and Trademarks Bruce A. Lehman).

⁹ 17 U.S.C. § 1201(a)(1).

¹⁰ 17 U.S.C. § 1201(a)(2).

¹¹ 17 U.S.C. § 1201(b).

¹² See *Chamberlain Group v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004); *Storage Tech. v. Custom Hardware Eng’g*, 421 F.3d 1307 (Fed. Cir. 2005), available online at <<http://fedcir.gov/opinions/04-1462.pdf>> (both requiring a causal relation between the unauthorized access achieved by circumvention and some subsequent act of infringement).

¹³ See, e.g., Electronic Frontier Foundation, *Unintended Consequences: Seven Years Under the DMCA* (Apr. 2006) available online at <http://www.eff.org/IP/DMCA/DMCA_unintended_v4.pdf>; Timothy B. Lee, *Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act* (Cato Institute Mar. 2006) available online at <<http://www.cato.org/pubs/pas/pa564.pdf>>.

circumvention. Such a provision is not inconsistent with the DCMA, and it appears in the U.S.-Chile Free Trade Agreement.¹⁴ Another narrowing element would be to require a higher level of proof to adequately allege a violation if the activity in question were not primarily commercial in nature.

3. Specific Safeguards to Be Considered.

Regardless of how narrowly tailored the ban is, it is nevertheless advisable that the ban incorporate specific safeguards. The use of explicit safeguards is consistent with prevailing international norms. The DMCA contains several explicit safeguards, although the undersigned organizations do not recommend the use of the DMCA as a model, as its existing safeguards have proved to be unduly narrow and insufficient to prevent abuse. This reflects the drafting philosophy of the DMCA: a broad, sweeping rule with narrow, targeted exceptions. Experience suggests that a wiser strategy would have been to institute a narrow, targeted rule that would not rely solely on exceptions to prevent abuse.

Thus, even when crafting a narrow, targeted rule, we recommend included safeguards such as those addressed below to protect important social and commercial interests.

- 1) *Do Not Prohibit Circumvention For Uses Not Connected to the Exercise of Authors' Rights or Otherwise Authorized by Law.*

In requiring “adequate legal protection and effective legal remedies against the circumvention of effective technological measures” securing copyrighted works, Article 11 of the WIPO Copyright Treaty did *not* mandate protection for TPMs in the case of non-infringing uses of works.¹⁵ Nor does the European Information Society Directive, sometimes called the “EU Copyright Directive,” which similarly contemplates prohibiting acts in relation to an author’s copyrights.¹⁶ In addition, the Directive also requires that “Members States shall take appropriate measures to ensure that rightsholders make available to the beneficiary of an exception or limitation provided for in national law... to the extent necessary to benefit from that exception or limitation and where the beneficiary has legal access”.¹⁷

Consistent with Article 11 of the WIPO Copyright Treaty, circumvention should not be prohibited when the use in question is either not in “connection with the exercise of [authors] rights” or not otherwise “authorized by the authors concerned or permitted by law.” In short, circumvention to make unauthorized but non-infringing uses should not be prohibited. Limiting liability to acts with a nexus to infringement would prevent anticircumvention rules from inhibiting uses encouraged by copyright law, such as fair use and the use of public domain works. Indeed, many DMCA abuses stem from efforts to use technological protection measures

¹⁴ United States-Chile Free Trade Agreement Art. 17.7(5), June 6, 2003, 42 I.L.M. 1026.

¹⁵ WIPO Copyright Treaty Art. 11 (requiring protection against uses “not authorized by the authors concerned *or* permitted by law.” (Emphasis supplied)).

¹⁶ Council Directive, 2001/29/EC, Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (May 22, 2001), art. 6(3).

¹⁷ *Id.* at art. 6(4).

to control uses not connected with an author's rights.¹⁸ Categorically excluding such control, consistent with Article 11, would help prevent anticircumvention abuse.

2) *Interoperability to promote competition and consumer interests.*

Because technological protection measures generally control how one product interfaces with another, they may be used anticompetitively to prevent competitors' products from interoperating with one's own. Recognizing that Section 1201 could prevent a developer of interoperable products from engaging in pro-competitive reverse engineering to ensure interoperability, Congress created an exception to the anticircumvention rule in Section 1201(f), which is explicitly directed toward the development of interoperable products.¹⁹ Section 1201(f) was modeled on the language of the European Software Directive, which pioneered the concept of protecting interoperability and reverse engineering in order to promote competition.²⁰ While Section 1201(f) has prevented some misconduct, its text is unduly narrow, leading scholars to observe that the DMCA nevertheless remains "ripe for anticompetitive abuse,"²¹ particularly in cases that have nothing to do with copyright piracy. Notwithstanding the exception provided in Section 1201(f), in a recent case software developers succeeded in using the law to prevent reverse engineering by competing products and services.²²

The DMCA has been used to lock consumers into purchasing proprietary products at higher prices. For instance, printer distributor Lexmark used the DMCA in a bid to block the creation of an aftermarket in recycled printer cartridges that were being sold to consumers at a lower price than Lexmark's own authorized refilled cartridges.²³ A garage door manufacturer, Chamberlain Group, attempted to use the DMCA to ban the sale of its competitor's universal garage remote control opener.²⁴ Although appellate courts ultimately rejected these uses of the DMCA, many defendants lack the substantial resources required to litigate cases to the appellate level in order to protect their rights. Given the burden of litigation, anticircumvention exceptions should be broad and unambiguous.

In addition, the DMCA has been employed to enforce geographic market segmentation. U.S. rightsholders have used technological protection measures involving region coding to

¹⁸ See note 9, *supra*.

¹⁹ The U.S. Senate Judiciary Committee explained the policy underlying Section 1201(f), stating that the 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." See S. Rep. No. 105-190, at 32 (1998).

²⁰ For example, the Software Directive and the DMCA share the same definition of interoperability ("interoperability can be defined as the ability to exchange information and mutually to use the information which has been exchanged"). Compare 17 U.S.C. § 1201(f)(4) with Council Directive, 91/250/EEC, Legal Protection of Computer Programs (May 14, 1991), recital 12.

²¹ Dan Burk, *Anticircumvention Misuse*, 50 UCLA L. Rev. 1095, 1096 (2003).

²² *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005).

²³ *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 253 F. Supp. 2d 943 (E.D. Ky. 2003), *vacated and remanded*, 387 F.3d 522 (6th Cir. 2004).

²⁴ *Chamberlain Group Inc. v. Skylink Techs., Inc.*, 292 F. Supp. 2d 1040 (N.D. Ill. 2003), *aff'd*, 381 F.3d 1178 (Fed. Cir. 2004), *cert. denied*, 125 S. Ct. 1669 (2005), *available online at* <<http://www.fedcir.gov/opinions/04-1118.doc>>. See also *Storage Tech. v. Custom Hardware Eng'g*, 421 F.3d 1307 (Fed. Cir. 2005), *available online at* <<http://fedcir.gov/opinions/04-1462.pdf>>.

geographically segment markets for DVDs, video games such as the Sony PlayStation, and even printer ink cartridges. This region-coding is protected by the DMCA, thereby allowing rightsholders to enforce differential pricing across markets and prevent aftermarket use of products in geographic in which they have declined to enter.²⁵ These abilities, of course, are not associated with the exploitation of an author's rights.

The solution to these problems is to provide a broad exception for circumvention in the course of reverse engineering. When viewed generally, however, this problem is not simply a question of interfaces, but competitive practices generally. For this reason, the inclusion of a limitation against monopolistic uses in the circumvention ban, prohibiting the use of technological measures for anti-competitive purposes, should be a principle part of any such rule.

3) *Do Not Hamstring Technological Innovation With a Mandate to Respond.*

Any circumvention ban should also include a "no mandate" provision, specifying that the ban does not mandate that a product, component, or service must respond to technological protection measures. In short, TPMs must be self-sufficient. Failure to include such a provision would impose upon technology products the obligation to identify and support countless potentially conflicting technological measures of various degrees of complexity and robustness.

In the debates leading up to enactment of the DMCA, the U.S. technology industry expressed concern that the ban on circumvention devices could be used by overzealous copyright owners to ban both existing technologies that were not designed to respond to TPMs subsequently added to works by copyright owners, or to require technology companies to design technologies to interact with copyright owners' particular TPMs, stifling technological innovation.

To address these concerns, the "no mandate" section in 1201(c)(3) was inserted in to the DMCA. That section provides that nothing in section 1201 shall require that the design of, or design and selection of parts and components for a consumer electronics, telecommunications or computing product, must respond to any particular TPM, so long as the part or component or product is not otherwise banned under the "tools" ban. Section 1201(c)(3) was designed to provide technology companies with a defense to the tools prohibition, in order to foster technological innovation.

4) *Computer Security and Scientific Research, and Publication Thereof*

²⁵ See, e.g., *Sony Computer Entertainment America Inc. v. Gamemasters*, 87 F.Supp.2d 976 (N.D. Cal. 1999); *Stevens v Kabushiki Kaisha Sony Computer Entertainment*, [2005] High Court of Australia (Oct. 6, 2005); David Pringle & Steve Stecklow, "Electronics With Borders: Some Work Only in the U.S.," *WALL ST. J.*, Jan. 17, 2005, at B1; Reuters, "HP Sued Over Printer Cartridge Expiration," *MSNBC*, Feb. 22, 2005, *available at* <<http://www.msnbc.msn.com/id/7012754/>>; Testimony of representatives of MPAA (S. Metalitz) and AOL/ Time Warner (D. Marks) Library of Congress, Copyright Office, Public Hearings on Exemption to Prohibition on Circumvention of Copyright Protection for Access Control Technologies, Docket No. RM 2002-4, May 15, 2003, Panel 3 (p. 263 ff), that multi-region DVD players violate section 1201, linked *available at* <www.copyright.gov/1201/2003/hearings/schedule.html>.

U.S. copyright owners have used the DMCA to block publication of research that discusses security vulnerabilities in protection technologies. There are concerns within the United States that this has weakened computer security, which depends on research and testing.

In 2001, a music industry group threatened DMCA liability against a Princeton professor and his research team when they tried to publish a research paper describing weaknesses in the music industry's proposed digital watermark technology. The industry group considered that the information in the paper was a "circumvention tool" and publishing it was banned under the DMCA. The research team withdrew their paper after the music industry also sent threat letters to their employers and the conference organizers. While a vetted version of its paper was published after several months of litigation, significant harm was done. One of the team lost his position and a second decided to discontinue computer security research as a result of the litigation.

This case has had an ongoing chilling effect on scientific research and publication. Researchers in the United States and overseas have refused to publish the results of security vulnerability research or have removed previously published research from the Internet for fear of DMCA liability. Within the United States there is growing concern about the impact of the DMCA on computer security research. In 2002, former White House Cyber Security adviser Richard Clarke admitted that the DMCA had had a chilling effect on security research and called for DMCA reform.

The importance of ensuring a safe environment for scientific research into encryption and computer security has been highlighted by the recent Sony 'rootkit' CD copy-protection episode, in which Sony surreptitiously caused the installation of a security-compromising application on the computers of millions of consumers and institutional users - including governments and militaries - which purchased certain copy-protected discs. The 'cloaking device' that Sony used to disguise this technological protection measure from consumers was subsequently exploited by hackers to launch computer attacks. If security researchers, professionals, or security applications developers attempted to remedy the security threat posed by the rootkit, they risked violating the anticircumvention rules - a potentially criminal act. While several groups successfully petitioned the U.S. Copyright Office to establish an administrative exemption in the law to protect against this threat, that exemption was not established for months after the threat manifested itself, and even today the order granting the exemption is being challenged in federal court.

4. A Regulatory or Administrative Proceeding Should Be Established to Address Subsequent Problems.

The circumstances of the 'rootkit' debacle noted above highlight another drawback of a broad prohibition with fixed exceptions: it is not possible to foresee all possible impacts on future circumstances. Exceptions that appear sufficient today prove to be too narrow in the future. Thus, any circumvention ban should incorporate a review of the impact of the circumvention ban, and an expedient regulatory or administrative process for subsequently granting specific exemptions to the full scope of any ban that is enacted.

This process should set a burden of proof for exemption proponents that is reasonable and commensurate with their ability to provide the evidence sought, perhaps employing government ministries to propose exemptions on behalf of affected communities. Once the threshold burden is met, exceptions should not “sunset” as they do under the DMCA. Such sunset provisions needlessly require exception proponents to repeatedly reestablish that which they have already shown – that the circumvention ban is too broad. Rather than wasting resources to prove the same fact time and time again, the burden of should shift to any exemption opponents to establish that circumstances have changed such that the current regulatory exemption is causing infringement.

In conclusion, an explicit circumvention ban may be redundant to an adequate secondary liability regime, but if a such a regime is deemed necessary, it should be narrowly focused and designed with explicit safeguards to prevent abuses of type that have been previously demonstrated.

Please feel free to contact us if we may be of any assistance.

Respectfully,

American Association of Law Libraries
American Library Association
Association of Research Libraries
Computer & Communications Industry Association
Electronic Frontier Foundation
Home Recording Rights Coalition
Media Access Project
Special Libraries Association