Before the
Federal Trade Commission
Washington, D.C.

In re Digital Rights Management (DRM) Town Hall	Project No. P094502 (Comment)

COMMENTS OF
COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

In response to the Federal Trade Commission's (FTC or "the Commission") announcement of a town hall meeting regarding digital rights management technology, the Computer and Communications Industry Association (CCIA) submits the following comments. CCIA is a trade association dedicated to open markets, open systems, and open networks. CCIA members participate in the Internet, information, and communications technology industries, ranging from small entrepreneurial firms to the largest in the business – companies which collectively generate more than $200 billion in annual revenues.

These comments focus on three issues: the notification and disclosure issues related to DRM, the risks to competition posed by DRM-related impediments to interoperability, and the fact that the use of DRM exacerbates the costs of current misconceptions about the balance between rights-holders' rights and consumer rights. To address the first issue, it is proposed that the Commission offer guidance to market actors about when disclosure is appropriate. To address the second issue, these comments urge the Commission to take a more active role before the courts, and, where appropriate, in the exercise of its jurisdiction as a competition authority. In response to the third issue, CCIA urges the Commission to reconsider the objections raised in

CCIA's 2007 complaint regarding certain rights-holders' misrepresentations about the scope of consumer rights.

I. Introduction and Overview

Digital rights management or "DRM" is a general term describing technology deployed in relation to copyrighted content in digital form, ostensibly to reduce the unauthorized exercise of a copyright-holder's exclusive statutory rights with respect to the protected work. Digital rights management was at one time viewed as the future of digital content. Arguably, it has yet to meet these expectations. A 1995 government report produced by an interagency working group stated that "[i]f content providers cannot be assured that they will be able to realize a commercial gain from the sale and use of their products using the NII ["national information infrastructure" – essentially, the Internet], they will have little incentive to use it." This reasoning supported a conclusion that "content providers must have secure and reliable means for delivering information products and services to consumers."[1] In reality, however, extraordinary amounts of legitimate, non-infringing information products and services are available via the Internet today and are neither secured nor encrypted in any fashion. This reflects the embrace of business models unlike the traditional copyrighted content distribution model for the monetization of information products.

Nevertheless, although DRM is unlikely to be the sole future of digital content, certain markets have prospered while deploying various digital rights management technologies. These markets are not economically insignificant. Notably examples include DVDs and certain proprietary computer software. Apple's iTunes model was another prominent example of a

[1] U.S. Dep't of Commerce Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: *The Report of the Working Group on Intellectual Property Rights* at 177 (1995).

widely deployed DRM technology, although, as has been widely reported, the company is now abandoning DRM on certain products.[2] Market circumstances will continue to influence consumers' willingness to accept DRM as well as rights-holders' willingness to market unencumbered content, and it is thus likely that as business models change, so too will the use of DRM. For the foreseeable future DRM will remain a feature of the digital content landscape.

In many cases, DRM technology may be an entirely appropriate tool to secure copyrighted works from copyright infringement. Generally, the market should decide when and where DRM is deployed. The public sector role should be to prevent DRM from being deployed in a manner that is unfair or deceptive to the public, or in a manner that is anticompetitive, which would impose higher prices and restrict choices of the consuming public. At these latter results conflict directly with CCIA's mission of promoting competition and openness in technology markets, it is the primary focus of these comments.

II. Legal Landscape of DRM

At the outset, it is necessary to distinguish DRM from a related term used in relation to the Digital Millennium Copyright Act of 1998 (DMCA):[3] technological protection measures (TPMs).[4] The DMCA contains in Section 1201 certain "anticircumvention" rules – legal protection for the technology itself, rather than the underlying work. *See* 17 U.S.C. § 1201.[5]

---

[2] Brad Stone, *Copy an iTunes Song? Go Ahead, Apple Says*, N.Y. Times, Jan. 7. 2009, at B1.

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

[4] More helpful and less obfuscating is the term "copyright protection system", which originally appeared in the NII White Paper, *supra* note 1, in which the origins of the DMCA may be found. This term was not used in the DMCA, however.

[5] Congress enacted the DMCA to implement obligations relating to Article 11 of the World Intellectual Property Organization (WIPO) Copyright Treaty (or "WCT"). In requiring "adequate legal protection and effective legal remedies against the circumvention of effective technological measures" securing copyrighted works, WCT art. 11 did not mandate protection for TPMs in the case of non-infringing uses of works, nor did it impose any obligation with respect to access controls, discussed *infra*. Unfortunately, Congress went far beyond the revisions necessary to conform American law to treaty obligations in enacting the DCMA, and conferred broad new "paracopyrights" on

The DMCA does not define what "technological measures" are, but rather defines their functions – TPMs may (1) control access and/or (2) protect the rights of a copyright owner. A technological measure "effectively control access to a work" or "effectively protects a right of a copyright owner" if it, "in the ordinary course of its operation: (1) "requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work," or (2) "prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title [Title 17, U.S. Code]", respectively.[6]

In discussing DRM, it is important to avoid using this term as a substitute for the subject matter of the DMCA. Due to the specificity of the DMCA's definitions, the circumvention of some DRM technologies may not satisfy the statutory definitions for triggering DMCA circumvention liability. The DRM at issue may not effectively control access, for example, and thus would not qualify for DMCA protection,[7] or circumventing the DRM at issue may not have any nexus to infringement, which has been construed as a prerequisite for a DMCA action by the Federal Circuit.[8] Thus, limiting a discussion of DRM to include only schemes protected by the DMCA would be under-inclusive. (Equating DRM with DMCA subject matter might also be over-inclusive, since it is possible that there are some copyright protection schemes potentially governed by the DMCA that might not necessarily be conceived of as DRM.)

---

rights-holders, to the detriment of consumers and competition. Further historical roots of the notion of paracopyright may be found in Article 6 of the European Copyright Directive. *See* Council Directive, 2001/29/EC, Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (May 22, 2001).

[6] 17 U.S.C. § 1201(a)(3)(B) & 1201(b)(2)(B). The statutory terminology is notably unhelpful in that it obscures whether the technology, when functioning as an access control, is controlling interests ultimately protected by copyright, instead of, for example, protecting a product or service provider's exclusive control over an aftermarket.

[7] *See, e.g.*, *Lexmark Int'l v. Static Control Components, Inc.*, 387 F.3d 522, 547 (6th Cir. 2004).

[8] *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1204 (Fed. Cir. 2004).

III. Effects of DRM on Consumers and Competition

When protected by a poorly crafted legal rule such as Section 1201 of the DMCA, DRM can threaten consumer rights, suppressing lawful uses that would benefit the public.[9] Currently, the nexus between DRM and legal protections thereof creates three separate problems: (1) there are demonstrated notification and disclosure issues with DRM; (2) when utilized in an anticompetitive fashion, DRM can restrict interoperability and access to aftermarkets; and (3) DRM exacerbates current misconceptions about the balance between rights-holders' rights and consumer rights. Although CCIA's comments focus on these issues, this is not to suggest that other DRM-related issues may not also warrant review.

A. DRM Frequently Poses Notification and Disclosure Issues.

One of the inherent tensions in DRM is that designers generally construct their applications to minimize consumers' ability to access the copy protection software in order to prevent that software from being defeated. This, particularly when combined with inadequate disclosure, can create problems.

The 2005 debacle involving Sony's cloaked DRM "rootkit" exemplifies this issue. As documented in this agency's complaint and action against Sony following the incident,[10] Sony surreptitiously caused the installation of a security-compromising application on the computers of millions of consumers and institutional users – including governments and militaries – who purchased or used certain copy-protected music compact discs. The cloaking device that Sony

[9] Numerous parties, ranging from civil liberties advocates to conservative think tanks, have criticized the anticompetitive and anti-consumer effect of the DMCA. *See* 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>.

[10] *In the Matter of Sony BMG Music Entertainment*, FTC File No. 062-3019 (order approved June 29, 2007).

used to disguise its DRM from consumers was subsequently exploited by hackers to launch malicious computer attacks. Yet if security researchers, professionals, and security applications developers attempted to remedy the security threat posed by the offending software, they risked violating the DMCA's anticircumvention rules – a potentially criminal act. While CCIA and others successfully petitioned the U.S. Copyright Office to establish an administrative exemption in the law to protect against this threat, the exemption did not issue until several months after the threat first manifested. The proper remedy is to ensure that anticircumvention rules do not impede security in the first place.

This crisis led to class action litigation, product recalls, and charges by the Commission. This security risk would have been unlikely had Sony not disguised its activities. The primary security threat was the fact that its software was hidden from the user. By secretly installing software on a consumer's PC that hid processes, Sony exposed the user to hidden malware threats from others who could take advantage of the same cloaking device. Of course, few consumers would willingly subject their PCs to such a risk.

Similarly, as demonstrated by the widely reported "Spore" incident, content providers may fail to adequately disclose how DRM limits the usage of a product. As other commenters will likely discuss in greater detail, Electronic Arts' highly anticipated computer game "Spore" provoked substantial consumer criticism because EA gave little notice that the game's DRM, SecuROM, limited the number of times the program could be installed, causing problems when consumers used multiple personal computers, or when software and hardware changes to a consumer's PC necessitated reinstallation.[11] As in Sony's case, class actions followed.

[11] Victor Godinez, *Anti-piracy software creates more problems than it solves*, Dallas Morning News, Oct. 21, 2008. EA subsequently began offering several game titles, including Spore, through Valve's online content distribution platform, Steam. Steam and similar platforms are an alternative to traditional DRM, where product validity can be determined by an online authorization instead of by a local content protection application. *See Ben*

To some extent, the marketplace disciplines use of anti-consumer DRM. Following EA's Spore problems, for example, some reports noted consumers' intentions to avoid other products utilizing SecuROM DRM, or to boycott EA products entirely.[12] Of course, this does not aid previously injured consumers, nor does it guide DRM developers as to what conduct is consistent with legal obligations.

One response to this issue, endorsed by CCIA and numerous other organizations, appeared in H.R. 1201, the Digital Media Consumers' Rights Act of 2005 (109th Cong.). Section 4 of the DMCRA would have amended the Federal Trade Commission Act (15 U.S.C. § 41 *et seq*.) to prohibit the introduction into commerce of inadequately labeled copy-protected compact discs. Although the proposal was limited only to music discs, it recognized the problems inherent in products being sold to consumers with inadequate notification about the restrictions upon them. Guidance from the Commission on labeling practices could help remedy the consumer confusion that this legislation attempted to address.

B. DRM Protected by Anticircumvention Law Can Undermine Competition, Leading to Less Innovation and Higher Prices.

Because DRM often requires controlling how one product interfaces with another, DRM may be used anticompetitively to prevent competitors' products from interoperating with one's own. Normally, competitors will reverse-engineer the product so as to understand its interface and achieve interoperability. In some cases, this can require circumventing DRM. If DRM is protected by law, however, businesses can legally lock out their competitors, to the ultimate detriment of the consumer.

Kuchera, *Valve says DRM is stupid*, Dec. 3, 2008, *available at* <http://arstechnica.com/gaming/news/2008/12/valve-calls-drm-stupid-microsoft-still-doesnt-get-it.ars>.

[12] *See e.g.*, Kuchera, *supra* note 11.

When the DMCA was pending before Congress, developers of interoperable computer products, including CCIA, explained that the act of reverse engineering – the uncovering of the interface specifications – could require the circumvention of a technological protection measure, an act which is presently prohibited by Section 1201 of that law. Recognizing that Section 1201 could prevent a developer of interoperable products from exercising fair use privileges,[13] Congress created an exception to Section 1201 explicitly directed toward the development of interoperable products: Section 1201(f).[14]

Notwithstanding this exception, there have been several cases in which companies used the DMCA's anticircumvention rule against competitors to lock them out, turning the law into an anticompetitive tool. Section 1201(f), although designed to prevent this, has proven too narrow. While Section 1201(f) has prevented some misconduct, the DMCA nevertheless remains "ripe for anticompetitive abuse,"[15] particularly in cases that have little to do with copyright infringement. For example, a printer manufacturer attempted to use DRM to suppress competition in the aftermarket for printer toner. In *Lexmark Int'l, Inc. v. Static Control*

[13] Since the U.S. Court of Appeals for the Ninth Circuit's 1992 Sega v. Accolade decision, no fewer than five U.S. courts have permitted incidental reproduction of code in the course of reverse engineering by invoking the fair use doctrine. *Atari Games Corp. v. Nintendo of America, Inc.*, 975 F.2d 832 (Fed. Cir. 1992); *Bateman v. Mnemonics, Inc.*, 79 F.3d 1532 (11th Cir. 1996); *DSC Communications Corp. v. DGI Techs.*, 898 F. Supp. 1183 (N.D. Tex. 1995), aff'd, 81 F.3d 597 (5th Cir. 1996); *DSC Communications Corp. v. Pulse Communications, Inc.*, 976 F. Supp. 359 (E.D. Va. 1997), *aff'd in part, rev'd in part, and vacated in part*, 170 F.3d 1354 (Fed. Cir. 1999); *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir.), *cert. denied*, 531 U.S. 871 (2000). Absent fair use, however, such copying would likely constitute infringement, and the wealth of benefits resulting from interoperability would be lost.

[14] The 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). The language of 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. 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* Software Directive, *supra* note 5 *with* 17 U.S.C. § 1201(f)(4).

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

Components, Inc.,[16] Lexmark invoked the DMCA's anticircumvention rule in order to prevent other manufacturers from selling competing toner in the aftermarket. While an appellate court ultimately denied this effort, it is not the only example.

In a similar case, *Chamberlain Group v. Skylink Technologies*,[17] Chamberlain, a garage door opener manufacturer, sued Skylink over Skylink's competing garage door opener remote. By designing a remote that worked with Chamberlain's garage door opener, Chamberlain claimed, Skylink allegedly violated Chamberlain's copyright by circumventing software code within Chamberlain's garage door opener. A federal district court in Chicago found for Skylink, as did the U.S. Court of Appeals for the Federal Circuit. Since interoperability lay at the heart of Skylink's actions, there could be no infringement. Yet Skylink, like SCC, endured years of litigation for attempting to compete in the aftermarket.[18]

In *Davidson & Associates v. Jung*,[19] the computer game developer Blizzard successfully employed the anticircumvention provisions of the DMCA to sue a group of developers who produced an open-source program that emulated Blizzard's official servers for online, multi-player gaming. This permitted users to engage in online multi-player games even if they were unable or unwilling to connect to Blizzard's servers. To prevent users playing games on servers that it did not control, Blizzard invoked the DMCA.

In each of these cases, a product provider attempted to control an aftermarket using DRM, and litigated against those who sought to compete. While competitors often succeed in reverse engineering and defeating a given DRM, the costs of litigating to access a market, even if

---

[16] 253 F. Supp. 2d 943 (E.D. Ky. 2003), *reversed*, 387 F.3d 522 (6th Cir. 2004).

[17] *The Chamberlain Group Inc. v. Skylink Techs., Inc.*, 292 F. Supp. 2d 1040 (N.D. Ill. 2003), *reversed*, 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>.

[18] *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>.

[19] *Davidson & Associates v. Jung*, 422 F.3d 630 (8th Cir. 2005).

ultimately successful, may deter market entry, allowing the primary product provider to charge consumers elevated prices when selling its own related products in the aftermarket. The current state of the law on this matter creates unpredictability, as the courts of appeal do not agree upon even the simplest matter – must DMCA actions have some connection to copyright infringement or not? The result of the muddled jurisprudence creates uncertainty in an area of law which bears directly on consumers and end-users.

Particularly with respect to such products as printer toner and garage door openers, consumers are unlikely to anticipate that copyright law may constrain their ability to purchase third party parts and services in the aftermarket. This fact heightens the need for notification and disclosure, as well as the need for the Commission to exercise vigilance in its role as a competition authority. It may also be constructive for the FTC to opine as *amicus* in appropriate cases on the consumer implications of expanded statutory protection for copyright protection schemes.

C. DRM May Be Particularly Problematic Insofar as Certain Rights-holders Misconstrue the Scope of their Rights and Consumers' Rights.

As CCIA argued in a complaint to the Commission in 2007, certain corporate rights-holders systematically misrepresent consumers' rights to use legally acquired content. CCIA argued that misrepresenting consumer rights under copyright law, and in some cases threatening criminal and civil penalties against consumers who choose to exercise statutorily or Constitutionally guaranteed rights, constituted unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

Commission staff declined to recommend formal action at the time, stating that "the general issue of representations to consumers about the scope of their rights to use copies of works they purchase is of growing importance in light of the widespread and expanding

distribution of copyrighted materials in digital form. We believe that changes in content delivery mechanisms, business models, and the nature of consumers' interactions with copyrighted works will likely result in this issue taking on added significance…." Citing Judge Richard Posner, the Commission's response also stated that "if consumers routinely confront exaggerated and inaccurate copyright warnings they may tend to disregard them altogether, to the detriment of consumers and copyright owners alike."[20] This issue takes on additional importance where digital content is protected by DRM. Insofar as certain rights-holders have misrepresented systematically the scope of their rights, any DRM protecting that content may manifest the same imbalance and disregard for consumers. The result of this may be to encourage similar conduct such as that which reportedly occurred in relation to Spore: consumers download infringing copies of products that they have already purchased in order to obtain the functionality that they believe they have paid for. This breeds contempt for copyright, sustains demand for infringing content, and strains the credibility of intellectual property law. It is thus critically important that any exploration of the use of DRM in the marketplace also explore its relation to consumers' rights and expectations regarding the use of content, including fair use of copyrighted works.

In light of these continuing effects, the FTC should reconsider the subject matter raised in CCIA's 2007 complaint regarding misrepresentations about the scope of consumer rights. Consumers' expectations about using copyrighted works is inextricably linked to what DRM restrictions are appropriate and inappropriate. Consumers who are misled about the scope of their rights will have expectations regarding the use of works that they have purchased that are inconsistent with the law. Frivolous assertions of copyright and demands for the take-down of non-infringing content, for example, are less likely be resisted, particularly when rights-holders

[20] *Letter from Mary K. Engle, Assoc. Director for Advertising Practices, Federal Trade Commission, to Edward Black*, Dec. 6, 2007, at 5, *available at* <http://www.ftc.gov/os/closings/staff/071206ccia.pdf>.

represent not only that the consumer has infringed the work, but has committed a circumvention violation as well. As private consumers generally lack the resources to respond to these misrepresentations, these practices should be considered by the Commission as unfair and deceptive practices affecting commerce and remedied appropriately.

IV. Conclusion

Just as intellectual property law must strike a balance between underprotection and overprotection, the use of DRM must balance the interest in protecting copyrights against consumer rights and the preservation of open and competitive marketplaces. If digital rights management technology is used in a manner that distorts this balance, it will frustrate intellectual property law's underlying constitutional goals.

Respectfully submitted,

/s/ Matthew Schruers
Matthew Schruers, Senior Counsel
Computer & Communications Industry Association
900 Seventeenth Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070