# Rethinking Anticircumvention's Interoperability Policy

*Aaron K. Perzanowski*[*]

*Interoperability is widely touted for its ability to spur incremental innovation, increase competition and consumer choice, and decrease barriers to accessibility. In light of these attributes, intellectual property law generally permits follow-on innovators to create products that interoperate with existing systems, even without permission. The anticircumvention provisions of the Digital Millennium Copyright Act ("DMCA") represent a troubling departure from this policy, resulting in patent-like rights to exclude technologies that interoperate with protected platforms. Although the DMCA contains internal safeguards to preserve interoperability, judicial misinterpretation and narrow statutory text render those safeguards largely ineffective.*

*One approach to counteracting the DMCA's restrictions on interoperability is to rely on antitrust scrutiny and the resulting mandatory disclosure of technical information. However, both doctrinal and policy considerations suggest that antitrust offers a less than ideal means of lessening the DMCA's impact on interoperability. Rather than relying on antitrust, this Article proposes a solution that addresses the restriction of interoperability at its source. This approach broadens the DMCA's existing interoperability exemption to create an environment more hospitable to interoperable technologies. To preserve the protections the DMCA offers copyright holders, this expanded exemption would disaggregate control over interoperable software and devices from the control over access and copying that Congress intended the DMCA to enable.*

[*] Microsoft Research Fellow, Berkeley Center for Law & Technology, UC Berkeley School of Law. Thanks to Pam Samuelson for her insight and guidance, and to Jonathan Band, Peter Menell, Jason Schultz, Ted Sichelman, Fred von Lohmann, and the participants of the 2008 IP Scholars Conference at Stanford Law School for helpful comments on earlier drafts.

TABLE OF CONTENTS

## INTRODUCTION

In our networked environment, interoperability — the ability of two systems to exchange and use information — is of mounting importance. The ability of information, products, and services from a variety of providers to work together is often key to commercial success, in part because consumers increasingly expect it.[1] More fundamentally, interoperability has implications for competition, innovation, and the public accessibility of creative works. To varying degrees, companies like Facebook, Flickr, and Google have embraced the potential of interoperability by opening their platforms to independent developers.[2] Other firms, perhaps most famously Apple, remain committed to the virtues of tightly controlled user experiences and thus limit interoperability.[3]

The degree and character of interoperability in a given market depend in part on law. The legal regulation of interoperability varies not only in the extent to which it favors interoperable technologies, but also in the degree to which it intervenes in private market-driven decisions. At the extremes, legal rules either forbid or require interoperability. Conversely, the law might reflect a noninterventionist sentiment, leaving the decision to interoperate in the hands of developers and consumers. Between these poles, legal rules can encourage or discourage interoperability to varying degrees and through a variety of means. The choice between these legal rules helps determine the circumstances under which developers achieve interoperability. Law might favor bilateral agreements between firms to interoperate, while frowning on unilateral efforts to interoperate with an unwilling partner, or vice versa.

This Article analyzes the impact of the Digital Millennium Copyright Act ("DMCA") on unauthorized unilateral attempts to

---

[1] *See* Pamela Samuelson & Jason Schultz, *Should Copyright Owners Have to Give Notice of Their Use of Technical Protection Measures?*, 6 J. TELECOMM. & HIGH TECH. L. 41, 43-46 (2007) (discussing importance of flexible personal use to consumers).

[2] *See* Damon Darlin, *A Journey to a Thousand Maps Begins with an Open Code*, N.Y. TIMES, Oct. 20, 2005, at C9 (discussing availability of application programming interfaces for Google Maps and Flickr); Posting of Brad Stone to Bits, http://bits.blogs.nytimes.com/2008/06/02/to-counter-google-facebook-sets-code-free/ (June 2, 2008, 4:33 EST) (discussing Facebook Platform and Google's Open Social).

[3] Apple has recently warmed to some measure of interoperability by opening its iPhone to third-party developers in response to consumer and developer demand. *See* Melissa J. Perenson, *Apple's iPhone SDK Strategy Both Promotes and Stifles Innovation*, PC WORLD, Mar. 6, 2008, http://www.pcworld.com/article/143210.

achieve interoperability. It argues that the anticircumvention provisions of the DMCA unnecessarily inhibit interoperability, and it calls for a legislative solution to reconcile the legitimate interests of copyright holders with the need for increased freedom to interoperate.

Part I of this Article defines interoperability and examines its implications for innovation and competition as well as its traditional treatment under intellectual property ("IP") law. Admittedly, interoperability does not always yield positive outcomes. Nonetheless, because interoperability tends to increase innovation, competition, and accessibility, promoting, or at least permitting, interoperability reflects sound policy. Moreover, such an approach is consistent with the general treatment of interoperability in IP law. The interoperability policy that emerges from trade secrecy, copyright, and patent law typically permits, and occasionally promotes, interoperability.

Part II discusses the DMCA's departure from this interoperability policy. The DMCA prohibits the acts of reverse engineering[4] that are often necessary to develop interoperable products, and bans the distribution of technologies that interact with works protected by technological measures, marking a substantial break from the earlier treatment of interoperability. Congress recognized the DMCA's potential impact on interoperability and enacted a statutory exemption — § 1201(f) — to limit its negative effects.[5] Courts, however, have consistently misinterpreted this exemption's basic statutory requirements. Moreover, the exemption's narrow focus on computer programs fails to account for technologies that rely on access to other types of copyrighted works to achieve interoperability.

Because the DMCA's internal safeguards fail to protect interoperability adequately, competitors, consumers, and regulators have increasingly turned to other legal doctrines to vindicate unauthorized interoperability. Part III describes the efforts of litigants and regulators in the United States and Europe to rely on antitrust and competition principles to limit the impact of anticircumvention. This Part expresses skepticism about the role of antitrust in restraining the protections offered by the DMCA. Standard antitrust theories appear unlikely to trigger liability consistently, even when tested against the most controversial efforts to limit interoperability through technological controls. The tight integration of Apple's iPod portable

[4] Reverse engineering is the process of "starting with the known product and working backward to find the method by which it was developed." UNIF. TRADE SECRETS ACT § 1 cmt. 2 (amended 1985).

[5] 17 U.S.C. § 1201(f) (2006).

player and iTunes store serves as one recent example of such an effort. More fundamentally, an antitrust analysis typically demonstrates considerable deference to the exercise of legitimately acquired IP rights. Sensitive only to behavior that meets its threshold for anticompetitiveness, antitrust cannot independently account for the unique considerations of incentives for creativity, access, and dissemination that define IP policy. Thus, the first response to any unwanted effects of the DMCA should focus on internal limitations on the scope of the power it affords rather than external constraints imposed by a separate body of law.

Part IV outlines an alternative approach to the DMCA's current treatment of interoperability. A broadened § 1201(f) would narrow the DMCA's scope, thereby limiting its ability to accommodate technologies that interoperate with all classes of copyrighted works, not just computer programs. The chief difficulty in expanding the DMCA's tolerance of interoperability is ensuring that a more inclusive § 1201(f) does not interfere with the ability of copyright holders to impose meaningful limits on access to and copying of their works. This Part suggests disaggregating such restrictions from control over playback technologies, striking an appropriate balance between empowering copyright holders and promoting interoperability.

## I. INTEROPERABILITY

This Part addresses three preliminary questions about interoperability. First, what is it? Second, why is it valuable? And third, to what extent does traditional IP doctrine regulate it?

In short, interoperability is a relationship between two or more systems by which they exchange usable information. Interoperability is valuable because it tends to promote innovation, competition, and access, each of which gives rise to more concrete benefits for consumers and society generally. Partly in recognition of these benefits, IP doctrine has largely avoided any direct regulation of unauthorized efforts to interoperate, instead leaving market forces to determine whether developers pursue such efforts. Some IP rules, most notably copyright's favorable treatment of reverse engineering, represent explicit efforts to promote interoperability. To the extent IP doctrine directly interferes with efforts to interoperate, it does so only under limited circumstances.

### *A. Defining Interoperability*

Interoperability is the ability of a system to work in conjunction or otherwise interact with another system.[6] With respect to information and communication technologies, interoperability takes on a more specific meaning — the ability of two systems to exchange information and to make use of the information exchanged.[7] Although both technical and legal definitions of interoperability vary in their precise formulations, they share at least two common attributes.

First, interoperability is a relational concept. The term does not refer to any inherent feature of a system, but describes a relationship between or among two or more systems. As a result, interoperability cannot be gauged in isolation. Instead, to determine whether a system exhibits interoperability, that system must be considered in light of others with which it interacts. Consequently, a system exhibiting interoperability in one context may be noninteroperable in others.

Second, interoperability is not typically binary, but rather a matter of degree.[8] The extent to which two systems interoperate is a function

[6] MERRIAM WEBSTER ONLINE, http://www.merriam-webster.com/dictionary/interoperability (last visited April 29, 2009) (defining interoperability as "ability of a system . . . to work with or use the parts or equipment of another system").

[7] *See* 17 U.S.C. § 1201(f) (defining interoperability as "the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged"); 44 U.S.C. § 3601(6) (Supp. III 2005) (defining interoperability as "the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner"); Council Directive 91/250/EEC, 1991 O.J. (L 122) 42 (EC) (defining interoperability as "the ability to exchange information and mutually to use the information which has been exchanged"); INST. OF ELEC. & ELEC. ENG'RS, IEEE STANDARD COMPUTER DICTIONARY: A COMPILATION OF IEEE STANDARD COMPUTER GLOSSARIES 114 (1990) [hereinafter IEEE] (defining interoperability as "[t]he ability of two or more systems or components to exchange information and to use the information that has been exchanged"); INT'L ORG. FOR STANDARDIZATION, INFORMATION TECHNOLOGY VOCABULARY: FUNDAMENTAL TERMS (1993) (stating that interoperability is "[t]he capacity to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units"); URS GASSER & JOHN PALFREY, BREAKING DOWN DIGITAL BARRIERS: WHEN AND HOW ICT INTEROPERABILITY DRIVES INNOVATION 4 (2007), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/interop-breaking-barriers_1.pdf (describing interoperability as "the ability to transfer and render useful data and other information across systems (which may include organizations), applications, or components"); European Interoperability Framework for Pan-European eGovernment Services Version 1.0, http://europa.eu.int/idabc/en/document/3761 (defining interoperability as "the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge").

[8] *See* JONATHAN BAND & MASANOBU KATOH, INTERFACES ON TRIAL 8 (1995).

of how much information they share and the degree to which they can utilize that information. Complete seamlessness in the exchange and use of information between systems is difficult to achieve, but interoperability does not demand perfection.[9]

Because it is both relational and gradated, interoperability is a flexible, context-sensitive descriptor of a variety of interactions. However, these characteristics also introduce considerable imprecision. Even after a relationship is classified as interoperable, some important questions remain unanswered, among them the degree of reciprocity between two interoperable systems. Interoperability does not require that the stream of useful information between two systems flow in both directions. Interoperability, therefore, can embrace both bidirectional and unidirectional information exchanges. Further, interoperability can arise from cooperation between two or more systems or from a unilateral decision by the designers of a single system to interoperate with another.

Indeed, either system in a potential exchange of information can take steps to facilitate or frustrate interoperability. As a result, either system in an interoperable relationship can do the heavy lifting in the exchange of information.[10] A system encourages interoperability by using open, unencrypted, or easily reverse-engineered file formats, data structures, and communications protocols. These design choices yield outputs that other systems can use without a great deal of effort or expense.

Conversely, systems that encrypt data, employ proprietary data structures or communications protocols, or erect barriers to reverse engineering, discourage interoperability.[11] When systems share information in ways that impede interoperability, a heavy burden falls on those attempting to make use of that information. To do so, developers must either reverse engineer or license the necessary information. Reverse engineers often contend with both technical

[9] ROBERT J. GLUSHKO & TIM MCGRATH, DOCUMENT ENGINEERING: ANALYZING AND DESIGNING DOCUMENTS FOR BUSINESS INFORMATICS AND WEB SERVICES 172 (2005) ("Interoperability doesn't require that two systems be identical in design or implementation, only that they can exchange information and use the information they exchange.").

[10] Even if developers of two systems fail to establish interoperability on their own initiative, third parties can step in to bridge the gap. By establishing interoperability with each of the two systems, a third party can render those two systems interoperable with each other.

[11] Such steps could include the introduction of unnecessary complexity intended to thwart interoperability or the updating of protocols or specifications to interfere with existing interoperability.

complexity and intentional obfuscation that renders their efforts more difficult. Further, licensing may entail prohibitive costs, especially when interoperability poses a competitive threat to those in possession of the desired information.

Finally, a full description of interoperability must account for the role of the various components of interoperable systems. Although interoperability is typically understood as a system-level attribute, some definitions refer to components, functional units, software, and hardware as potentially interoperable objects.[12] Likewise, commentators sometimes speak of the importance of data interoperability.[13] However, understanding the role of data in enabling interoperable relationships requires reflection.

A system is "[a] collection of components organized to accomplish a specific function or set of functions."[14] These components include not only software and hardware, but data as well. Thinking of hardware or software as sharing usable information poses little difficulty. Just as systems can share and use information, so can the programs that comprise them. Data, however, does not immediately lend itself to being characterized as sharing and using information.

Data can be conceptualized as either passive or active. The passive view holds that data conveys information only after it has been processed or operated on by a program or other external interpreter.[15] So while data may be passed from one system to another, it does not engage in the active process of sharing usable information that defines interoperability. This conception of data as inert suggests that "interoperable data" simply means data presented in a manner that facilitates the exchange of usable information between systems. Data that is unencrypted or organized using standard formats contributes to interoperability even if, standing alone, that data does not actively share information.

The active view, in contrast, recognizes that the line between program and data is often not clearly defined.[16] Just as programs

[12] *See supra* note 7.

[13] *See, e.g.*, Stacy Baird, *The Government at the Standards Bazaar*, 18 STAN. L. & POL'Y REV. 35, 37-41 (2007) (discussing need for data interoperability in healthcare and national security contexts); Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2376 (1994) ("Interoperability applies to data as well.").

[14] IEEE, *supra* note 7, at 196.

[15] *See* R.L. Ackoff, *From Data to Wisdom*, 16 J. APPLIED SYS. ANALYSIS 3, 3-4 (1989).

[16] *See* MARTIN DAVIS, THE UNIVERSAL COMPUTER: THE ROAD FROM LEIBNIZ TO TURING 164-65 (2000) (describing distinction between program and data as illusion); Allen Newell, *The Models Are Broken, The Models Are Broken!*, 47 U. PITT. L. REV. 1023, 1033

contain instructions for the interpretation and manipulation of data, the structure and arrangement of data is itself partly responsible for its interpretation. From this perspective, data is not just a collection of raw facts, but contains ordered and structured information that it can share with interoperable systems.

The active view of data has some explanatory force. When two programs do not interact directly, it might make more sense to think of an interoperable relationship existing between one program and data created by another. Imagine two word processors — Microsoft Word and Apple's Pages — residing on separate systems. When Pages opens and renders a Word file, is it interoperating with an application or data? Because Pages does not interact directly with Word, characterizing the relationship as program-to-data interoperability could be a more helpful conceptual tool. Regardless of which characterization more accurately describes the role of data, both perspectives confirm that data, just like programs, can facilitate interoperability.

Interoperability, then, is a nonbinary description of a relationship between two or more systems or their components — among them hardware, software, and data — wherein information is shared and used. With this general understanding of interoperability established, the next subpart turns to the value of interoperability, in particular its impact on innovation and competition.

### *B. Valuing Interoperability*

Although the intrinsic value of interoperability is often apparent to end-users, particularly in its absence, its value is largely instrumental. Interoperability is typically celebrated because it fosters a number of socially desirable ends: innovation, competition, consumer choice, and accessibility, among others.[17] Although these justifications for promoting interoperability hold true in most cases, a fuller account of the practical consequences of interoperability reveals considerable complexity and nuance.[18] In some instances, increased interoperability could lower innovative and competitive incentives and

(1986) (stating that "the boundary between data and program — that is, what is data and what is procedure — is very fluid").

[17] *See* S. REP. NO. 105-190, at 32 (1998), (discussing the role of interoperability in "foster[ing] competition and innovation"); Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 3 (2005) (describing concern of network neutrality advocates that "reduction in interoperability would impair the environment for competition and innovation").

[18] *See* GASSER & PALFREY, *supra* note 7, at 18.

undermine the strategies of firms that hope to establish exclusivity over ancillary goods and services.

Interoperability encourages certain types of innovation, but can reduce incentives for others. Incremental innovation, the process of improving and extending existing technologies, benefits from the interaction with existing products that interoperability enables. Because incremental innovation leverages prior innovative activity, it typically requires less investment, spurring contributions from a wider variety and greater number of developers. Not surprisingly, these incremental advances account for the lion's share of innovation.[19] However, interoperability potentially hampers innovators who create new technologies from the ground up. First, the network effects that emerge from interoperable technologies could prove difficult to overcome, even for a superior offering.[20] Second, the possibility that follow-on innovators could interoperate and appropriate some of the value of a revolutionary innovation could reduce incentives for creating groundbreaking products.[21]

The effect of interoperability on competition is similarly complicated. In markets that feature interoperability, barriers to entry tend to be lower because innovations can take advantage of existing infrastructure and customer bases. Likewise, interoperability lowers switching costs because existing investments are not lost when migrating to a new interoperable product. As a result of increased competition, consumers of interoperable products tend to enjoy lower prices and a greater number and variety of available choices.

Under some circumstances, however, interoperability can reduce competition. Competition could suffer if a handful of firms agree to interoperate but exclude newcomers from the resulting interoperable network. Further, interoperability may also discourage Schumpeterian competition.[22] Incentives to create new technologies

---

[19] *See* Steve P. Calandrillo & Ewa M. Davison, *The Dangers of the Digital Millennium Copyright Act: Much Ado About Nothing?*, 50 WM. & MARY L. REV. 349, 407 (2008).

[20] *See* Joseph Farrell & Garth Saloner, *Standardization, Compatibility, and Innovation*, 16 RAND J. ECON. 70, 71 (1985). Network effects or network externalities exist when the value of a good or service to a consumer increases as more consumers utilize that good or service. *See id.*

[21] *See* Joseph Farrell & Michael L. Katz, *The Effects of Antitrust and IP Law on Compatibility and Innovation*, 43 ANTITRUST BULL. 609, 636 (1998).

[22] *See* Michael L. Katz & Howard A. Shelanski, *"Schumpeterian" Competition and Antitrust Policy in High-Tech Markets*, 14 COMPETITION 47 (2005) ("At the heart of the Schumpeterian argument is the assertion that, in important instances, competition primarily occurs through cycles of innovation, rather than through static price or

that supplant the current market, rather than compete within it, are arguably lessened where competitors are free to interoperate. Without the promise of temporary dominance and monopoly rents, the investment necessary for innovation-based competition is a less attractive risk.[23]

Interoperability also promotes consumer access to innovation and creative works. Other considerations being equal, information and services are more likely to find their way into more hands in markets that feature interoperability than those that do not. In part, increased accessibility is an outgrowth of the reduced price and increased choice brought about by competition. In addition, interoperability facilitates access by allowing information to permeate technological barriers that limit distribution. But this permeability could have unexpected consequences. The strong network effects interoperability creates could marginalize information excluded from a dominant network. These potential exclusionary practices aside, generally as interoperability increases, so too does accessibility.

These considerations suggest that the methods by which interoperable products and services are created matter. For example, if interoperability requires agreements between competitors, incentives for radical innovation and dynamic competition might increase. However, the risk of collusive behavior and barriers to entry for incremental innovators would likely increase accordingly. On the other hand, legal rules permitting unauthorized efforts to achieve interoperability could have the opposite effect, spurring incremental innovation and increased static competition.

The net impact of interoperability is a fact-intensive question and one this Article will not endeavor to resolve fully.[24] To the extent unauthorized interoperability reduces incentives for radical innovation, but increases incentives for incremental improvements, that question turns, in part, on the relative value of those species of innovation and the competition they encourage. Any such estimate must also account for the potential disparity between the incentives currently provided by IP regimes and those necessary to spur innovation. An optimal IP

output competition. Firms in such markets compete for temporary dominance of the market through the introduction of new generations of relevant technology.").

[23] Imagine, for example, that prior to inventing the telephone, Bell had been informed that rather than enjoying decades of exclusivity with respect to his incipient technology, competitors could freely interoperate with the network his invention would yield. Under such circumstances, Bell's incentives to undertake the innovative process likely would have been reduced.

[24] *See* GASSER & PALFREY, *supra* note 7, at 18.

system offers incentives sufficient to induce innovative activity, but no more.[25] In an IP system that over-incentivizes innovators, unauthorized interoperability could serve to reduce deadweight loss. Under such circumstances, interoperability could eliminate unnecessary exclusivity that inhibits competition and follow-on innovation, but does not yield any increase in innovative activity.

Regardless of interoperability's broadly dispersed benefits, individual firms have strong incentives to limit interoperability with their own offerings. Firms with large user bases and established reputations are particularly likely to oppose interoperability for two reasons.[26] First, interoperability tends to lower barriers to entry created by network effects.[27] Second, interoperability increases the relative value of competing products by enabling access to the dominant network.[28] Both of these effects favor less-established firms over their larger rivals.

History offers no shortage of examples of efforts to resist interoperability.[29] Edison's refusal to allow his records to be played on Columbia and Victor phonographs evidenced a reluctance to permit rivals to profit from his established network and reputation.[30] Railroads offer another useful set of early examples. Czarist Russia used railroad gauges wider than those common in Europe to slow

[25] *See* William W. Fisher III, *Property and Contract on the Internet*, 73 CHI.-KENT L. REV. 1203, 1249 (1998) (arguing copyright should "give creators enough entitlements to induce them to produce the works from which we all benefit but no more"); Glynn S. Lunney, Jr., *Patent Law, the Federal Circuit, and the Supreme Court: A Quiet Revolution*, 11 SUP. CT. ECON. REV. 1, 5 (2004) (suggesting patent protection should be conferred only to "precise extent[] necessary to secure each individual innovation's *ex ante* expected profitability").

[26] Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424, 425 (1985).

[27] Farrell & Katz, *supra* note 21, at 611 (discussing tendency of network effects to increase barriers to entry).

[28] Farrell & Saloner, *supra* note 20, at 71.

[29] Sometimes third parties that reap the benefit of inefficiencies introduced by incompatibility, oppose interoperability. In 1853 for instance, an effort to replace the three gauges of railroad tracks in Erie, Pennsylvania, with a uniform track width prompted bloody riots. *See* Achsah Nesmith, *A Long Arduous March Toward Standardization*, SMITHSONIAN MAG., Mar. 1, 1985, at 176. Local workers that unloaded cargo, changed car wheels, and then reloaded cargo at the juncture of these incompatible gauges rightly feared unemployment. *See id.*

[30] Columbia and Victor records were interchangeable because their phonographs used the same playback technology. Edison utilized a unique playback technology — ensuring that its records could only be played on its machines — and refused to license an adapter to allow Edison records to play on competing hardware. *See* RANDALL STROSS, THE WIZARD OF MENLO PARK 219-20 (2007).

potential invaders,[31] a strategy shared by developers who rely on proprietary formats to limit access to their platforms.[32] In India, the British laid nonuniform tracks to regionalize trade,[33] a tactic not unlike the contemporary region coding of DVDs and video games to enable market segmentation.[34]

Regardless of the desires of particular firms to exercise control over interoperable technologies, the precise social value of interoperability remains difficult to measure. Although it spurs innovation and competition in many instances, it may inhibit them in others. Despite this uncertainty, as the discussion below describes, IP law operates from the typically implicit, but occasionally explicit, assumption that interoperability should be encouraged, or at least permitted, in most circumstances. Nonetheless, IP doctrine reflects some sensitivity to the potential downsides of interoperability through the greater degree of exclusivity afforded by patent protection.

### *C. IP & Interoperability Policy*

Trade secrecy, copyright, and patent law have each adopted their own set of principles, rules, and exceptions that implicate interoperable technologies. As a result, IP law does not exhibit any explicit, unified approach to interoperability. Nonetheless, an articulable interoperability policy emerges from the aggregate operation of these doctrines. That policy generally permits, and occasionally encourages, unauthorized interoperability. This policy infrequently interferes with attempts to create unlicensed interoperable technologies — most notably, when a valid patent controls the interfaces necessary for communication between two systems. Although this policy is partly the result of specific exceptions and defenses sensitive to interoperability concerns, it flows largely from freestanding limits on the scope of the relevant exclusive rights.

The law of trade secrets facilitates interoperability by recognizing reverse engineering — the process of "starting with the known product and working backward to find the method by which it was

---

[31] *See* BAND & KATOH, *supra* note 8, at 40-41.

[32] The Nintendo Gamecube console, for example, was designed to accept miniature game discs rather than standard-sized DVDs as a means to prevent use of unauthorized copies. *See* Alex Pham & Jon Healey, *Games Prove a Hassle for Web Pirates*, L.A. TIMES, May 17, 2003, at C1.

[33] *See* BAND & KATOH, *supra* note 8, at 41.

[34] *See* Stephen Manes, *You Can't Do That to Me!*, FORBES, Oct. 30, 2006, at 82, *available at* http://www.forbes.com/forbes/2006/1030/082.html.

developed"[35] — as a legitimate means to obtain information about lawfully acquired products.[36] Without reverse engineering, developers would be unable to discover communications protocols, format specifications, and other program interfaces that enable interoperability.[37] The favored status of reverse engineering, however, grows out of fundamental limits on the scope of trade secret protection, rather than any express intent to encourage interoperability.

Likewise, the longstanding limits on the extent to which copyright regulates interoperable technologies create a legal environment hospitable to interoperability. First, copyright law does not grant exclusive rights in systems or their functional components, and excludes them from the scope of protection of otherwise protected subject matter.[38] By refusing protection for this key class of potentially interoperable objects, copyright law avoids directly regulating

[35] UNIF. TRADE SECRETS ACT § 1 cmt. 2 (amended 1985); *see* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) (defining reverse engineering as "starting with the known product and working backward to divine the process which aided in its development or manufacture"); Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1577 (May, 2002) (defining reverse engineering as "the process of extracting know-how or knowledge from a human-made artifact").

[36] *See Kewanee Oil*, 416 U.S. at 476 (recognizing reverse engineering as proper); Nat'l Tube Co. v. E. Tube Co., 3 Ohio C.C (n.s.) 459, 462 (1902) (permitting use of information discovered "by examination of the manufactured products sold or offered for sale to the public"); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995); UNIF. TRADE SECRETS ACT § 1 cmt. 2 (stating reverse engineering is proper if product was acquired by "fair and honest means").

[37] *See, e.g.*, Secure Serv. Tech., Inc. v. Time & Space Processing, Inc., 722 F. Supp. 1354, 1361 (E.D. Va. 1989) (permitting reverse engineering of secure facsimile machines to discover implementation of communications protocol necessary for interoperability). In the business-to-business context, when products are made available only to those who have agreed to terms prohibiting disclosure or reverse engineering, rather than the public at large, such acts face more substantial challenges. *See* ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.05[5][III] (2004) (discussing likelihood that contractual terms could render reverse engineering improper in some circumstances).

[38] *See* Baker v. Selden, 101 U.S. 99, 107 (1879) (holding that copyright in text describing system of accounting did not extend to system itself); *see also* Perris v. Hexamer, 99 U.S. 674, 675 (1878) (holding that copyright in map "marked with arbitrary coloring and signs" was not infringed by map using similar system). Congress codified Baker's holding in the Copyright Act of 1976. *See* 17 U.S.C. § 102(b) (2006). For a detailed discussion of *Baker*, its progeny, and their implications for the scope of copyright protection, see Pamela Samuelson, *Why Copyright Law Excludes Systems and Processes from the Scope of Its Protection*, 85 TEX. L. REV. 1921, 1921-77 (2007).

interoperability.[39] The originality requirement,[40] the doctrines of merger, scènes à faire,[41] and copyright misuse likewise contribute to copyright's permissiveness regarding interoperability.[42]

Copyright law also avoids interference with interoperability by limiting the extent to which its exclusive rights reach users of copyrighted works and developers of technology. The mere use of lawfully acquired copies of protected works — as opposed to their reproduction and distribution — typically falls outside of the copyright holder's statutory monopoly.[43] Simply put, copyright

[39] *See* Lotus Dev. Corp. v. Borland Int'l, 49 F.3d 807, 815 (1st Cir. 1995) (holding that menu command hierarchy of spreadsheet application was method of operation), *aff'd by an equally divided court*, 516 U.S. 233, 233 (1996); Brown Instrument Co. v. Warner, 161 F.2d 910, 910-11 (D.C. Cir. 1947) (holding chart that served as component of measuring device ineligible for copyright protection); Taylor Instrument Cos. v. Fawley-Brost Co., 139 F.2d 98, 100 (7th Cir. 1943) (holding that chart used as component of apparatus that measured and recorded temperatures was "as indispensable to the operation of a recording thermometer as are any of the other elements," and thus "not the proper subject of copyright"); *see also* Samuelson, *supra* note 38, at 1936-37 (discussing *Taylor*).

[40] The originality requirement reinforces *Baker* by limiting copyright protection for the output of an unprotectable system. *See, e.g.*, ATC Distrib. v. Whatever It Takes Transmissions & Parts, Inc., 402 F.3d 700, 707 (6th Cir. 2005) (holding that system of numbering transmission parts was ineligible for copyright protection as either taxonomy or compilation of data); Southco, Inc. v. Kanebridge Corp., 390 F.3d 276, 282 (3d Cir. 2004) (en banc) (holding that serial numbers for identifying parts were characterized by "an utter absence of creativity," and allowing distributors of interchangeable parts to utilize identical numbers); Mitel, Inc. v. Iqtel, Inc., 124 F.3d 1366, 1376 (10th Cir. 1997) (holding that command codes used to program telecommunications hardware were unoriginal, allowing competitor to use interoperable codes). *But see* ADA v. Delta Dental Plans Ass'n, 126 F.3d 977, 979 (7th Cir. 1997) (holding that taxonomy of medical codes was original).

[41] Applied to computer programs, the merger and scènes à faire doctrines suggest that if a limited number of options exist to achieve a given function efficiently, interoperate with another application, or run in a given environment, copyright will not permit exclusive control over those program elements. *See* Computer Assocs. Int'l v. Altai, Inc., 982 F.2d 693, 709-10 (2nd Cir. 1992) (holding that merger doctrine precludes exclusive rights in structural choices dictated by efficiency, and analogizing programming constraints dictated by external hardware compatibility and interoperability requirements to those recognized by scènes à faire doctrine).

[42] *See* Alcatel USA, Inc. v. DGI Techs., Inc. 166 F.3d 772, 792-94 (5th Cir. 1999) (holding that reasonable juror could have concluded that license agreement that prevented development of interoperable products was misuse of copyright because it resulted in patent-like protections for unpatented devices).

[43] *See* Stover v. Lathrop, 33 F. 348, 349 (C.C.D. Colo. 1888) (holding that "the effect of a copyright is not to prevent any reasonable use of the book which is sold . . . merely using it, in no manner infringes upon the copyright"). Of course, public performance and display of a work crosses the line separating unregulated private use and a public exploitation within the copyright grant. *See* 17 U.S.C. § 106(4), (5) (2006).

provides no exclusive right to read.[44] Without the power to dictate the circumstances under which consumers read books, listen to records, or watch films, copyright holders are poorly positioned to control the use of interoperable technologies. Even where the use of such technologies gives rise to direct infringement by a user, limits on indirect liability insulate developers in most instances.[45]

But not all copyright rules favoring interoperability grow out of independent constraints on the scope of copyright protection. The reverse engineering privilege more explicitly recognizes the value of interoperability and copyright's role in promoting it. Although the discovery of unprotected program elements through reverse engineering often requires the literal copying of protected expression, courts regard such copying as a fair use when undertaken to achieve interoperability.[46] This willingness to enlist the fair use defense to address threats to interoperability suggests that copyright not only tolerates interoperable technologies, but also promotes them.

Patent protection offers rights holders the most direct means of asserting control over interoperable technologies. Nonetheless, much like trade secrecy and copyright, patent law avoids directly regulating interoperability in most cases. The creation of products that interoperate with patented inventions does not infringe unless it entails making, using, or selling the patented invention.[47] Although the Patent Act neither expressly prohibits nor permits reverse engineering,[48] the exhaustion doctrine ensures that purchasers are free

[44] *But see* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29, 31-32 (1994) (warning that expansive reading of reproduction right in digital environment could lead to copyright holder control over act of reading and other personal uses).

[45] Indirect liability enables copyright holders to exert control over the distribution and use of technologies that give rise to end-user infringement under four circumstances: first, if the distributor had actual knowledge of specific instances of infringement and failed to act on that knowledge; second, if the technology at issue is incapable of substantial noninfringing use, *see* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 490-93 (1984); third, if the distributor of that technology intentionally encourages or induces end-user infringement, *see* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 935-36 (2005); or fourth, if the distributor possesses the legal right and practical ability to control end-user infringement and enjoys a direct financial benefit from such infringement, *see* Perfect 10, Inc. v. Amazon.com, 508 F.3d 1146, 1173 (9th Cir. 2007) (citing *Grokster*, 545 U.S. at 930).

[46] *See* Sega Enters. v. Accolade, Inc., 977 F.2d 1510, 1527-28 (9th Cir. 1992) (holding that copying necessary to engage in reverse engineering was fair use); *infra* Part II.B.

[47] *See* 35 U.S.C. § 271 (2006).

[48] *Id.* (defining patent infringement and omitting any reference to acts of reverse

to use a patented product once lawfully sold.[49] Such use could include reverse engineering to achieve interoperability.

In the software context, however, patents may offer greater opportunities to restrict interoperability. First, reverse engineering software may entail copying or "making" the invention rather than merely using it, potentially rendering an exhaustion defense unavailable.[50] Second, given the prevalence of licensing agreements in the software context, such licenses could override the exhaustion principle to the extent courts treat unilateral prohibitions on reverse engineering as enforceable license limitations.[51] These concerns aside, patents most directly threaten the creation of unauthorized interoperable technologies when they cover interfaces that define communication between two systems. If a particular protocol or process is necessary to exchange information with a device or program and a valid patent controls that interface, interoperability requires the patent holder's permission.[52]

However, even acknowledging the role of patents, IP law infrequently interferes with unauthorized attempts to achieve interoperability. Some of the doctrines that contribute to this overarching policy are longstanding limits on the scope of IP rights; others are of more recent vintage and reflect direct judicial awareness of the value of interoperability. As the next Part details, the DMCA

engineering).

[49] *See* United States v. Univis Lens Co., 316 U.S. 241, 250-51 (1942) (holding when patent holder made first unrestricted sale of patented item, its exclusive rights with respect to that particular item were exhausted).

[50] Julie E. Cohen & Mark A. Lemley, *Patent Scope and Innovation in the Software Industry*, 89 CAL. L. REV. 1, 32 (2001) (noting that reverse engineering computer program by decompilation could constitute infringing "making," but urging courts to reject this approach).

[51] *See* Bowers v. BayState Techs., Inc., 320 F.3d 1317, 1323-25 (Fed. Cir. 2003) (enforcing anti-reverse engineering clause of software license); Mallinckrodt, Inc. v. Medipart, Inc., 976 F.2d 700, 707-09 (Fed. Cir. 1992) (holding that label reading "single use only" established a conditional sale sufficient to overcome exhaustion). *But see* Cohen & Lemley, *supra* note 50, at 33-34 (noting that courts have been divided on role of unilateral license provisions in altering application of exhaustion principles); Samuelson & Scotchmer, *supra* note 35, at 1630 (suggesting that courts should avoid enforcing anti-reverse engineering provisions to the extent they create "detrimental effect on competitive development and innovation").

[52] *See* Pamela Samuelson, *Are Patents on Interfaces Impeding Interoperability?*, 93 MINN. L. REV. (forthcoming 2009) (manuscript at 16-19, *available at* http://ssrn.com/abstract=1323838) (discussing impact of interface patents on interoperability); *see, e.g.*, Atari Games Corp. v. Nintendo of Am., Inc., 30 U.S.P.Q. 2d (BNA) 1401, 1414-15 (N.D. Cal. 1993) (holding that development of interoperable product infringed interface patent).

embodies a dramatic shift away from IP law's general receptiveness to interoperability. The DMCA facilitates unprecedented control over interoperable devices and services without any compelling justification for its departure from the interoperability policy that emerged in prior decades.

## II. ANTICIRCUMVENTION & INTEROPERABILITY

As network communication and digital copying technologies increased the threat of infringement, copyright holders expressed reluctance to distribute their works on the Internet in the absence of additional legal protections to "make digital networks safe places to disseminate and exploit copyrighted materials."[53] Reflecting these fears, two World Intellectual Property Organization treaties called for "adequate legal protection" against the circumvention of technological protection measures ("TPM").[54] Congress, ostensibly to implement its treaty obligations, enacted the DMCA in 1998.[55]

The DMCA defines two types of technological controls and two restrictions on their manipulation. Access controls are technological measures intended to prevent unauthorized access to copyrighted works. Copy controls are measures intended to prevent infringement of the exclusive rights afforded by copyright.[56] The DMCA regulates both circumvention — the act of decrypting an encrypted work, or otherwise disabling, removing, or avoiding a technological measure[57] — and trafficking — the manufacture, distribution, sale, or offering to the public of devices, tools, or technologies that enable circumvention.[58] With respect to access controls, the DMCA prohibits

[53] S. REP. NO. 105-190, at 2 (1998).

[54] WIPO Copyright Treaty art. 11, Dec. 20, 1996, S. Treaty Doc. No. 105-17 (1997), 36 I.L.M. 65, 84 (1997); WIPO Performances and Phonograms Treaty art. 18, Dec. 20, 1996, S. Treaty Doc. No. 105-17 (1997), 36 I.L.M. 76, 86 (1997)

[55] Arguably, implementing legislation was unnecessary in the United States because indirect copyright infringement liability reached the production and distribution of circumvention devices incapable of substantial noninfringing uses. *See* Pamela Samuelson, *Why the Anti-Circumvention Rules Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 531-32 (1999).

[56] 17 U.S.C. § 1201(a)(3)(B), (b)(2)(B) (2006). These two varieties of TPMs often overlap in practice, and courts struggle to classify them. *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 438 n.5 (2d Cir. 2001) (stating TPM is copy control even though "it might very well be that copying is not blocked"); 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085, 1097 (N.D. Cal. 2004) (stating TPM is copy control if copying allowed "is not particularly useful").

[57] 17 U.S.C. § 1201(a)(3)(A).

[58] *Id.* § 1201(a)(2), (b)(1). The trafficking bans apply to devices: (1) primarily

both circumvention and trafficking in circumvention technologies.[59] The DMCA likewise bans trafficking in technologies that circumvent copy controls.[60] The act of circumventing a copy control, while not prohibited by § 1201, may constitute copyright infringement.

This Part considers the impact of these prohibitions on interoperability. Because the DMCA enables broad rights-holder control over interoperable technologies, it deviates from IP law's traditional treatment of interoperability. Recognizing the DMCA's potential impact, Congress enacted § 1201(f) as a statutory exemption designed to limit the extent to which anticircumvention law disturbed existing interoperability policy. Both Congress and the courts, however, have undermined § 1201(f)'s effectiveness. First, courts have misinterpreted several of its basic requirements, encouraging overreaching claims far exceeding the scope of the DMCA's core concerns. Second, Congress chose to limit the scope of § 1201(f) to computer programs, a policy choice that rendered § 1201(f) ill equipped to safeguard interoperability fully.

### *A. The DMCA's Departure from Existing Interoperability Policy*

As Congress intended, the DMCA addresses activities that, if unfettered, could have discouraged the development of robust digital marketplaces for copyrighted works. By virtue of its breadth, however, the DMCA gives rise to a number of unintended consequences, including restricting interoperability.[61] Rather than allowing or encouraging interoperability in the absence of an applicable patent right, the DMCA enables those who employ TPMs to restrict the development, distribution, and use of interoperable technologies.

The DMCA, of course, does not prohibit interoperability. Developers remain free to interoperate with systems that do not incorporate TPMs. Likewise, the DMCA permits interoperation with TPM-restricted works so long as access and copying are authorized.

---

designed for circumvention; (2) with only limited commercially significant uses aside from circumvention; or (3) marketed for use in circumvention. *Id.*

[59] *Id.* § 1201(a)(1)(A), (a)(2).

[60] *Id.* § 1201(b)(1).

[61] *See* John A. Rothchild, *The Social Costs of Technological Protection Measures*, 34 FLA. ST. U. L. REV. 1181, 1198-1204 (2007) (discussing various negative externalities resulting from use of TPMs). *See generally* ELEC. FRONTIER FOUND., UNINTENDED CONSEQUENCES: TEN YEARS UNDER THE DMCA (2008), http://www.eff.org/files/DMCAUnintended10.pdf (reporting cases in which DMCA's anticircumvention provisions were used to suppress legitimate activities).

Developers that enable interoperability with works restricted by TPMs without the permission of the relevant rights holders, however, face potential liability under the DMCA.

The restraints on unilateral efforts to achieve interoperability are threefold. First, the DMCA discourages the creation of unauthorized interoperable products by prohibiting certain acts of reverse engineering.[62] The DMCA's circumvention ban functions at its core as a bar against the reverse engineering of products containing effective access controls.[63] To interoperate with a work protected by such a control, a developer must discover interface information through reverse engineering. Those acts of reverse engineering generally require access to the underlying work. But a developer that "avoid[s], bypass[es], remove[s], deactivate[s], or impair[s]" a TPM to gain access and obtain interoperability information risks violation of § 1201.[64]

Second, the DMCA adversely affects interoperability by prohibiting the distribution of interoperable products.[65] To interoperate with a work that incorporates an effective TPM, a product must include code that enables access or copying of the protected work. Otherwise, it would lack the ability to exchange information with the TPM-protected system. Products designed to access or copy a work protected by an effective TPM, however, are subject to the trafficking ban. Thus, the distribution of a product that interoperates with a work protected by a technological measure could constitute an independent violation of § 1201. Third, because the use of such a product could entail an act of circumvention, the DMCA exposes end users to potential liability for utilizing devices that enable interoperability.

In short, creating, distributing, or using products that interoperate with works restricted by effective TPMs may violate the circumvention or trafficking bans. [66] As a result, in the absence of any applicable

---

[62] *See* 17 U.S.C. § 1201(a)(1)(A).

[63] An access control is effective if "in the ordinary course of its operation, [it] requires the application of information, or a process or a treatment" before access to the underlying work is granted. 17 U.S.C. § 1201(a)(3)(B). Copy controls must meet an even lower bar. They are effective "if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title." *Id.* § 1201(b)(2)(B).

[64] *Id.* § 1201(a)(3)(A).

[65] *See* 17 U.S.C. § 1201(a)(2) & (b)(1).

[66] Imagine, for example, a device that enables unauthorized playback of TPM-restricted video content purchased from an online retailer. To create such a product, its developers would most likely reverse engineer the TPM system to understand its authentication system, likely engaging in one or more acts of circumvention in the

defense, the DMCA entitles copyright holders, TPM developers, or mere licensees to prevent the emergence of interoperable products so long as their protection measures satisfy the minimal statutory threshold for effectiveness.[67] This potential for control over interoperable technologies represents a marked departure from the treatment of interoperability under earlier IP doctrine. By yielding power over the development and distribution of products that interface with TPM-protected works, the DMCA results in control over interoperable technologies on par with that conferred by a patent grant.[68] But unlike a patent, which must satisfy the comparatively exacting standards of novelty and nonobviousness, an effective TPM must only restrict access and copying in the ordinary course of operation.[69] As a result, the DMCA offers a far less demanding path to exclusive control over interoperable technologies.

### *B. Section 1201(f): The Interoperability Exemption*

The DMCA's potential restraint of interoperability did not go unnoticed during the congressional debate.[70] Software industry groups argued that the DMCA would undermine *Sega v. Accolade*,[71] a case decided just six years earlier that vindicated the reverse engineering of software programs.[72] In response, Congress enacted § 1201(f) to preserve the right to reverse engineer computer programs for interoperability purposes.

process. To the extent the resulting device is designed to bypass that authentication system to ensure interoperability with TPM-restricted videos, the developers face potential liability under the DMCA's trafficking bans. Finally, if the device enables circumvention, each time an end user plays back a protected video, that user arguably engages in an act of circumvention.

[67] *See supra* note 63.

[68] *See* Dan L. Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 570 (2005) (suggesting "the anti-circumvention provisions may therefore play the role that patents sometimes play in suppressing device interoperation").

[69] 17 U.S.C. § 1201(a)(3)(B), (b)(2)(B).

[70] In addition to addressing concerns over interoperability, Congress attempted to limit the reach of the DMCA by creating a number of statutory exemptions protecting activities including encryption research and security testing. *See id.* § 1201(d)-(j). In addition, the DMCA permits the Librarian of Congress to define temporary exemptions from the circumvention ban for specific classes of copyrighted works if their noninfringing use has been adversely affected. *Id.* § 1201(a)(1)(B)-(C).

[71] JONATHAN BAND, INTEROPERABILITY UNDER THE DMCA 12 (2008), *available at* http://files.ali-aba.org/thumbs/datastorage/skoobesruoc/pdf/TSPV09_chapter_02_thumb.pdf.

[72] *See* Sega Enters. v. Accolade, Inc., 977 F.2d 1510, 1527-28 (9th Cir. 1992).

In *Sega*, the Ninth Circuit Court of Appeals held that creating intermediate copies of a computer program during reverse engineering was a fair use when undertaken to isolate unprotected program elements.[73] Sega developed the Genesis, a home video game console, and licensed third-party developers to create compatible games. Accolade, unwilling to agree to Sega's licensing terms, decided to create games interoperable with the Genesis system without Sega's assistance or approval. Instead, Accolade reverse engineered Genesis games to determine the console's interoperability requirements, creating copies of Sega's code in the process. Accolade then used the interface information gleaned from Sega's code to create its own interoperable games.[74] Sega sued Accolade, maintaining that the intermediate copying of its code in the reverse engineering process constituted copyright infringement.

The Ninth Circuit agreed with Sega that intermediate copying of software programs was a *prima facie* violation of the reproduction right.[75] Nonetheless, the court recognized that reverse engineering, and the attendant intermediate copying, were "the only means of gaining access to . . . unprotected aspects of the program" necessary to achieve interoperability.[76] Accordingly, the court held that Accolade's copying was a fair use.[77] While acknowledging that other legitimate interests could justify reverse engineering, *Sega* unambiguously identifies interoperability as worthy of promotion.[78] Other courts followed suit, holding that copying necessary for reverse engineering is a fair use.[79]

Software companies worried that the DMCA would allow platform developers like Sega to exclude unauthorized developers from achieving interoperability by veiling their works behind even the thinnest of technological measures. Sega, in fact, employed a

[73] *Id.* at 1527.

[74] *Id.* at 1515.

[75] *Id.* at 1519.

[76] *Id.*

[77] *Id.* at 1520.

[78] *Id.*

[79] *See, e.g.*, Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 603 (9th Cir. 2000) (holding that intermediate copying was necessary to reverse engineer BIOS of Sony Playstation to "gain access to [its] unprotected functional elements"); Atari Games Corp. v. Nintendo of Am., Inc., 975 F.2d 832, 843 (Fed. Cir. 1992) ("Reverse engineering, untainted by the purloined copy of the 10NES program and necessary to understand 10NES, is a fair use."). *But see* Compaq Computer Corp. v. Procom Tech., 908 F. Supp. 1409, 1419-21 (S.D. Tex. 1995) (holding that reverse engineering and copying plaintiff's hard drive threshold values was not fair use).

rudimentary protection measure to thwart the use of unlicensed games on its Genesis console.[80] Six years before the DMCA however, Accolade had no legal obligation to respect that restraint.[81] Developers understandably viewed a broad anticircumvention right as a threat to the freedom to interoperate endorsed by the Ninth Circuit in *Sega*.

Congress heeded these concerns by including an exemption to both the circumvention and trafficking bans meant to "ensure that the effect of [*Sega*] is not changed by enactment" of the DMCA.[82] Congress's intention 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 [the DMCA]" represented explicit congressional recognition of the permissibility of reverse engineering and the value of interoperability.[83]

Section 1201(f)(1) allows the circumvention of access controls if: (1) those controls restrict access to portions of a computer program; (2) the circumventor lawfully acquired a copy of that program; (3) circumvention occurs for the sole purpose of identifying and analyzing program elements necessary to achieve interoperability; (4) interoperability is sought with an independently created program; (5) the information obtained through reverse engineering is not otherwise readily available; and (6) the identification and analysis of the underlying work does not constitute infringement.[84] Section 1201(f)(2) allows the development and use of technologies that enable circumvention to the extent necessary to achieve

[80] *See Sega*, 977 F.2d at 1528.

[81] *See id.*

[82] S. REP. NO. 105-190, at 32 (1998), (citing *Sega*, 977 F.2d 1510). But § 1201(f), while titled the "Reverse Engineering" exemption, does not privilege all acts of reverse engineering, but only acts undertaken to achieve interoperability. *Sega* strongly suggests that reverse engineers with other legitimate rationales for identifying unprotected program elements could benefit from the fair use defense as well. *See Sega*, 977 F.2d at 1520. As a result, § 1201(f) does not permit reverse engineering to the full extent of prior law, but only under a limited subset of the circumstances permitted under *Sega*. *See* Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium"*, 23 COLUM.-VLA J.L. & ARTS 137, 149 n.35 (1999) (suggesting that § 1201(f) might not embrace all reverse engineering permitted under prior law).

[83] S. REP. NO. 105-190, at 32.

[84] 17 U.S.C. § 1201(f)(1) (2006). The language and basic requirements of § 1201(f) borrow heavily from Article Six of the EU Software Directive. *See* Council Directive 91/250/EEC, 1991 O.J. (L 122) 42 (EC); *see also* Jonathan Band & Taro Isshiki, *The New Anti-Circumvention Provisions in the Copyright Act: A Flawed First Step*, 3 CYBER LAW. 2 (1999).

interoperability.[85] Further, circumventors may distribute information lawfully acquired, or tools lawfully developed, for the sole purpose of enabling interoperability.[86]

Early § 1201 litigation demonstrated that Congress's concern over safeguarding interoperability was warranted. The very first complaint alleging violation of § 1201, as well as an early companion suit, targeted interoperable products created through reverse engineering.[87] Sony developed and marketed the Playstation, a video game console that played games stored on CD-ROM. Two companies, Connectix and Bleem, developed software emulators that allowed the owners of Playstation discs to play those games on their computers.[88] While the emulators were similar enough to the Playstation to enable cross-platform game play, Connectix and Bleem did not copy every element of the Playstation's internals. According to Sony, the emulators ignored an access control built into the Playstation platform — an authorization code on each disc. If a game disc did not contain this code, the Playstation refused to load it. Sony argued that because the emulators did not scan for this code, Connectix and Bleem circumvented a TPM that controlled access to Playstation games.[89]

[85] 17 U.S.C. § 1201(f)(2). Arguably the protections offered by § 1201(f) do not extend to end users of circumvention technologies, but only to their developers. Although § 1201(f)(2) permits one to "employ technological means to circumvent a technological measure . . . for the purpose of enabling interoperability," that subsection refers only to § 1201's antitrafficking provisions, not its anticircumvention provision. *Id.* The omission of a specific reference to circumvention liability in § 1201(f)(2) is peculiar for at least two reasons. First, one who "employs" a circumvention tool appears to be engaged in acts of circumvention rather than acts of trafficking, rendering defenses to the antitrafficking provisions inapposite. Second, the failure to extend protection against circumvention liability to end users would seem to undermine the purpose of exempting developers of circumvention tools. Developers would enjoy immunity for reverse engineering to obtain interoperability information, creating circumvention tools, and distributing those tools to enable interoperability. But consumers would still face liability for utilizing those admittedly privileged tools, a rather curious result. To the extent a literal reading of § 1201(f)(2) demands such a counterintuitive result, the statutory text should be revised. *See infra* note 266.

[86] *Id.* § 1201(f)(3).

[87] *See* ELEC. FRONTIER FOUND., *supra* note 61, at 11; *see also* Band & Isshiki, *supra* note 84 (noting that Sony's complaint against Connectix was first to allege circumvention violations under § 1201).

[88] The Connectix and Bleem emulators were developed for the Mac and Windows operating systems, respectively. To achieve interoperability, Connectix reverse engineered the copyrighted Playstation BIOS, an act ultimately deemed a fair use by the Ninth Circuit. *See* Sony Computer Entm't Inc. v. Connectix Corp., 203 F.3d 596, 609 (9th Cir. 2000).

[89] *See* Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 222-23 (2000) (testimony of

Sony's anticircumvention theory, however, was deeply flawed. Because any standard CD-ROM drive could read Playstation game data, it is far from clear that the Playstation authorization code functioned as an effective access control.[90] Thus, the "no mandate" provision of the DMCA freed the emulators of any obligation to comply with the Playstation authentication code.[91] In addition, Sony filed its complaints during the initial two-year moratorium on enforcement of the DMCA's circumvention ban.[92] Not surprisingly, Sony ultimately chose to abandon its § 1201 claims.[93]

Assuming Sony could have overcome these threshold obstacles,[94] the emulator cases would have provided an opportunity for courts to

Jonathan Hangartner), *available at* http://www.copyright.gov/1201/hearings/1201-519.pdf.

The source of Sony's hostility towards emulation is worth pausing to consider. Sony may have feared that emulators would encourage infringement of Playstation games, a worry of the very sort Congress hoped to alleviate with the DMCA. On the other hand, Sony may have feared that emulation offered the emerging PC gaming platform a competitive advantage. With the introduction of emulators, PC gamers could play the entire stock of Playstation games in addition to games developed specifically for the PC. If PCs became the dominant gaming platform, Sony risked losing a sizable portion of its revenues — in the form of reduced console sales and decreased licensing revenue — as consumers and game developers defected to the PC platform. Tellingly, after losing its copyright infringement suit against Connectix, Sony purchased the company, eventually discontinuing the emulation software rather than implement support for the Playstation authorization code. *See* Peter Cohen, *Sony Acquires Virtual Game Station from Connectix*, MACWORLD, Mar. 15, 2001, http://www.macworld.com/article/20791/2001/03/vgs.html; Sony Computer Entertainment, Inc. v. Connectix Corp., http://www.coolcopyright.com/cases/chp7/sonyconnectix.htm (last visited Apr. 21, 2009). Regardless of Sony's motivation, its anticircumvention claims would have resulted in control over interoperable technologies regardless of either copyright or patent infringement, control not envisioned by Congress when it enacted the DMCA.

[90] Standard CD-ROM drives do not read the region of the disc containing the authentication code, so the fact that the emulators did not acknowledge the code is not surprising. *See Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, *supra* note 89, at 222-23.

[91] *See* 17 U.S.C. § 1201(c)(3).

[92] *Id.* § 1201(a)(1)(A).

[93] Sony continued its litigation against Connectix and Bleem on other theories. *See Connectix*, 203 F.3d at 609 (holding that reverse engineering of PlayStation BIOS by Connectix was fair use); Sony Computer Entm't, Inc. v. Bleem, LLC, 214 F.3d 1022, 1030 (9th Cir. 2000) (holding that Bleem's use of screen shots from PlayStation games was fair use).

[94] Sony eventually succeeded in enforcing Playstation access controls under the DMCA. *See* Sony Computer Entm't Am., Inc. v. GameMasters, 87 F. Supp. 2d 976, 987-88 (N.D. Cal. 1999) (enjoining vendor of Game Enhancer device that allowed players to load games intended for foreign markets). Notably, Sony offered no proof that the Game Enhancer enabled infringement, only that it interfered with Sony's

apply § 1201(f) to facts similar to those that motivated its creation. The activities of Bleem and Connectix — reverse engineering a console to discover the technical requirements for interoperability — shared obvious similarities to the conduct at issue in *Sega*. In fact, the Ninth Circuit eventually held that Connectix was entitled to the *Sega* fair use defense for its reverse engineering of the Playstation console.[95]

The Playstation emulators present a fairly simple § 1201(f) analysis. Sony's alleged protection measure restricted access to Playstation games, computer programs lawfully acquired by Connectix and Bleem. The reverse engineering appears to have occurred for the sole purpose of obtaining information necessary to render Playstation games interoperable with independently created emulators. Further, § 1201(f)(1) would have permitted circumvention because these acts of reverse engineering did not constitute infringement — so long as the interoperability information was not readily available. Moreover, the distribution of the emulator software, assuming it enabled acts of circumvention, would have been privileged so long as facilitating interoperability was the sole purpose of its distribution.

The first case to consider § 1201(f), *Universal City Studios v. Reimerdes,* presented very different facts. The defendants were accused of distributing DeCSS, an application that defeated the Content Scramble System ("CSS") designed to prevent unlicensed players from decrypting and playing DVD movies.[96] According to the defendants, DeCSS fell within the protections of § 1201(f) because it enabled DVDs to interoperate with playback software written for Linux operating systems.[97]

The *Reimerdes* court offered expansive readings of the DMCA's liability provisions and narrow interpretations of its various defenses, among them § 1201(f).[98] The court's primary basis for rejecting defendants' § 1201(f) defense, one supported by both the text and legislative history of the provision, was that § 1201(f) applies only to the circumvention of protection measures that restrict access to

market segmentation strategy. *Id.*; *see also* Sony v. Divineo, 457 F. Supp. 2d 957, 968 (N.D. Cal. 2006) (granting summary judgment against defendants who trafficked in Playstation modification chips).

[95] *Connectix*, 203 F.3d at 609.

[96] Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 214 (S.D.N.Y. 2000).

[97] *Id.* at 218.

[98] *See id.*; Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 323 (S.D.N.Y. 2000) (asserting that DMCA "fundamentally altered the landscape" of copyright).

computer programs, not copyrighted works generally.[99] Because CSS restricted access to movies stored on DVDs, not computer programs, § 1201(f) did not apply. Had the court been satisfied with this decisive rationale, there would be little reason to criticize its § 1201(f) analysis. But *Reimerdes* considered additional elements of the interoperability defense, muddying the waters for future courts.

First, the court appeared to heighten the already demanding sole purpose requirement of § 1201(f) — that any acts of reverse engineering be undertaken for the "sole purpose" of achieving interoperability. Defendants argued that DeCSS was necessary to enable interoperability with Linux-based DVD player software. At the time, no licensed Linux-compatible DVD players were available, preventing Linux users from viewing lawfully purchased DVDs on their computers.[100] DeCSS, however, ran under both Windows and Linux. Because Windows users faced no shortage of authorized DVD players, the court concluded that DeCSS was not developed solely to enable interoperability.[101] Given defendants' emphasis on Linux-based players, the court's concern over Windows compatibility is understandable. In addition, the court likely recognized the risk that defendants might invoke interoperability as a pretext to legitimize circumvention aimed at infringement. Even acknowledging this worry, the mere fact that DeCSS could enable interoperability on both platforms, standing alone, reveals little about the purpose of its development. To the extent *Reimerdes* suggests that the sole purpose requirement demands a showing that interoperability is necessary to access or use a work, it misapplies the statute.

Second, the court misconstrued the limits on distribution of interoperability information and circumvention tools under § 1201(f)(3). Ignoring the plain language of § 1201(f), the court claimed the statute permitted dissemination of information obtained through reverse engineering, but not the means of circumvention used to obtain such information.[102] The court also erred in imposing a blanket rule against the public distribution of exempted tools and information.[103] The statute contains no express ban against public dissemination. Instead, it permits information lawfully obtained through reverse engineering, as well as exempted circumvention tools, to be made available so long as the sole purpose requirement is

[99] *See Reimerdes*, 82 F. Supp. 2d at 218; *infra* Part II.D.3.

[100] *See* DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 189 (Ct. App. 2004).

[101] *See Reimerdes*, 82 F. Supp. 2d at 218.

[102] *See* 17 U.S.C. § 1201(f)(2)-(3) (2006).

[103] *See Reimerdes*, 111 F. Supp. 2d at 320.

satisfied.[104] A defendant who makes information or tools widely available might face more difficulty meeting this requirement than one who makes a more limited disclosure, but the statute imposes no freestanding limit on the scope of distribution.

Since *Reimerdes*, § 1201(f) has been the subject of surprisingly little judicial analysis. In light of the interoperability concerns looming in many DMCA disputes, one would expect a higher frequency of § 1201(f)-based defenses. Nonetheless, only a handful of published opinions refer to § 1201(f), and no defendant has yet succeeded on a § 1201(f) defense. In the years following the DMCA's enactment, *Reimerdes* offered the sole judicial analysis of § 1201(f). The approach to DMCA interpretation embodied by *Reimerdes*, characterized by an expansive application of the DMCA's liability provisions and skepticism towards its statutory exemptions, has emboldened plaintiffs to test the bounds of their control over interoperable products.[105]

### *C. The Durable Goods Cases*

Early DMCA litigation focusing on entertainment content, while arguably protecting legitimate copyright interests, evinced a desire on the part of some plaintiffs to interfere with interoperable technologies.[106] As consumer electronics manufacturers began to enforce TPMs incorporated in their products however, any pretense of protecting against the threat of Internet-based infringement was abandoned. Courts ultimately proved hostile to these efforts to suppress interoperability, but failed to clarify the application of § 1201(f) in the process.

*Lexmark International v. Static Control Components* addressed one of the first attempts to incorporate TPMs into durable goods.[107] Lexmark, a manufacturer of laser and inkjet printers, like many of its competitors, sold printers cheap, but charged a premium for ink cartridges. To lessen incentives to refill empty cartridges or purchase cartridges refilled by third parties, Lexmark sold "prebate" cartridges at a deep discount in exchange for an agreement that consumers

[104] The court claimed that § 1201(f) permits the sharing of interoperability information only by one who acquires that information.

[105] See Jerome H. Reichman et al., *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981, 1005-06, 1024 (2007).

[106] *See* Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1110-11 (2003) (discussing anticompetitive uses of DMCA); Burk, *supra* note 68, at 561-65 (same).

[107] 387 F.3d 522 (6th Cir. 2004).

would use the cartridge only once and return it to Lexmark.[108] Lexmark employed a TPM intended to prevent unauthorized cartridges from interoperating with its printers.[109]

Lexmark alleged that Static Control Components ("SCC"), creator of the SMARTEK chip, which mimicked Lexmark's authentication sequence, was trafficking in a circumvention device.[110] According to Lexmark, the operation of its printers relied on the Printer Engine Program ("PEP"). If users installed a non-Lexmark cartridge, the authentication sequence would fail, rendering inaccessible those portions of the PEP that enabled printer functionality. The SMARTEK chip bypassed this control and allegedly enabled unauthorized access to the PEP.[111]

Although the District Court for the Eastern District of Kentucky granted Lexmark's request for a preliminary injunction,[112] the Sixth Circuit Court of Appeals regarded Lexmark's argument with palpable skepticism. The court eventually concluded that § 1201 did not apply to Lexmark's technology at all. According to the court, the authentication sequence did not control access to the PEP, which was neither encrypted nor otherwise protected against literal copying.[113] Because the authentication sequence did not meaningfully control access to the code, the DMCA simply did not apply.[114]

In *Chamberlain Group v. Skylink*, the Federal Circuit faced a similar theory.[115] Chamberlain manufactured the Security+ garage door opener ("GDO") system, which utilized a "rolling code" to modify the signal used by Chamberlain's remote transmitter to activate the GDO.[116] Skylink marketed universal remotes designed to interoperate

[108] This agreement took the form of a shrink-wrap license on the cartridge packaging. *Id.* at 530. Non-prebate cartridges, which were not subject to this restriction, could be purchased at a higher price. *Id.*

[109] Each time a printer was turned on, the printer and cartridge initiated an authentication sequence whereby each would calculate a code using an encryption algorithm. *Id.* If the codes matched, the printer accepted the cartridge and operated normally. *Id.* If the authentication sequence failed, the printer would not operate. *Id.*

[110] *Id.*

[111] *Id.*

[112] Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943, 974 (E.D. Ky. 2003). SCC admitted that its SMARTEK chips avoided or bypassed Lexmark's authentication sequence, and that they were designed to do so. *Id.* at 968.

[113] *Lexmark*, 387 F.3d at 546-47. Instead, according to the court, access was controlled by the purchase of a Lexmark printer. *Id.*

[114] *Id.* at 548.

[115] 381 F.3d 1178 (Fed. Cir. 2004).

[116] *Id.* at 1183.

with a variety of GDO systems, including the Security+ line.[117] Chamberlain filed suit, alleging that Skylink's universal transmitter violated the DMCA's anticircumvention provision. Under Chamberlain's theory, the rolling code system controlled access to the copyrighted code that operated its Security+ GDOs. By imitating the rolling code, Skylink transmitters permitted unauthorized access to the software that operated Chamberlain's GDOs. The district court rejected Chamberlain's theory, holding that consumers who purchased Chamberlain products were entitled to access the GDO software.[118]

On appeal, the Federal Circuit agreed that Chamberlain customers possessed an "inherent legal right to use" the software embedded in their GDOs.[119] Perhaps more importantly, the court held that to maintain an action under § 1201, a plaintiff must establish not only that an effective TPM restricts access to a copyrighted work, but that the circumvention of that TPM bears some "reasonable relationship to the protections that the Copyright Act otherwise affords."[120] Because consumers were entitled to access the GDO software, Chamberlain was unable to prove "the critical nexus between" the access facilitated by Skylink's device and the protection of a legitimate copyright interest.[121]

Together *Lexmark* and *Chamberlain* placed important limits on the scope of anticircumvention liability, but they left some questions unresolved. *Lexmark*, because of the technical and fact-specific basis of its holding, could allow future plaintiffs to succeed under slightly different facts. After all, if Lexmark had restricted access to the PEP more fully, perhaps by encrypting the program code, its § 1201 claim could have moved forward. Judge Merritt's concurrence took pains to warn that future litigants could not escape the court's hostility to similar claims through minor variations on the *Lexmark* facts.[122] How such permutations will be analyzed by future courts remains to be seen.

*Chamberlain* suffers from the opposite problem. Rather than being tied to specific facts, the Federal Circuit's nexus requirement offers courts and litigants limited guidance as to the factual and legal

[117] Rather than implementing an identical rolling code sequence, Skylink transmitters sent three signals in rapid succession that reset the rolling code sequence and activated the opener. *Id.* at 1184.

[118] Chamberlain Group, Inc. v. Skylink Techs., 292 F. Supp. 2d 1040, 1045-46 (N.D. Ill. 2003).

[119] *Chamberlain*, 381 F.3d at 1202.

[120] *Id.*

[121] *Id.* at 1204.

[122] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 551-52 (6th Cir. 2004) (Merritt, J., concurring).

predicates necessary for liability. Although the Federal Circuit held in a subsequent case that a defense under § 117 of the Copyright Act undermined the nexus,[123] the boundaries of the requirement remain largely undefined.

*Lexmark* and *Chamberlain*, although decided on different grounds, were motivated by a common set of concerns. Lingering below the surface of both cases were overarching worries over competition and interoperability that explain both courts' eagerness to deny protection under § 1201. Ultimately, Lexmark and Chamberlain had little interest in protecting their code from unauthorized access or copying. Instead, access to their works served as a convenient predicate for DMCA enforcement meant to protect aftermarkets for interoperable products. Both courts worried that by adding fragments of copyrighted code to consumer goods, manufacturers could "gain the right to restrict consumers' rights to use [their] products in conjunction with competing products."[124] Such power, in turn, could "create monopolies of manufactured goods"[125] that relied on the DMCA to provide "broad exemptions from . . . the antitrust laws."[126]

Despite the role interoperability played in motivating the *Lexmark* and *Chamberlain* courts, and the fact that § 1201(f) was briefed in both cases, neither court relied on the defense nor thoroughly analyzed its application.[127] The district court in *Chamberlain* made no mention of § 1201(f), and the Federal Circuit declined to reach the issue.[128] Because the court was satisfied that Chamberlain could not prove a *prima facie* violation of § 1201, the failure to delve into an affirmative defense provides little cause for criticism.[129]

---

[123] Storage Tech. v. Custom Hardware Eng'g, 421 F.3d 1307, 1319 (Fed. Cir. 2005). Section 117 of the Copyright Act provides an exception to infringement liability for the creation of copies of computer programs for the purposes of maintenance and repair of computer equipment. *See* 17 U.S.C. § 117(c) (2006).

[124] *Chamberlain*, 381 F.3d at 1201.

[125] *Lexmark*, 387 F.3d at 551 (Merritt, J., concurring).

[126] *Chamberlain*, 381 F.3d at 1193.

[127] *See* Brief of Computer & Communications Industry Ass'n as Amicus Curiae Supporting Skylink Technologies, Inc., *Chamberlain*, 381 F.3d 1178 (No. 04-1118); Brief of Electronic Frontier Foundation as Amicus Curiae Supporting Static Control Components, Inc., *Lexmark*, 387 F.3d 522 (No. 0305400).

[128] *Chamberlain*, 381 F.3d at 1201 n.15.

[129] The court continued this silence on § 1201(f) in *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, 421 F.3d 1307 (Fed. Cir. 2005). There, the district court held that because the defendant infringed plaintiff's copyright, § 1201(f) did not apply. Storage Technology Corp. v. Custom Hardware Eng'g & Consulting, Inc., No. 02-12102, 2004 U.S. Dist. LEXIS 12391, at *15 (D. Mass. July 2, 2004). Although it reversed the infringement holding, the Federal Circuit saw no

*Lexmark* offered some clarification of the independent creation requirement of § 1201(f), even if only in dicta. The Sixth Circuit explained that independent creation only requires proof of originality; the new program must not infringe the protected program.[130] The district court's findings that SCC's program "serve[d] no legitimate purpose other than to circumvent Lexmark's authentication sequence" and contained copies of unprotected Lexmark code were insufficient to undermine SCC's defense.[131] In the end, however, *Lexmark* offered no definitive holding on § 1201(f), concluding only that SCC "may benefit from the interoperability defense, at least in the preliminary injunction context."[132]

Although both courts were reluctant to reach the issue, the facts in *Lexmark* and *Chamberlain* presented fairly straightforward applications of § 1201(f). SCC and Skylink both sought to circumvent TPMs that restricted access to computer programs, clearing the hurdle that proved decisive in *Reimerdes*. Likewise, both defendants wrote interoperable programs that contained original code sufficient to qualify as independently created. Lastly, neither their acts of reverse engineering nor the distribution of the resulting tools constituted copyright infringement.

Perhaps most importantly, *Lexmark* and *Chamberlain* offered an opportunity to clarify the demands of the sole purpose requirement.[133] Certainly, both SCC and Skylink were motivated by a desire to render their products interoperable with systems restricted by TPMs. But this motive was in no strict sense their sole purpose. Interoperability was not their ultimate aim, but an instrumental goal. The sale of ancillary products and the undermining of their rivals' market positions are just two examples of the many purposes from which the desire to interoperate could flow. Rather than focus on higher order goals that a court may find suspect, the analysis of § 1201(f) should rely on a functional investigation of the circumventor's objective that looks to the manner in which the information obtained was used. This is precisely

need to revisit the interoperability question.

[130] Likewise, because the Toner Loading Program was not protected, its copying did not constitute infringement under § 1201(f)(3). *Lexmark*, 387 F.3d at 551. The court rejected two other limitations on § 1201(f) proposed by Lexmark: (1) any independently created programs "must have existed prior to" the acts of reverse engineering; and (2) any technological means developed to circumvent must be "necessary or absolutely needed" to achieve interoperability. *Id.* at 550-51.

[131] Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943, 974 (E.D. Ky. 2003).

[132] *Lexmark*, 387 F.3d at 550.

[133] *See* 17 U.S.C. § 1201(f)(1) (2006).

the sort of inquiry the Ninth Circuit undertook in *Sega*, the case Congress expressly intended § 1201(f) to preserve. Under such an analysis, § 1201(f)'s permitted purpose — identifying and analyzing program elements necessary for interoperability — can be contrasted with the desire to distribute copies of protected works or to identify elements necessary for the development of noninteroperable programs. Circumventors who make such uses lack the requisite sole purpose.

No evidence suggests that SCC hoped to develop its own program to control the internal operation of printers manufactured by Lexmark or any of its competitors. Nor did Skylink circumvent Chamberlain's rolling code to copy its GDO firmware or create a competing GDO. In both instances, regardless of the downstream motivation of the defendants, the sole functional purpose of their reverse engineering was to obtain interoperability information.

*Lexmark* and *Chamberlain*, much like *Connectix* and *Bleem*, represent missed opportunities for courts to counterbalance the misinterpretation of § 1201(f) offered in *Reimerdes*. *Lexmark* and *Chamberlain* both articulated meaningful outer boundaries on the scope of § 1201. However, they may have more effectively curbed further efforts to restrict interoperability had they squarely addressed § 1201(f). As discussed below, the absence of clear authority applying § 1201(f) has given rise to subsequent DMCA case law that threatens interoperability despite the limits imposed by *Lexmark* and *Chamberlain*.

### *D. The Continuing Threat to Interoperability*

Commentators have rightly praised *Lexmark* and *Chamberlain* for resisting the expansive interpretation of the DMCA embodied in *Reimerdes*,[134] but neither opinion has proven a panacea for the DMCA's restriction of interoperability. Plaintiffs have continued to view the DMCA as a tool to reduce competition from interoperable products, and § 1201(f) has become mired in even deeper judicial misinterpretation. However, the inadequacy of anticircumvention's interoperability policy cannot be placed entirely at the feet of the courts; some blame rests with the narrow text of § 1201(f).

[134] *See, e.g.*, Burk, *supra* note 68, at 571 ("The *Chamberlain* and *Lexmark* opinions radically change the trend begun in *Reimerdes* . . . ."); Niva Elkin-Koren, *Making Room for Consumers Under the DMCA*, 22 BERKELEY TECH. L.J. 1119, 1132-34 (2007) (noting approvingly explicit recognition of consumer interests in *Chamberlain*).

1. Durable Goods Revisited

In the wake of *Lexmark* and *Chamberlain*, mobile phones emerged as the next consumer product subject to specious anticircumvention claims. Just like printers sold cheap in the hope of profits from expensive ink, mobile phones are often subsidized by service charges recouped over the life of the phone.[135] As a result, providers have strong incentives to limit the availability of interoperable services.

Mobile phones contain various programs that enable their many functions, including firmware that controls the ability to connect to a cellular network. Carriers typically configure phones to connect only to their own network[136] and rely on a variety of TPMs to prevent users from accessing and reconfiguring firmware to allow connections to competing networks.[137] Not surprisingly, consumers have been eager to overcome these restrictions on the use of interoperable networks, and third-party vendors have assisted them. Through a process known as unlocking, consumers and vendors bypass these TPMs to enable connections to other networks. In some instances, unlocking involves the input of reverse-engineered numeric codes.[138] In other cases, end users unlock their phones by deleting both the firmware and the associated TPM, then installing new firmware that enables connectivity.[139]

TracFone is a vendor of prepaid mobile phones, which it sells at a loss.[140] Once the prepaid minutes included with each phone expire, customers can purchase additional minutes from TracFone. To prevent customers from obtaining cheaper service elsewhere, TracFone relies on TPMs that prevent connections to competing networks.[141] TracFone has filed a series of lawsuits alleging violations of § 1201 by vendors that unlocked and resold its phones.

---

[135] *See* Tim Wu, *Wireless Carterfone*, 1 INT'L J. COMMS. 389, 398-99 (2007).

[136] *See* COMMENTS OF THE WIRELESS ALLIANCE & ROBERT PINKERTON 4, http://www.copyright.gov/1201/2006/comments/granick_wirelessalliance.pdf.

[137] *See id.* at 7 (discussing variety of technological means used by carriers).

[138] *See Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 40-41 (Mar. 23, 2006), http://www.copyright.gov/1201/2006/hearings/transcript-mar23.pdf [hereinafter *Hearings*] (testimony of Jennifer Granick and Steven Metalitz).

[139] *See id.*

[140] TracFone Wireless, Inc. v. GSM Group, Inc., 555 F. Supp. 2d 1331, 1333 (S.D. Fla. 2008).

[141] *Id.* at 1334. Apple too has drawn criticism for its use of technological measures to require iPhone customers to subscribe to the AT&T network. *See generally* Mark DeFeo, *Unlocking the iPhone: How Antitrust Law Can Save Consumers from the Inadequacies of Copyright Law*, 49 B.C. L. REV. 1037 (2008) (noting consumer

As the Register of Copyrights recognized in the 2006 DMCA Anticircumvention Rulemaking,[142] a consumer who unlocks a phone to connect to another network is not "engaging in copyright infringement or in activity that in any way implicates copyright infringement or the interests of the copyright owner."[143] Because unlocking is a noninfringing use, mobile phone firmware was included in a temporary exemption from the circumvention ban so long as unlocking occurs for the sole purpose of lawfully connecting to a wireless network.[144]

Nonetheless, this exemption has not deterred TracFone from continuing its aggressive pursuit of those who unlock its handsets. Indeed, TracFone has prevailed in a string of recent § 1201 cases, only one of which even considered the mobile phone exemption.[145] In that case, the court denied a motion to dismiss notwithstanding the exemption because the complaint alleged that the defendants' purpose was not solely wireless network connectivity, but also reselling unlocked phones.[146]

The court's unreasonably rigid analysis of the exemption's sole purpose requirement falls into the same trap discussed above in connection with § 1201(f). That requirement does not ask courts to peer into the ultimate aim or purpose for which lawful connection to a wireless network is sought. Its drafters intended that language to exclude circumvention by those seeking access to ringtones, video content, and other copyrighted works stored on mobile phones.[147]

opposition to Apple's exclusive arrangement with AT&T and evaluating potential antitrust challenges).

[142] *See* 17 U.S.C. § 1201(a)(1)(C) (2006) (empowering Librarian of Congress to exempt, on a temporary basis, classes of copyrighted works from anticircumvention ban to extent it interferes with noninfringing use of those works).

[143] RECOMMENDATION OF THE REGISTER OF COPYRIGHTS 50 (Nov. 17, 2006), http://www.copyright.gov/1201/docs/1201_recommendation.pdf [hereinafter RECOMMENDATION].

[144] *Id.* at 50-51.

[145] *See GSM Group*, 555 F. Supp. 2d at 1337 (rejecting defense premised on unlocking exemption on basis of allegations that defendant's sole purpose was not lawful connection to telephone network); TracFone Wireless, Inc. v. Bitcell Corp., No. 07-22249, 2008 U.S. Dist. LEXIS 41955, at *9 (S.D. Fla. May 28, 2008) (entering consent judgment and permanent injunction); TracFone Wireless, Inc. v. Dixon, 475 F. Supp. 2d 1236, 1238 (M.D. Fla. 2007) (granting unopposed permanent injunction on basis of both circumvention and trafficking claims); TracFone Wireless, Inc. v. Sol Wireless, No. 05-23279, at 3 (S.D. Fla. Feb. 28, 2006), *available at* http://www.stopcellphonefraud.com/wp-content/uploads/1-tracfone-v-sol-wireless-group-inc-et-al.pdf (entering stipulated final judgment enjoining unlocking).

[146] *GSM Group*, 555 F. Supp. 2d at 1337.

[147] *See Hearings*, *supra* note 138, at 44-46 (testimony of Steven Metalitz).

Although the mobile phone exemption should have prevailed over TracFone's circumvention theory, the exemption offered no colorable defense to its trafficking claim.[148] So even assuming courts apply the temporary mobile phone exemption more carefully, trafficking allegations could persist.

TracFone's litigation strategy suggests that *Lexmark* and *Chamberlain* did not close the door on the use of the DMCA to suppress interoperability, even in markets for consumer electronics with embedded software. As the Copyright Office understood, TracFone has no interest in protecting its copyrighted firmware from potential infringement.[149] Instead, it hopes to protect its business model and pricing scheme from competitive forces by preventing consumers from connecting to interoperable networks. TracFone's success has been largely unopposed, with the courts lending their imprimatur to private settlement agreements. It remains far from clear whether TracFone's § 1201 theory will hold up to genuine scrutiny.

To the extent TracFone alleges that unlockers delete firmware and the TPM that protects it, § 1201 appears altogether inapposite. Read literally, the DMCA might prohibit the removal of a TPM regardless of whether or not such removal enables access to the underlying work.[150] But where the protected code is neither run nor accessed, but simply deleted along with the TPM, none of the interests Congress intended to recognize in § 1201 are implicated. Copyright does not protect against the deletion of computer programs, and the DMCA should not be read to confer new power over the removal of programs from lawfully acquired hardware.

If instead, unlockers bypass protection measures to gain unauthorized access to firmware, the threshold requirements of § 1201 could be met. Under appropriate facts, *Lexmark* and *Chamberlain* may limit liability.[151] But TracFone's success suggests

---

[148] Although the Copyright Office can exempt certain works from the ban on circumvention, its rulemaking authority does not extend to the prohibition on trafficking in circumvention devices or services. 17 U.S.C. § 1201(a)(1)(E) (2006). *See generally* Aaron Perzanowski, *Evolving Standards and the Future of the DMCA Anticircumvention Rulemaking*, 10 J. INTERNET L. 1 (2007) (detailing limitations on scope of Copyright Office's rulemaking authority).

[149] *See* RECOMMENDATION, *supra* note 143, at 50.

[150] *See* 17 U.S.C. § 1201(a)(3)(A) (including "remov[al]" of TPM among acts considered circumvention).

[151] *Chamberlain* relied in part on customers' "inherent legal right to use" their garage door openers, a right unrestricted by any contractual obligations. *Chamberlain*, 381 F.3d 1178, 1202 (Fed. Cir. 2004). But if carriers contractually restrict the ability of customers to connect to competing networks, *Chamberlain* may prove inapplicable.

that the limits those cases impose are sufficiently unclear to justify settlement by multiple defendants, even if TracFone's claims are ultimately flawed on the merits.

Section 1201(f) offers unlockers another plausible defense. Although unlocking enables interoperability with communications networks, those networks are composed of not only base stations and radio signals, but also software that controls network communications.[152] Therefore, the practical effect of unlocking is interoperability between mobile phone firmware and other independently created programs. But without applicable precedent, courts may be reluctant to apply § 1201(f) to facts that appear, on the surface, far from those that Congress anticipated. As discussed below, the opinions that followed *Lexmark* and *Chamberlain* did little to encourage courts to extend § 1201(f) to those facts or any others.

2. *Davidson*: Re-Misinterpreting § 1201(f)

Just one year after *Lexmark* and *Chamberlain*, the Eighth Circuit Court of Appeals affirmed the most extensive and deeply misguided analysis of § 1201(f) to date. *Davidson & Associates v. Jung* tested the application of the DMCA to the development of interoperable services for the online play of copyrighted video games.[153] While *Reimerdes* introduced considerable uncertainty, *Davidson* and the district court opinion it affirmed threaten to undermine fundamentally § 1201(f) through their consistently hostile misinterpretation of the statute.[154]

*Davidson* involved Blizzard, the developer of several multi-player PC games. Blizzard offered an online matchmaking service, Battle.net, which allowed players to compete over the Internet. Battle.net relied on a secret handshake with Blizzard games to validate unique CD keys. If the key was invalid or in use by another player, Battle.net denied access, preventing the use of infringing copies of Blizzard games on the Battle.net server.[155]

But as the Copyright Office has confirmed, unlocking poses no threat to legitimate copyright interests, so the nexus required by *Chamberlain* appears utterly lacking. *See* RECOMMENDATION, *supra* note 143, at 50.

[152] KAVEH PAHLAVAN & ALLEN H. LEVESQUE, WIRELESS INFORMATION NETWORKS 10 (2005) (noting role of base stations, radio signals and antennae, and software programs in cellular networks).

[153] 422 F.3d 630 (8th Cir. 2005).

[154] *See id.* at 640-42; Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1183-85 (E.D. Mo. 2004), *aff'd sub nom.*, 422 F.3d 630 (8th Cir. 2005).

[155] *Davidson*, 422 F.3d at 633 nn.2-3.

A group of Blizzard enthusiasts, frustrated with certain shortcomings of Battle.net, developed an alternative matchmaking service, dubbed bnetd, that interoperated with Blizzard games.[156] The bnetd project reverse engineered the protocols used by Blizzard games to communicate with Battle.net and developed a functionally equivalent server and software that allowed players to connect to it.[157] But because bnetd lacked access to Blizzard's database of CD keys, it was unable to ensure that all players used legitimate copies of Blizzard games.[158]

Blizzard sued the bnetd team, alleging violations of the circumvention and trafficking bans of § 1201. Blizzard argued that the secret handshake controlled access to "Battle.net mode," the ability to play Blizzard games online.[159] Bnetd raised § 1201(f) as a defense, arguing that any circumvention of Blizzard's access controls simply enabled reverse engineering necessary to render the bnetd server software interoperable with Blizzard games. Any tools bnetd distributed that facilitated circumvention, it maintained, were likewise intended to enable interoperability.[160]

The district court rejected bnetd's § 1201(f) defense for several reasons. First, the court claimed that bnetd could not rely on § 1201(f) because it lacked permission to circumvent. The district court appeared to confuse the basic elements of a § 1201 violation with the requirements of the interoperability defense, stating that "[t]he statute . . . only exempts those who obtained permission to circumvent the technological measure."[161] Of course, if bnetd had permission, an affirmative defense would be unnecessary.

Second, the court found that the sole purpose of bnetd's circumvention was not to enable interoperability, but "to avoid the anticircumvention restrictions of the game and to avoid the restricted

---

[156] These complaints included frequent unreliability and widespread cheating. *Id.* at 635 n.6.

[157] *Id.* at 636.

[158] *Id.*

[159] Premising DMCA liability on access to "Battle.net mode" was problematic. Neither the district court nor the Eighth Circuit settled on any one description of Battle.net mode, suggesting at various turns that it was a component of the game code, a part of the Battle.net server, and something in between. *See* A.H. Rajani, Note, Davidson & Associates v. Jung*: (Re)interpreting Access Controls*, 21 BERKELEY TECH. L. J. 365, 377-78 (2006). But users of bnetd gained no access to the Battle.net server and already had access to the contents of their unencrypted Blizzard game discs.

[160] Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1183 (E.D. Mo. 2004), *aff'd sub nom.*, 422 F.3d 630 (8th Cir. 2005).

[161] *Id.* at 1185 (citing Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001)).

access to Battle.net."[162] If the court meant that bnetd's purpose for circumvention was to circumvent, it is correct. But this tautology does little to resolve the question of the purpose of bnetd's circumvention.

The court offered four reasons to suspect bnetd's motives: (1) the bnetd server did not verify users' CD keys; (2) the bnetd software was distributed for free; (3) bnetd distributed its software in binary form; and (4) the bnetd server source code was made available.[163] Again, rather than probing bnetd's motives for achieving interoperability, the court should have confined its inquiry to the functional purpose of the acts of reverse engineering made possible by circumvention. Bnetd did not circumvent in hopes of copying Blizzard's protected expression or creating an infringing game. The bnetd developers used the information they sought solely to create a program that interoperated with Blizzard's games. Whether bnetd distributed the resulting program for free or for profit, with closed or open source, is of little consequence.

Only the first of the court's reasons points to any plausible basis to doubt bnetd's purpose.[164] If bnetd created a tool that achieved interoperability but disregarded Blizzard's efforts to suppress the use of infringing copies of its games, perhaps bnetd's purpose embraced not only interoperability but the encouragement of infringement as well. The evidence, however, suggests that any inference drawn against bnetd, even on this ground, was unjustified. The bnetd developers requested access to Blizzard's CD key database to enable screening for infringing copies, a request Blizzard denied.[165] Blizzard, of course, had no obligation to comply, but bnetd's request is entirely consistent with a lawful purpose to enable interoperability.

Third, the court rejected bnted's § 1201(f) defense on the grounds that the bnetd server was not an independently created computer program because it was "intended as a functional alternative to the Battle.net service," one that was indistinguishable from Battle.net from the standpoint of users.[166] But this functional equivalence simply suggests that bnetd was successful in its attempt to enable interoperability. By counting this fact against bnetd, the court

---

[162] *Id.* at 1186.

[163] *Id.* at 1185.

[164] Denying protection under § 1201(f) because bnetd distributed its software for free is particularly inappropriate. The court could just as easily have imputed impure motives to bnetd for profiting from its interoperable software.

[165] *See* Letter from Cindy A. Cohn to Rod Rigole (Mar. 11, 2002), http://www.eff.org/pages/eff-letter-blizzard-vivendi.

[166] *Davidson*, 334 F. Supp. 2d at 1185.

betrayed a deep misunderstanding of the activities § 1201(f) was meant to privilege. Moreover, the court ignored clear congressional intent. Independent creation requires only that "[t]he resulting product . . . be a new and original work, in that it may not infringe the original computer program."[167] As the court should have understood, the fact that the two servers were functionally interchangeable did not establish infringement.

This failure to analyze any supposed infringement was central in the court's fourth reason for rejecting bnetd's defense. According to the court, "the development and distribution to others [of the bnetd software] constituted copyright infringement," violating the final requirement of § 1201(f).[168] But the court articulated no theory, much less an analysis, of copyright infringement. The bnetd software, although functionally equivalent to the Battle.net server, does not appear to have copied any of its code. Nor does the record support a finding of infringement based on copying of any Blizzard games. Without any infringement analysis, the court's conclusion, that bnetd could not avail itself of the § 1201(f) defense as a result of its supposed acts of infringement, is entirely unfounded.

On appeal, the Eighth Circuit failed to improve upon the district court's mangled reading of § 1201(f). Instead, it introduced further confusion. The court rejected bnetd's defense on the grounds that its circumvention constituted infringement because unauthorized copies of Blizzard games could be played on the bnetd server.[169] As an initial matter, the court was wrong to ask whether the circumvention was an act of infringement. The relevant question is whether the acts of identification and analysis enabled by circumvention, or the subsequent sharing of information and tools that enable circumvention, were acts of infringement. Here the Eighth Circuit may have confused § 1201(f)'s reference to "infringement" — the unauthorized exercise of the exclusive rights defined in § 106 of the Copyright Act — with a violation of § 1201. However, if "infringement" referred to § 1201 violations, qualifying for the interoperability defense would be a logical impossibility because acts of infringement are a bar to a § 1201(f) defense.

These flaws aside, the fact that some users connected to the bnetd server using unauthorized copies of Blizzard games does not prove that bnetd infringed Blizzard's copyrights. Unless bnetd's reverse

[167] S. REP. NO. 105-190, at 32 (1998).

[168] *Davidson*, 334 F. Supp. 2d at 1187.

[169] Davidson & Assocs. v. Jung, 422 F.3d 630, 642 (8th Cir. 2005).

engineering entailed unfair copying or its software tools contained infringing expression, the court lacked any justification for its conclusory finding of infringement. The Eighth Circuit's opinion simply contains no analysis to support its pronouncement of infringement.

The district court's struggle in *Davidson* to make sense of the basic elements of § 1201(f), coupled with the Eighth Circuit's disinterest in an independent analysis, leave developers of interoperable technologies in an unenviable position. Aside from the Sixth Circuit's nonbinding receptiveness to § 1201(f) in *Lexmark*, defendants can point to no favorable interpretations of the defense. As a result, even defendants who fall squarely within the protections for reverse engineering and interoperability created by Congress face considerable uncertainty. Judicial misinterpretation, however, explains only part of the failure of § 1201(f). Congress's choice to limit the exemption's scope to computer programs ensures that the statute cannot insulate all interoperable technologies from liability.

### 3. The Shortcomings of § 1201(f)

The text of § 1201(f) reflects the legislative compromise responsible for its enactment. The exemption tempered the nearly unlimited anticircumvention provisions favored by the entertainment industry, but gave advocates of reverse engineering and interoperability fewer safeguards than they might have preferred. Reverse engineers who extract uncopyrightable processes and principles to create noninteroperable products are not privileged under § 1201(f).[170] Nor are researchers who investigate the operation of TPMs, their effectiveness, and their implications for security and privacy.[171]

---

[170] *See* H.R. REP. NO. 105-551, pt. 2, at 43 (1998) ("If a person makes this information available for a purpose other than to achieve interoperability . . . then such action is a violation of this Act.").

[171] Sections 1201(g) and (j), the encryption research and security testing exemptions, offer researchers some protection under narrowly defined circumstances. For a discussion of the impact of § 1201(g) on encryption research, see generally Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L.J. 501 (2003) (arguing that academic encryption research should be allowed under DMCA). Even outside of the encryption context, TPM research can offer significant benefits to the public. As the Sony BMG rootkit incident made clear, TPMs can cause serious security and privacy threats best discovered and exposed by independent researchers. *See* Deirdre K. Mulligan & Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. 1157, 1232 (2007). More recently, DRM employed on PC video games has given rise to similar concerns. *See* Comment of J. Alex Halderman, In the Matter of Exemption to

Aside from its failure to accommodate reverse engineering for other legitimate purposes, § 1201(f) does not embrace all interoperable technologies. Section 1201(f) permits the circumvention of technological measures that protect computer programs, but not "works generally, such as music or audiovisual works . . . distributed in digital form."[172] As a result, interoperable products that make use of technologically protected entertainment content or other works are open to attack under the DMCA.

The disparity in the treatment of these two classes of interoperable technologies is the result of two problematic distinctions. First, this inequality relies on a clear division between technological measures that protect computer programs and those that protect other copyrighted works. Second, it relies on a distinction between program interoperability and data interoperability. Both distinctions are the product of factual oversimplifications, and neither supports exempting one class of interoperable technologies while subjecting the other to DMCA liability.

TPMs cannot be neatly divided between those that restrict the use of entertainment content and those that control the use of computer programs. Frequently, the same TPM serves both functions. An early § 1201 dispute, *RealNetworks, Inc. v. Streambox, Inc.*, illustrates the difficulty in drawing such distinctions. RealNetworks ("Real") developed technology for streaming audio and video files encoded in its RealMedia formats. Real used a "secret handshake" between its RealServer and RealPlayer client to ensure that third-party applications could not stream RealMedia files. If an application requesting a file from RealServer did not execute the handshake, access was denied.[173]

Real obtained a preliminary injunction against Streambox, developers of the VCR, an application that mimicked the secret handshake to interoperate with RealServer. The court found that the handshake served as an effective access control, one the VCR circumvented by mimicking RealPlayer.[174] The key question the RealPlayer presented, however, was not whether the handshake

Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. RM 2008-8, at 5-6, http://www.copyright.gov/1201/2008/comments/halderman-reid.pdf (describing risks associated with Macrovision's SafeDisc and Sony's SecuROM technologies).

[172] H.R. REP. NO. 105-551, pt. 2, at 33; *see also* Samuelson & Scotchmer, *supra* note 35, at 1635 n.289 (noting that § 1201(f) does not extend to program-to-data interoperability).

[173] RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889, at *6 (W.D. Wash. Jan. 18, 2000).

[174] *Id.* at *19-20.

restricted access, but rather, to what copyrighted works it restricted access. Although the court correctly found that the handshake restricted access to RealMedia files, it also restricted access to the RealServer application. Without authentication, users were unable to access that portion of the RealServer that enabled streaming. To prevent access to RealMedia files, Real simultaneously limited access to the RealServer software. To the extent that TPMs restrict access to both entertainment content and computer programs, the clean distinctions presupposed by the DMCA are difficult to draw.[175]

The *Streambox* litigation also illustrates the second problematic distinction at work in § 1201(f). The StreamboxVCR ignored Real's "Copy Switch," a bit of code that reflected copyright holder preferences about end user copying. As a result, Streambox could have faced difficulty in establishing that interoperability was its sole purpose under § 1201(f).[176] But setting aside that fact, consider a hypothetical application that interoperated with the RealServer and fully complied with the copy switch: one that functioned exactly like RealPlayer and presented precisely the same risk of infringement. Because the handshake restricted access to entertainment content, § 1201(f) would have been unavailable.

The unavailability of § 1201(f) in such circumstances ignores the role of data in enabling interoperable relationships, hampering § 1201(f)'s ability to accommodate interoperability fully.[177] While interoperability sometimes depends on access to a computer program, it may depend on the ability to extract interoperability information from data created or used by that application. When access to these inputs and outputs is restricted, interoperability suffers.

Even the definition of interoperability in § 1201(f) — "the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged" —

[175] The text and legislative history of § 1201(f) are clear that the defense was meant to apply to TPMs that restrict access to computer programs and not to those that restrict access to digital media. The status of dual purpose TPMs — those that simultaneously restrict access to both types of works — is ambiguous as a textual matter. However, the DMCA's definitional focus on program-to-program interoperability strongly suggests that circumvention that aims to enable interoperability between a program and data or media would not be privileged under § 1201(f).

[176] Unlike in *Davidson*, no evidence suggests that Streambox made any effort to comply with the copy switch.

[177] *See* URS GASSER & JOHN PALFREY, DRM-PROTECTED MUSIC INTEROPERABILITY AND EINNOVATION 21 (2007), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/interop-drm-music_0.pdf.

reflects an undue focus on program-level interoperability.[178] Under Congress's definition, computer programs exhaust the class of potentially interoperable objects. Had Congress embraced a broader system-level view of interoperability, rather than drawing a bright line between programs and data, it may have recognized that both programs and data are system components capable of enabling interoperability.

Congress's focus on program-level interoperability has two related explanations. First, the content industry, concerned that broad exemptions would undo § 1201's prohibitions, opposed the adoption or expansion of proposed exemptions.[179] Second, the software industry, the primary proponent of § 1201(f), had finite influence. The software industry focused its efforts on maintaining the ability to access other programs for reverse engineering, a practice central to prevailing industry practices. Data interoperability presented a less pressing concern to software developers, and by extension, Congress.

The distinction between program and data interoperability, while explicable as a matter of legislative process, is deeply problematic. The definition of "computer program" provided by the Copyright Act hints, albeit unintentionally, at the difficulty of drawing inflexible distinctions between program and data. Section 101 defines a computer program as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result."[180] Of course, the result experienced by a user of digital content is brought about by instructions contained in both the application and the data file.

A hard and fast distinction between program and data is particularly inappropriate with respect to § 1201(f) for two additional reasons. Congress explicitly intended the interoperability exemption to preserve *Sega*. The *Sega* court permitted the reverse engineering of video games — works that straddle the line between computer programs and digital entertainment content. Further, files distributed in TPM-restricted formats exhibit program-like characteristics. Those files contain functional instructions distinct from the movies or music

[178] 17 U.S.C. § 1201(f)(4) (2006).

[179] *See, e.g.*, *Hearing on H.R. 2281 Before the H. Subcomm. on Telecommunications, Trade, and Consumer Protection*, 105th Cong. 7-8 (June 5, 1998) (testimony of Steven J. Metalitz), *available at* http://www.hrrc.org/File/June5-98Hearing.pdf (describing "a host of additional amendments . . . to narrow the anti-circumvention provisions" that were "not absolutely necessary . . . and that cut back on the rights of copyright owners" as "not . . . especially popular with the MPAA or its member companies").

[180] 17 U.S.C. § 101 (2006).

they encode. Files in TPM-restricted formats contain instructions that control the ability of other programs or devices to interoperate.

Ultimately, the distinction between data and program interoperability cannot justify the stark differences that distinction creates in the scope of DMCA protection. As a more recent dispute makes clear, the narrow language of § 1201(f) furnishes providers of TPM-restricted content unprecedented control over playback technologies.

Several years after its litigation against Streambox, RealNetworks was at the center of another interoperability controversy, this time as the alleged circumventor. Apple's iPod is the world's most popular portable music player, and its iTunes store is the top music retailer in the United States.[181] The only digital rights management ("DRM") technology supported by the iPod is Apple's FairPlay. Real's competing download service utilized its own Helix DRM technology. Thus, music purchased from Real could not be played back on the iPod.[182] Given the iPod's popularity, Real's customers demanded compatibility.

Real proposed a tactical alliance, under which Apple would license Real's use of FairPlay, and Real would promote the iPod to its customers.[183] Apple declined.[184] Months later, determined to enable iPod interoperability, Real announced a technology called Harmony that converted Real's Helix-protected files into a format that successfully mimicked FairPlay.[185] Real touted Harmony as a boon for "[c]ompatibility, choice and quality" that "follow[ed] in a well-established tradition of fully legal, independently developed" interoperable technologies.[186] Apple responded by accusing Real of "adopt[ing] the tactics and ethics of a hacker to break into the

---

[181] *See* Eric Bangeman, *Apple Passes Wal-mart, Now #1 Music Retailer in US*, ARS TECHNICA, Apr. 2, 2008, http://arstechnica.com/news.ars/post/20080402-apple-passes-wal-mart-now-1-music-retailer-in-us.html; Arik Hesseldahl, *A Real Rival for Apple's iPod?*, BUSINESS WEEK, Sept. 19, 2006, http://www.businessweek.com/technology/content/sep2006/tc20060918_036885.htm.

[182] *See* John Borland, *RealNetworks Breaks Apple's Hold on iPod*, CNET, July 26, 2004, http://news.cnet.com/RealNetworks-breaks-Apples-hold-on-iPod/2100-1027_3-5282063.html.

[183] *See* Geoff Duncan, *Apple Refuses to Sing with Real's Harmony*, TidBITS, Aug. 2, 2004, http://db.tidbits.com/article/7756.

[184] *See id.*

[185] Press Release, RealNetworks Statement About Harmony Technology and Creating Consumer Choice (July 29, 2004), http://realnetworks.com/company/press/releases/2004/harmony_statement.html.

[186] *Id.*

iPod."[187] Apple then threatened both legal action under the DMCA and technological self-help to disrupt Harmony.[188]

Ultimately, Apple relied on the latter option. A few months after the release of Harmony, Apple updated its iTunes software to block the use of converted Real files.[189] Nonetheless, Real eventually achieved iPod interoperability. It did so not by reverse engineering or licensing FairPlay, but by selling mp3 files unencumbered by DRM and compatible with all portable players, including the iPod.[190]

Because Apple did not file suit against Real, it never clearly articulated its DMCA theory. Harmony enabled Real customers to access music protected with its own Helix DRM on the iPod; it did not enable them to access music purchased from iTunes and protected with FairPlay. Thus, an argument that Real trafficked in a tool that enabled unauthorized access to iTunes content was a non-starter. However, Apple may have contended that FairPlay restricted access not to iTunes music, but to the iPod's embedded software. In the ordinary course of operation, iPod users could access the playback software on their iPod only if they loaded unencrypted or FairPlay-protected files on the device. By mimicking FairPlay, Apple could have argued, Harmony enabled unauthorized access to software embedded on the iPod.

Although the connection to potential infringement is arguably more substantial than in *Chamberlain*, a court so inclined could have rejected Apple's claim based on the Federal Circuit's nexus requirement. The act of accessing the iPod's software to play lawfully purchased content creates little, if any, risk of infringement. Likewise, a court could have held that users were authorized to access the iPod's software by virtue of purchasing the device. More importantly, to the extent that Apple characterized its DRM as restricting access to the iPod software, it opened the door to a § 1201(f) defense, a defense Real stressed in its response to Apple's threats. In short, a DMCA theory premised on unauthorized access to the iPod faced substantial difficulties.

Apple's more plausible claim would have alleged that Real's reverse engineering during the creation of Harmony circumvented FairPlay,

---

[187] Apple Statement (July 29, 2004), http://prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/07-29-2004/0002221065.

[188] *Id.*

[189] *See* John Borland, *Apple Fights RealNetworks' 'Hacker Tactics'*, CNET, Dec. 14, 2004, http://news.cnet.com/2102-1027_3-5490604.html.

[190] *See* Arnold Kim, *Rhapsody Relaunches with iPod-Compatible MP3s*, MACRUMORS, June 30, 2008, http://www.macrumors.com/2008/06/30/rhapsody-relaunches-with-ipod-compatible-mp3s.

resulting in unauthorized access to iTunes music. If such circumvention occurred,[191] a § 1201(f) defense would face major challenges. Although Real's reverse engineering was intended to enable interoperability between its system and the iPod, the protections of § 1201(f) would be unavailable under the prevailing reading because FairPlay restricted access to entertainment content, not iPod software.[192] Likewise, *Lexmark* would have been of limited value to Real. FairPlay, unlike the TPM at issue in *Lexmark*, utilized encryption to control effectively access to the underlying copyrighted material.

The *Chamberlain* framework represented Real's strongest potential defense. To the extent Real circumvented FairPlay solely for reverse engineering purposes, an act squarely within the fair use privilege under *Sega*, any nexus between circumvention and infringement would appear to be lacking. But a number of considerations suggest that the success of such a defense would have been far from certain. First, although the Federal Circuit has relied on statutory defenses — namely the maintenance and repair provisions of § 117[193] — to disconfirm the required nexus, it has not explicitly held that the notoriously context-dependent fair use defense would apply with equal force. Second, while at least one district court has followed the Federal Circuit's *Chamberlain* framework, no other Courts of Appeals have yet adopted *Chamberlain*.[194] Third, *Chamberlain*'s hostility to the

[191] Real claimed it developed Harmony using only publicly available information, suggesting that circumvention was unnecessary. Indeed, Real may have created Harmony by reverse engineering existing FairPlay circumvention tools. *See* Posting of Ernest Miller to Corante, http://importance.corante.com/archives/005301.php (July 26, 2004, 17:52 EST).

[192] The hurdles facing a § 1201(f) defense in the context of digital media interoperability can be contrasted with the greater likelihood of success of that same defense in the context of iPhone application interoperability. Apple tightly controls the applications authorized for use on the iPhone. Low-level cryptographic checks ensure that the iPhone operating system has not been altered and that all installed applications have been approved. Developers unable or unwilling to obtain Apple's approval for their applications, as well as the users of such applications, must rely on "jailbreaking" — the process of reconfiguring the iPhone to run unapproved code. Apple maintains that this activity violates § 1201. *See* Responsive Comment of Apple Inc., In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. RM 2008-8, at 26, http://www.copyright.gov/1201/2008/responses/apple-inc-31.pdf. But because the TPMs at issue are designed to restrict access to computer programs, the threshold requirement of § 1201(f) is satisfied. Although the other elements of the defense, most importantly the sole purpose requirement, must also be met, jailbreakers enjoy a reasonable likelihood of success under § 1201(f).

[193] *See supra* note 123.

[194] *See* Agfa Monotype Corp. v. Adobe Sys., Inc., 404 F. Supp. 2d 1030, 1034 (N.D.

DMCA claims at issue stem in part from the incongruity of using a statute enacted to protect digital media content to gain exclusivity over household appliances. Because the digital music protected by FairPlay is much nearer to the core concerns Congress intended to address with the DMCA, courts may have been reluctant to apply *Chamberlain* in this context.

Section 1201(f), the DMCA's primary legislative safeguard for interoperability, has proven inadequate. The *Chamberlain* and *Lexmark* decisions, while placing important limits on the scope of DMCA protection, offer developers of interoperable technologies insufficient assurance in the digital media context. In response, developers and advocates of interoperable technologies have turned to other legal frameworks to resist the restrictions on interoperability enabled by the DMCA. Not surprisingly, given the potential competitive implications of the DMCA, antitrust has emerged as the preferred means of externally restraining the power afforded by § 1201 over interoperable technologies. The next Part examines both the efficacy and desirability of this approach.

## III. ANTITRUST & INTEROPERABILITY

Because the DMCA is ill equipped to address fully its interference with interoperability, consumers, competitors, and regulators have looked to antitrust law to limit the control TPMs yield over interoperable technologies. This Part considers recent efforts to use antitrust principles to lower the barriers facing unauthorized interoperable products, taking the controversy surrounding Apple's DRM technology as a useful test case for gauging the role antitrust is likely to play in this arena. Although antitrust remedies — notably, mandatory disclosure of technical information — could facilitate interoperability, antitrust law may not offer an ideal set of tools for correcting the DMCA's impact. Whether their activities are characterized as tying, denial of essential facilities, or refusal to deal, firms that rely on TPMs to impede interoperability appear unlikely to face consistent antitrust enforcement efforts. Given the deference antitrust law typically affords to the lawful exercise of legitimately acquired IP rights,[195] antitrust appears unlikely to disturb the enforcement of the broad grants provided by the DMCA.

Ill. 2005) (adopting *Chamberlain* framework).

[195] Reliance on antitrust to enable interoperability has practical implications as well. To the extent that it is less subject to capture than the IP legislative process, antitrust may be well suited to balance the value of creative incentives against the

### *A. Mandating Disclosure*

The mandatory disclosure of interoperability information is not an uncommon antitrust remedy. U.S. antitrust authorities, and their European counterparts, have required parties to license or disclose information to enable the development of competing and interoperable products.[196] The cases against Microsoft in the U.S. and Europe provide recent examples of mandatory disclosures of interoperability information. In its settlement with the United States, Microsoft agreed to disclose communications protocols and application programming interfaces.[197] In Europe, Microsoft was required to disclose protocol specifications that enabled interoperability between Windows and work group server operating systems.[198]

value of a robust public domain. *See* Herbert J. Hovenkamp, *Innovation and the Domain of Competition Policy*, 60 ALA. L. REV. 103, 117 (2008). In addition, antitrust allows for forward-looking remedies that may guard against technological efforts to disrupt interoperability. On the other hand, these ongoing remedial structures could pose administrability problems for courts. *See* Verizon Commc'ns v. Law Offices of Curtis V. Trinko, 540 U.S. 398, 414 (2004); *see also* Phillip Areeda, *Essential Facilities: An Epithet in Need of Limiting Principles*, 58 ANTITRUST L.J. 841, 853 (1989) (arguing that "when compulsory access requires the court to assume the day-to-day controls characteristic of a regulatory agency," no antitrust remedy should be available). Speed is the most important practical downside of relying on antitrust to promote interoperability. An IP regime that favors reverse engineering would afford developers immediate self-help, whereas years may pass before an antitrust remedy could be put in place. *See* Philip J. Weiser, *The Internet, Innovation, and IP Policy*, 103 COLUM. L. REV. 534, 551-52 (2003) (arguing that speed of reverse engineering self-help renders it preferable to antitrust conduct remedy).

[196] *See, e.g.*, Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d 1255, 1291 (N.D. Ala. 1998) (granting preliminary injunction requiring disclosure of technical information), *vacated on other grounds*, 195 F.3d 1346 (Fed. Cir. 1999); *see also In re* Silicon Graphics, Inc., No. 951-0064, 1995 FTC LEXIS 159, at *18-19 (Federal Trade Commission, June 13, 1995) (requiring respondent to port computer games optimized for computing platforms, and requiring publication of APIs for interoperability purposes); *In re* Xerox Corp., 86 F.T.C. 364, 373-80 (1975) (requiring licensing of patents and disclosure of related know-how). As part of a 1984 undertaking with the European Commission, IBM agreed to disclose interface information to enable hardware and software interoperability. *See* F.M. Scherer, *Microsoft and IBM in Europe*, 84 Antitrust & Trade Reg. Rep. (BNA) 65 (Jan. 23, 2003).

[197] United States v. Microsoft, 97 F. Supp. 2d 59, 67 (D.D.C. 2000) (requiring disclosure of "APIs, Communications Interfaces and Technical Information" used to enabled interoperability); *see also* United States v. Microsoft, No. 98-1232, 2006 U.S. Dist. LEXIS 76862, at *10-11 (D.D.C. Sept. 7, 2007) (Modified Final Judgment); United States v. Microsoft, 231 F. Supp. 2d 144, 186-95 (D.D.C. 2002) (approving settlement agreement containing provisions for mandatory disclosure of interoperability information).

[198] Commission Decision, COMP/C-3/37.792, Art. 5(a) (Mar. 24, 2004); Case T-201/04, Microsoft Corp. v. Comm'n, 2004 E.C.R. 249.

Recently, Apple emerged as the new preferred target of antitrust and competition scrutiny. In 2004, around the time Real released Harmony, French download service Virgin Mega filed a complaint under European competition law alleging that Apple abused its dominant position by refusing to license FairPlay.[199] Virgin sought mandatory disclosure of the FairPlay system in exchange for a reasonable royalty. According to Virgin, Apple leveraged its dominance in the market for portable players into the music download market by precluding interoperability by other download services, denying competitors allegedly indispensable access to the iPod. The French Competition Authority ("FCA") rejected Virgin's argument, noting that the market for portable players was competitive and that only a small percentage of downloaded music was transferred to such devices.[200] Perhaps more importantly, the FCA pointed out that customers could easily convert TPM-restricted files purchased from Virgin to an iPod-compatible format by burning them to CD, and then importing those CDs using iTunes.[201]

Because existing competition law did not prohibit Apple's refusal to share its FairPlay technology, the French Parliament pursued a legislative effort to ensure iPod interoperability. In 2006, France enacted the *loi relative au Driot d'Auteur et aux Droits Voisins dans la Societe de l'Information* ("Dadvsi") to implement the European Copyright Directive and, by extension, the WIPO Copyright Treaty.[202] Although Dadvsi created DMCA-like prohibitions against the circumvention of effective TPMs, it also required TPM providers to disclose information, including technical documentation and program interfaces, to developers of interoperable products.[203] Dadvsi also

[199] For a detailed discussion, see generally Giuseppe Mazziotti, *Did Apple's Refusal to License Proprietary Information Enabling Interoperability with its iPod Music Player Constitute an Abuse Under Article 82 of the EC Treaty?*, BERKELEY CTR. FOR LAW & TECH. 2005, http://works.bepress.com/mazziotti/1 (discussing 2004 French Competition Authority decision regarding Apple's refusal to license proprietary technology and risks of compulsory licensing to incentive model of IP rights).

[200] *See* Conseil de la Concurrence, Decision No. 04-D-54, at 17-18 (Nov. 9, 2004), *available at* http://www.conseil-concurrence.fr/pdf/avis/04d54.pdf.

[201] *Id.* at 14.

[202] Law No. 2006-961 of Aug. 1, 2006, *available at* http://droit.org/jo/20060803/MCCX0300082L.html [hereinafter *Dadvsi*] (Law on Copyright and Neighboring Rights in the Information Society). For a discussion of the debate leading to the enactment of Dadvsi, see generally Deana Sobel, Note, *A Bite out of Apple? iTunes, Interoperability, and France's Dadvsi Law,* 22 BERKELEY TECH. L.J. 267 (2007) (discussing Dadvsi, its attempt to reconcile IP rights with consumer rights, and government regulation of interoperability).

[203] Code de la Propriete Intellectuelle, Article L. 331-5 and 331-7, *available at*

created the Regulatory Authority for Technical Measures to hear disputes over TPM interoperability, thus bypassing the FCA, which had endorsed Apple's DRM strategy.[204]

Apple dubbed the interoperability provisions of Dadvsi "state sponsored piracy."[205] But France was not alone in its efforts to increase interoperability between iPods and competing music services. The Dutch Consumer Ombudsman filed a complaint with competition authorities.[206] And the Norwegian Ombudsman found that iTunes imposed unreasonable terms and conditions on users, in part because of the absence of interoperability with other offerings.[207] Denmark, Finland, Germany, and Sweden also threatened action over Apple's restriction of interoperability.[208]

In the U.S., antitrust authorities have proven more sanguine about Apple's DRM strategy. At the height of European scrutiny, Thomas Barnett, Assistant Attorney General in the Antitrust Division of the Department of Justice, expressed skepticism about the role of antitrust enforcement in promoting interoperability between Apple's offerings and those of its competitors.[209] Although U.S. antitrust authorities have declined to pursue enforcement actions against Apple, private plaintiffs have not. Two pending class action complaints allege that Apple's refusal to license its FairPlay DRM technology and its

http://www.celog.fr/cpi/. Publication of the source code of an interoperable product is prohibited if it would "seriously undermine the security and effectiveness" of the TPM, creating potential difficulties for developers of open source software that interacts with TPM-restricted content. *Id.*

[204] *See* Dadvsi, *supra* note 202, at art. 14.

[205] *See* Michael Geist, *The Legal Limits of Government Tinkering With Technology*, Apr. 17, 2006, http://www.michaelgeist.ca/index.php?option=com_content&task=view&id=1211.

[206] *See* Jan Libbenga, *Dutch Consumer Chief Puts Apple Through the Mill*, THE REGISTER, Jan. 25, 2007, http://www.theregister.co.uk/2007/01/25/dutch_out_of_tune_with_apple/.

[207] Letter from Norwegian Consumer Ombudsman to iTunes at 8-10 (May 30, 2006), www.forbrukerombudet.no/asset/2406/1/2406_1.pdf.

[208] *See* Tom Braithewaite & Kevin Allison, *Crunch Time for Apple's Music Icon*, FIN. TIMES, June 13, 2006, http://www.ft.com/cms/s/2/21682106-faff-11da-b4d0-0000779e2340.html; Forbrukerombudet, *European Consumer Organisations Join Forces in Legal Dispute over iTunes Music Store*, Jan. 22, 2007, http://www.forbrukerombudet.no/index.gan?id=11037079&subid=0. But European regulators were placated by Apple's decision to sell music without TPM restrictions, capable of playback on a wide variety of portable players. *See* Forbrukerombudet, *Interesting Signals from Apple Regarding iTunes*, Feb. 8, 2007, http://www.forbrukerombudet.no/index.gan?id=11037506.

[209] *See* Thomas O. Barnett, Address at the George Mason University School of Law Symposium: Interoperability Between Antitrust and IP 9-14 (Sept. 13, 2006), *available at* http://www.usdoj.gov/atr/public/speeches/218316.pdf.

unwillingness to support competing DRM systems constitute anticompetitive conduct.[210] As discussed below however, there are good reasons to doubt whether antitrust provides a reliable tool for counteracting the DMCA's restriction of interoperability.

### *B. Questioning the Sufficiency of Antitrust Theories*

Firms that rely on the legal enforcement of technological restrictions to suppress interoperability face potential antitrust claims based on three theories: tying, essential facilities, or refusal to deal. As discussed below however, all three of these theories face significant hurdles that call into question their ability to counteract consistently the power over interoperability conferred by the DMCA.

Rather than analyze the potential application of these theories in the abstract, this subpart will consider claims arising out of Apple's allegedly anticompetitive use of its FairPlay DRM. In many respects, Apple is an attractive target for antitrust plaintiffs and an ideal test case. Apple dominates the markets for both portable media players and licensed music downloads — commanding market shares above seventy percent in both sectors.[211] Even assuming, however, that Apple has market power, it is far from clear that its DRM strategy violates U.S. antitrust law.

#### 1. Tying

A tying arrangement is "an agreement by a party to sell one product but only on the condition that the buyer also purchases a different (or tied) product, or at least agrees that he will not purchase that product from any other supplier."[212] A per se tying claim requires proof of a tie between two separate products offered by a defendant with sufficient

[210] Tucker v. Apple, 493 F. Supp. 2d 1090, 1102 (N.D. Cal. 2006); Slattery v. Apple, No. 05-0037, 2005 WL 2204981, at *1-2 (N.D. Cal. Sept. 9, 2005). The antitrust complaints lodged against Apple have targeted a number of its business practices, only some of which implicate the DMCA. Apple's decision, for example, to disable support for Microsoft's WMA format, while potentially relevant to an antitrust inquiry, is not an exercise of any power Apple wields as a result of the protections afforded by the DMCA.

[211] See Beleaguered Creative Reports Loss; Seeks to Boost Sales with Apple iPod Accessories, MACDAILYNEWS, May 2, 2007, http://www.macdailynews.com/index.php/weblog/comments/13492; Rhapsody to Challenge Apple's iTunes with MP3 Download Service, MAIL ONLINE, June 30, 2008, http://www.dailymail.co.uk/sciencetech/article-1030486/Rhapsody-challenge-Apples-iTunes-MP3-download-service.html.

[212] Eastman Kodak Co. v. Image Tech. Servs. Inc., 504 U.S. 451, 461-62 (1992) (quoting N. Pac. R.R. Co. v. United States, 365 U.S. 1, 5-6 (1958)).

economic power in the tying product market to affect a substantial volume of commerce anticompetitively in the tied market.[213]

Apple faces two potential tying claims: first, that it forces iPod customers to purchase digital music from iTunes; second, that iTunes customers are required to purchase an iPod to playback digital media. Neither of these scenarios presents a tying arrangement in the classical sense. Apple does not condition the sale of either product, explicitly or implicitly, on the sale of the other. A customer who wants to buy an iPod without ever spending a dollar at the iTunes store can do so. Likewise, customers are free to purchase music from iTunes without buying an iPod.

But the fact that the two products can be purchased independently is, in itself, insufficient to overcome a tying claim.[214] Tying can occur if a customer purchases the tied product in response to some illegitimate use of the leverage acquired through the seller's power over the tying product. Here, the theory goes, customers are free to buy either half of the iPod/iTunes combination without the other, but those who do so are denied the full value of their purchases. Customers who buy an iPod, but refuse to use iTunes, are unable to play licensed downloads on their device. Further, customers cannot play music purchased from the iTunes store on a portable device that is not an iPod. As a result, Apple "refuses to accommodate those who prefer one without the other."[215]

Both of these tying theories are factually flawed. The notion that using the iPod to play licensed downloads requires customers to purchase content from the iTunes store is belied by the available alternatives. Setting aside the fact that the vast majority of music on iPods originates from either existing CD collections or illicit downloads, a variety of licensed download services are compatible with the iPod. eMusic, founded in 1998, is the second largest digital music retailer and exclusively sells DRM-free mp3 files.[216] Although eMusic's four million-track library focuses on independent labels,[217] retailers including Amazon, Real, Napster, and Walmart offer DRM-free downloads from both independent and major labels.[218]

---

[213] *See id.* at 462.

[214] *See id.*

[215] Phillip E. Areeda & Herbert Hovenkamp, FUNDAMENTALS OF ANTITRUST LAW § 17.01i (3d ed. 2006).

[216] *See* About eMusic, http://www.emusic.com/about/index.html (last visited Mar. 17, 2009).

[217] *See id.*

[218] *See* Kenneth Corbin, *Rhapsody Bets DRM-Free Downloads Can Foil iTunes*,

Similarly, the claim that Apple forces iTunes customers to buy an iPod to make use of purchased digital content overstates the case. Customers are, of course, free to listen to purchased content using a Windows or Mac computer. But even restricting the inquiry to use on a portable player, iTunes customers can easily and legally convert FairPlay-protected tracks to DRM-free mp3 files.[219] Recently, in response to European critics and customers, Apple has replaced nearly all of the Fairplay-restricted music in the iTunes catalog with DRM-free files that consumers can play on a host of portable devices.[220]

The ability to play iTunes tracks on other devices not only undermines the notion of a tie between iTunes and the iPod, but also figures in the analysis of the essential facilities doctrine discussed below.

2. Essential Facilities

Another line of attack against Apple's tight control over interoperability characterizes access to the iPod and iTunes store as competitive necessities for rivals. A monopolist that refuses a competitor feasible access to an essential facility that cannot be reasonably duplicated faces liability under § 2 of the Sherman Act.[221] Although the essential facilities doctrine developed out of early Supreme Court precedent,[222] the Court has recently cast doubt on its vitality.[223] Some commentators have called for the doctrine's

INTERNETNEWS.COM, June 30, 2008, http://www.internetnews.com/ec-news/article.php/3756246.

[219] The process of burning a CD copy and then importing that CD does impose some degree of inconvenience and may result in some discernible loss of audio quality.

[220] *See* Apple.com, *Changes Coming to the iTunes Store* (Jan. 6, 2009), http://www.apple.com/pr/library/2009/01/06itunes.html. Television programs, music videos, and motion pictures available through iTunes, however, still rely on FairPlay, as do iPhone applications.

[221] *See* Alaska Airlines, Inc. v. United Airlines, Inc., 948 F.2d 536, 542 (9th Cir. 1991) ("[T]he essential facilities doctrine imposes liability when one firm, which controls an essential facility, denies a second firm reasonable access to a product or service that the second firm must obtain in order to compete with the first."); MCI Commc'ns Corp. v. Am. Tel. & Tel. Co., 708 F.2d 1081, 1132-33 (7th Cir. 1982) (citing Otter Tail Power Co. v. United States, 410 U.S. 366 (1973)).

[222] *See* Otter Tail Power Co. v. United States, 410 U.S. 366, 377 (1973); United States v. Terminal R.R. Ass'n, 224 U.S. 383, 394-95 (1912).

[223] *See* Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 410-11 (2004) (suggesting that Court has never recognized essential facilities doctrine).

abandonment,[224] and even some of its supporters caution against applying it to IP.[225]

Assuming the doctrine represents a distinct monopolization theory — as most lower courts do — and that Apple has monopoly power in the relevant markets,[226] potential plaintiffs must first identify the essential facility to which Apple controls access. Music retailers would maintain that access to the iPod is essential for their viability, while device manufacturers would insist that access to the iTunes store is necessary for any competitive offering. Access to both of these putative essential facilities is controlled, at least in part, by FairPlay. A music retailer who wants maximum iPod interoperability can rely on no TPM other than FairPlay. Similarly, manufacturers who want their devices to play the entire iTunes catalog must be able to decrypt FairPlay-protected tracks. Because Apple has refused to license FairPlay these facilities have been off limits to its competitors.[227]

An "indispensable requirement" of a monopolization claim premised on an essential facilities theory is the unavailability of access to that facility.[228] Here that element appears to be lacking. Online music retailers — including Apple's chief rivals — have managed to gain access to the iPod by selling DRM-free music. Although major record labels refused to distribute their works without TPM restrictions in the past, they have relented, perhaps in part in response to studies demonstrating that protected content is equally vulnerable to widespread infringement.[229] Moreover, because Apple itself sells much of its catalog in an unrestricted format, devices other than the iPod can play iTunes content. Likewise, to the extent Amazon, Napster, and others offer extensive catalogs of DRM-free content at competitive

---

[224] *See* Areeda, *supra* note 195, at 841. *But see* Brett Frischmann & Spencer Weber Waller, *Revitalizing Essential Facilities*, 75 ANTITRUST L.J. 1, 3-5 (2008).

[225] *See* Abbot B. Lipsky & J. Gregory Sidak, *Essential Facilities*, 51 STAN. L. REV. 1187, 1218-19 (1999).

[226] *See* United States v. Grinnell Corp., 384 U.S. 563, 571 (1966) (holding 87% market share was monopoly); Am. Tobacco Co. v. United States, 328 U.S. 781, 797 (1946) (holding that more than two thirds of market established monopoly).

[227] Before the introduction of Apple's iPhone, which combines the feature set of a smart phone with an iPod, Apple licensed Motorola's ROKR, a cellular phone that supported playback of FairPlay-protected iTunes tracks. *See* Apple.com, *Motorola & Cingular Launch World's First Mobile Phone with iTunes* (Sept. 7, 2005), http://www.apple.com/pr/library/2005/sep/07rokr.html.

[228] *Trinko*, 540 U.S. at 411 ("[W]here access exists, the doctrine serves no purpose.").

[229] *See* Tim Anderson, *How Apple Is Changing DRM*, GUARDIAN, May 15, 2008, at 1, *available at* http://www.guardian.co.uk/technology/2008/may/15/drm.apple (reporting claim that FairPlay has no effect on infringement).

prices, there is little reason to suspect that device manufacturers are truly dependent on access to iTunes. Without evidence that access to a distribution platform or device serves as a competitive necessity or that access to such a facility is indeed denied, attacks on exclusive DRM systems premised on the essential facilities doctrine are unlikely to succeed.

3. Refusal to Deal

A monopolization claim could also be premised on refusal to deal grounds. Under this theory, Apple's consistent refusal to license Fairplay to competing device manufacturers and download services constitutes anticompetitive conduct.[230] Courts, however, are generally reluctant to interfere with the long-recognized right to refuse unilaterally to deal with competitors.[231] Forced sharing of

[230] Apple's refusal to license FairPlay and the resulting tight integration of the iPod and iTunes could serve a number of procompetitive purposes. Apple's agreements with the record labels require it to correct any compromise of the FairPlay system within "a small number of weeks . . . or they can withdraw their entire music catalog from [the] iTunes store." Steve Jobs, *Thoughts on Music* (Feb. 6, 2007), http://www.apple.com/hotnews/thoughtsonmusic. Apple maintains that the likelihood of breaches and the difficulty of rectifying them would increase if it disclosed its technology to licensees. As a result, "Apple has concluded that if it licenses FairPlay to others, it can no longer guarantee to protect the music it licenses from the big four music companies." *Id.*

Another justification for tight integration is a desire to provide a consistent and seamless end-user experience. Much of the appeal of Apple products stems from their ease of use and reliability, features Apple believes are dependent on vertical integration. *See* LEANDER KAHNEY, INSIDE STEVE'S BRAIN 12 (2008) ("[The] desire to craft complete customer experiences ensures Apple controls the hardware, the software, online services, and everything else. But it produces products that work seamlessly together and infrequently break down."). Apple's success, while due in part to industrial design and marketing, depends on the perception that its products "just work." *See* Julio Ojeda-Zapata, *Verizon's Chocolate Phone Isn't as Sweet as an iPod*, ST. PAUL PIONEER PRESS, Aug. 21, 2006, at 1D ("Apple's hot-selling music players are popular because they're so glitch-free and easy to use. They just work."); Jason Snell, *Inside Apple TV: What We Know and What's New Since Last Year's Announcement*, MACWORLD, Mar. 1, 2007 (discussing "'it just works' simplicity we've come to expect from Apple"). The refusal to license its Mac OS to other manufacturers reflects in part Apple's effort to control the user experience by defining hardware configurations. Likewise, "had Apple opened its iTunes-iPod juggernaut to outside developers, the company would have risked turning its uniquely integrated service into a hodgepodge of independent applications." Leander Kahney, *Evil Genius*, WIRED, Apr. 2008, at 138, *available at* http://www.wired.com/techbiz/it/magazine/16-04/bz_apple.

[231] United States v. Colgate & Co., 250 U.S. 300, 307 (1919) (explaining that Sherman Act "does not restrict the long recognized right of [a] trader or manufacturer engaged in an entirely private business, freely to exercise his own independent

competitively valuable assets may lessen incentives for investment and could lead to collusion among competitors.[232] Mandatory licensing of IP rights presents additional difficulties. The power to exclude is the core of the IP grant, so antitrust enforcement that denies a rights holder the ability to exclude competitors is in tension with the IP grant itself.[233] As a result, antitrust interferes with enforcement of IP rights or unilateral refusals to license only under narrowly defined circumstances.[234]

Courts have taken two approaches with respect to the refusal to license IP rights. Both approaches endorse the general principle that rights holders are free to refuse to license competitors. Some courts have held that such refusals are legal per se.[235] Others have imposed a rebuttable presumption of legality.[236] However, IP rights obtained by fraud or that are the subject of sham enforcement efforts are the proper focus of antitrust scrutiny.[237] Antitrust scrutiny is likewise appropriate when rights holders rely on IP grants to "facilitate monopolization that extends beyond the scope of the intellectual property right itself."[238]

This framework raises two questions when applied to Apple's alleged reliance on the DMCA to monopolize the portable player and digital download markets. First, do the protections the DMCA extends to copyright holders, TPM developers, and their licensees establish IP rights that fall within this framework? If so, does Apple's refusal to license FairPlay exceed the scope of its statutory rights?

---

discretion as to parties with whom he will deal").

[232] *See Trinko,* 540 U.S. at 407-08 ("Compelling . . . firms to share the source of their advantage is in some tension with the underlying purpose of antitrust law . . . .").

[233] *See* Herbert Hovenkamp et al., *Unilateral Refusals to License in the U.S.*, *in* ANTITRUST, PATENTS AND COPYRIGHT: EU AND US PERSPECTIVES 12, 15-16 (François Lévêque & Howard Shelanski eds., 2005).

[234] Courts have held that firms that terminate existing profitable courses of dealing are subject to antitrust scrutiny. *See* Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585, 603-05 (1985). But no court has yet applied that rationale to a refusal to license IP rights. *See* Hovenkamp et al., *supra* note 233, at 34.

[235] *See In re* Indep. Serv. Orgs. Antitrust Litig., 203 F.3d 1322, 1325 (Fed. Cir. 2000); *see also* Intergraph Corp. v. Intel Corp., 88 F. Supp. 2d 1288, 1293 (N.D. Ala. 2000); Telecomm Tech. Servs. v. Siemens Rolm Commc'ns, Inc., 150 F. Supp. 2d 1365, 1369 (N.D. Ga. 2000).

[236] *See* Image Technical Servs., Inc. v. Eastman Kodak Co., 125 F.3d 1195, 1218 (9th Cir. 1997); Data Gen. Corp. v. Grumman Sys. Support Corp., 36 F.3d 1147, 1186 (1st Cir. 1994).

[237] *See* Walker Process Equip., Inc. v. Food Mach. Corp., 382 U.S. 172, 176-77 (1965).

[238] Hovenkamp et al., *supra* note 233, at 27.

The DMCA, which Congress enacted under its commerce authority rather than its patent and copyright power, does not confer IP rights in the strictest sense of that term. Nevertheless, it grants powers to exclude others from the use of technologies and content sufficiently similar to traditional IP rights to suggest that the typical antitrust treatment of IP rights should inform analysis of the DMCA.[239]

The scope of the rights conferred by the DMCA is ambiguous. *Chamberlain* and *Lexmark* suggest that the use of TPMs to restrict interoperability and reduce competition in ancillary markets may fall beyond the legitimate scope of those rights. But the holdings in those cases were not explicitly premised on interference with interoperability and hinged, in part, on skepticism regarding the underlying copyright interests at stake.[240] Few courts would doubt that FairPlay protects fully copyrightable expression from a genuine threat of unauthorized access. In addition, the narrow drafting of § 1201(f) suggests that Congress did not intend to exclude all interference with interoperable offerings. In the end, interference with interoperability, standing alone, is unlikely to place DMCA enforcement efforts beyond the statute's legitimate scope. Ultimately, because antitrust is unable to define the legitimate scope of the DMCA independently, it must defer to the rights Congress created.

### *C. Deferring to the Scope of IP Rights*

Antitrust typically defers to valid exercises of legitimately acquired IP rights. Without this degree of deference, antitrust would risk direct conflict with IP doctrine because the rights to exclude that IP provides with one hand, antitrust could take away with the other. This deference acknowledges that antitrust law is not well positioned to second-guess the scope of IP grants established through the legislative process.[241] As one commentator explained, "courts cannot and should not try to use the antitrust laws to reign [sic] in what may appear to a

[239] *But see* Chamberlain v. Skylink, 381 F.3d 1178, 1203 (Fed. Cir. 2004) ("Congress chose to create new causes of action for circumvention and for trafficking in circumvention devices. Congress did not choose to create new property rights.").

[240] *See id.* (noting that Chamberlain did not bring a claim for copyright infringement); Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 541 & 548 (6th Cir. 2004) (describing PEP as "purely functional" and rejecting district court's determination that Lexmark's Toner Loading Program was sufficiently original to support preliminary injunction).

[241] *See* Hovenkamp, *supra* note 233, at 23-24 ("[A]ntitrust laws were not designed to repair other government regulatory process, but rather to take these processes as given and strive to further competition consistent with their mandates.").

judge to be excessive congressional grants of economic power through the intellectual property laws."[242]

This deference, however, does not mean that IP rights are altogether unchecked. Patent and copyright have developed internal mechanisms for defining the legitimate scope of the rights they confer. Aside from generally applicable limitations on the scope and length of exclusive rights, patent and copyright law rely on their respective misuse doctrines to limit the extent to which rights holders can leverage their rights to gain control that exceeds the statutory grant.[243] Although the precise relationship between antitrust and misuse has varied over time, the doctrines are closely related and serve a similar function — to restrain uses of IP rights that extend beyond the limits Congress defined.[244]

The extent to which antitrust can target potentially anticompetitive exercises of IP rights depends largely on how Congress has crafted, and the courts have interpreted, those rights. When IP rights are over-broad, the first line of defense should be narrowing the scope of those rights, not imposing an additional layer of regulation through antitrust enforcement. Rather than grant an expansive right, await abuse, and then rely on antitrust to serve as a corrective, IP policy must recognize its obligation to circumscribe carefully the legitimate bounds of the rights it confers to avoid harms to competition and innovation.[245]

Two cases decided by the European Court of Justice demonstrate the importance of both deference to IP rights and the resulting duty of IP doctrine to define the limits of its exclusive rights appropriately. *Radio Telefis Eireann v. Commission of the European Communities*, more commonly referred to as the *Magill* case, arose when three Irish television broadcasters obtained an injunction against Magill's publication of a weekly listing of their programming schedules. Irish

---

[242] David McGowan, *Innovation, Uncertainty, and Stability in Antitrust Law*, 16 BERKELEY TECH. L. J. 729, 780 (2001).

[243] *See* Burk, *supra* note 68, at 571. In both the patent and copyright contexts, misuse is an equitable doctrine that prevents the enforcement of IP rights when a rights holder attempts to extend the scope of its statutory grant improperly. *See* Lasercomb Am., Inc. v Reynolds, 911 F.2d 970, 973 (4th Cir. 1990).

[244] *See* Mark A. Lemley, *A New Balance Between IP and Antitrust*, 13 SW. J. L. & TRADE AM. 237, 255 (2007).

[245] *See* Jonathan Zittrain, *The Un-Microsoft Un-Remedy: Law Can Prevent the Problem That It Can't Patch Later*, 31 CONN. L. REV. 1361, 1363 (1999) (arguing with respect to potential remedies in Microsoft antitrust litigation that "the key may rest in giving [copyright holders] less of a monopoly to begin with, rather than waiting for the exploitation of that monopoly to take shape, have effect, and then land a market leader in court for antitrust violations").

copyright law provided the broadcasters exclusive rights in their program listings, and each published its own weekly programming guide.[246] Because the injunction prevented Magill from competing with these existing weekly listings, it brought a complaint alleging violation of European competition law. Confirming two lower decisions, the European Court of Justice was satisfied that the broadcasters abused their dominant position in refusing to license weekly listings to Magill.[247]

Similarly, *IMS Health v. NDC Health* addressed a refusal by IMS to license its "1860 brick structure" — a system for reporting German pharmaceutical sales data — to its competitor NDC.[248] After years of use and promotion by IMS, the 1860 brick emerged as the industry standard for packaging data for drug companies, accounting firms, and insurance providers.[249] When NDC's predecessor adopted the 1860 brick to distribute its own independently generated data, IMS sued for infringement. After IMS obtained an injunction barring NDC from using the 1860 brick, NDC attempted to obtain a license to use the system. IMS refused, prompting NDC to complain that IMS abused its dominant position. The European Court of Justice, consistent with an earlier Commission decision requiring IMS to license the 1860 brick structure, ruled that the case, like *Magill*, presented "exceptional circumstances" that justified mandatory licensing of an IP right as a matter of competition law.[250]

The European approach to the relationship between IP and competition law differs in important respects from the deference typical in the United States. Rather than leaving the determination of the proper bounds of exclusive rights to the appropriate IP doctrines, European competition law scrutinizes IP rights directly. In large part, this approach stems from the fact that competition law is a product of the European Economic Community Treaty, while individual member states determine the scope of IP rights.[251] Reconciliation of national IP regimes with the broader goals of "the free movement of goods" requires occasional subservience of IP rights to competition principles.[252]

---

[246] *See* BBC v. Magill, [1990] I.L.R.M. 534, 541-42 (Ir.).

[247] Case 241/91P, Radio Telefis Eireann v. Comm'n of the European Cmty., 1995 E.C.R. I-743, ¶ 1.

[248] IMS Health v. NDC Health, [2004] 4 C.M.L.R. 28, at 1549-50.

[249] *Id.* at 1550.

[250] *Id.* at 1578-79, 1582.

[251] *See Radio Telefis Eireann*, E.C.R. 337 at ¶¶ 2-4.

[252] *See id.*

Putting aside the differences between the U.S. and E.U. treatment of IP and competition law, *IMS* and *Magill* teach two lessons. First, antitrust enforcement can create uncertainty and inefficiency if courts are free to reconsider existing IP rules. If IP doctrine alone does not settle the question of the proper scope of IP rights, the threat of antitrust challenges could result in a lack of clarity that lessens incentives for innovation and creativity. As these cases demonstrate, the acquisition and litigation of IP rights are insufficient to adjudicate an infringement claim when antitrust enforcement enjoys the latitude to enforce standards inconsistent with IP doctrine.

Perhaps more importantly, *Magill* and *IMS* illustrate what happens when IP grants fail to account adequately for their potential competitive impact. Although deference ensures greater clarity and more efficient adjudication, IP doctrine must keep up its end of the bargain by carefully crafting grants of exclusive rights. There are good reasons to doubt the wisdom of the copyright claims endorsed in the disputes that underlie *Magill* and *IMS*. Certainly both would be suspect under U.S. law. The Irish decision permitting exclusive rights in programming schedules provided exclusive rights in facts, a grant fundamentally inconsistent with U.S. law.[253] Likewise, U.S. law would protect the 1860 brick structure, if at all, by patent.[254] Had the relevant IP rights not afforded such sweeping protections, neither Magill nor NDC would have found themselves in the unenviable position of seeking licenses, let alone pursuing competition claims for the right to obtain them. Ultimately, *Magill* and *IMS* reflect the impact of a failure to tailor IP rights appropriately.[255]

Limits on IP rights, however, do more than avoid conflicts with antitrust law. The primary function of IP protection is to create incentives for the creation and dissemination of new works. Even in fully competitive markets, the scope of IP rights can be adjusted to better serve the instrumental goal of incentivizing new works and the ultimate end of promoting the progress of science and the useful arts. If responsibility for determining the outer limits of IP enforcement is left to antitrust, only behavior that threatens competition will be prohibited, blunting the ability to fine tune IP policy.

---

[253] *See* Feist Publ'n, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 347 (1991).

[254] Even if the brick were considered copyrightable subject matter, the external constraints facing developers of alternate systems would likely limit the scope of any potential copyright protection.

[255] *See* Kenneth Glazer, *The* IMS Health *Case: A U.S. Perspective*, 13. GEO. MASON L. REV. 1197, 1198 (2006) ("If the [IMS] copyright was questionable, that could (and should) have been handled by the copyright system directly.").

Imagine ten competitors that each offer integrated, noninteroperable systems for the purchase and playback of TPM-restricted digital music downloads. Rather than a market dominated by the iPod and iTunes, assume these ten firms controlled roughly equal-sized shares of the device and download markets. In the absence of some concerted action, no threat to competition would exist. Nonetheless, the power to prevent interoperable services still raises important questions for IP policy. From the patent perspective, would more innovation occur under a system that offers stronger incentives by limiting interoperability? Or would greater room for new entrants ultimately lead to more valuable incremental innovation? From the copyright and DMCA perspective, would noninteroperability encourage greater participation by copyright holders in digital marketplaces? Or would interoperability yield broader dissemination of copyrighted works? Regardless of the answer to these questions, they should be analyzed as matters of IP policy, rather than through the narrower lens of antitrust. As the next Part discusses, legislative change to the DMCA offers a preferable means of addressing its impact on interoperability.

## IV. RECONCILING ANTICIRCUMVENTION & INTEROPERABILITY

The DMCA's restriction of otherwise permissible uses of copyrighted works, including efforts to achieve interoperability, has prompted a variety of proposals. Dan Burk has argued that anticircumvention law requires its own doctrine of misuse, drawing on analogous patent and copyright doctrines, to address efforts to leverage the rights provided by the DMCA.[256] Timothy Armstrong has suggested that courts should more readily draw on fair use principles to create a body of judge-made fair circumvention law.[257] Jerome Reichman, Graeme Dinwoodie, and Pamela Samuelson have proposed a reverse notice and takedown regime under which rights holders would be obligated to remove TPM restrictions after user notification of a desire to make lawful uses of TPM-protected works.[258] Each of these proposals has substantial merit and would help address the many unintended consequences of the DMCA. However, none of

[256] Burk, *supra* note 68, at 571-72.

[257] Timothy K. Armstrong, *Fair Circumvention*, 74 BROOK. L. REV. 1, 43-48 (2008).

[258] Jerome H. Reichman et al., *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981, 985 (2007); *see also* Jacqueline D. Lipton, *Solving the Digital Piracy Puzzle: Disaggregating Fair Use from the DMCA's Anti-Device Provisions*, 19 HARV. J.L. & TECH. 111, 116 (2005) (proposing administrative mechanism to enable particular fair uses of works protected by DRM).

these proposals specifically targets the DMCA's interference with efforts to create unauthorized interoperable technologies. This Part offers a proposal that addresses that narrower concern.[259]

Section 1201(f) reflects Congress's understanding that interoperability has value worth preserving. But the narrow text and consistent misinterpretation of § 1201(f) have greatly diminished its capacity to safeguard interoperability. Although more reasonable judicial application of § 1201(f) would increase protections for interoperability with respect to TPM-restricted computer programs, a legislative solution is necessary to enable interoperable use of digitally encoded content.

In addition to the unwarranted distinction between program and data at the heart of § 1201(f), the DMCA's impact on interoperability stems from its protection of noncopyright interests. In its effort to facilitate greater control over accessing and copying works, the DMCA reinforces both legitimate copyright holder interests and concerns entirely divorced from the statutory grant of copyright. To guard against unauthorized copying, for example, content owners can tie their works to selected secure platforms. But this same tethering, and its legal enforcement under the DMCA, can be used to prevent interoperability for reasons unrelated to concerns over infringement.

Two changes are necessary to preserve the value Congress intended the DMCA to offer copyright holders while making room for interoperability. First, the exclusive focus of § 1201(f) on computer programs must be abandoned in favor of an exemption that applies to all classes of copyrighted works. Such a change would recognize the role data plays in enabling system-level interoperability. Second, legitimate copyright interests must be disaggregated from the control over distribution and playback technologies that impedes interoperability.[260] The nexus requirement articulated by the Federal

[259] Others have offered limited proposals that address the DMCA's restriction of interoperability in the durable goods context. *See* Jacqueline Lipton, *The Law of Unintended Consequences: The Digital Millennium Copyright Act and Interoperability*, 62 WASH. & LEE L. REV. 487, 490 (2005) (proposing legislative limitation on application of DMCA in cases involving replacement parts for durable goods that incorporate software code). The proposal outlined here, because it addresses the role of data interoperability, envisions a more comprehensive response.

[260] Limiting the ability of TPM providers to sue under the DMCA offers one rough means of separating legitimate copyright interests from efforts to restrict interoperability. *See* 17 U.S.C. § 1203(a) (2006) (providing remedy to "[a]ny person injured by a violation of section 1201"). As the debate over Real's Harmony demonstrated, copyright holders may not object to all alleged circumvention. *See* Borland, *supra* note 182.

Circuit in *Chamberlain* reflects this need to separate copyright and noncopyright interests in applying the anticircumvention provisions. But there is a risk that future courts will feel more constrained by the exceedingly detailed statutory framework of the DMCA and thus less inclined to engage in the common law reasoning that gave rise to the *Chamberlain* decision. The solution offered here provides an unambiguous statutory basis for drawing such distinctions.

The disaggregation of control over copyrighted works from control over interoperable technologies addresses the chief difficulty in expanding § 1201(f). Because the anticircumvention provisions restrict technologies that interact with TPM-restricted works, a broad § 1201(f) could prove the exception that swallows the rule. The liability provisions of § 1201 could be stripped of practical effect if measures protecting copyrighted works could be circumvented to achieve interoperability with any device or program without further constraints. Suppose a user wants to render a FairPlay-protected iTunes track interoperable with a program capable of playing only DRM-free mp3 files. An unqualified right to achieve interoperability would entitle the user to avoid not only those restrictions that tie the track to the iPod, but also other substantive limitations on the rights acquired by the user.[261] Such limitations are not necessarily inconsistent with meaningful interoperability. To the extent restrictions intended to effectuate legitimate copyright interests can be untangled from those meant to enable control over playback and distribution technologies, interoperability can be reconciled with the increased control over the copyrighted material that Congress intended to bolster.

The current § 1201(f) contains some limited assurances against legitimate copyright holder interests being sacrificed in the name of interoperability. The statute, for example, requires potential

But this approach is both over- and under-inclusive. The class of copyright holders includes device manufacturers, like Lexmark and Chamberlain, keen on limiting interoperability. And financial ties between copyright holders, device manufacturers, and TPM providers contribute to a potential overlap of interests. *See* Jeff Leeds, *Microsoft Strikes Deal for Music*, N.Y. TIMES, Nov. 9, 2006, at C1 (describing Microsoft's agreement to pay Universal royalty for each Zune sold). Equally importantly, there may be good reasons to allow TPM providers redress under the DMCA. In trafficking cases, evidence of specific acts of circumvention may be lacking, leaving TPM providers better positioned and more motivated to pursue § 1201 claims.

[261] Such limitations could include caps on the number of computers authorized to play a track or the number of times a playlist can be burned to a CD. They could also extend to restrictions on the period of time during which access is authorized in the case of subscription or rental services.

circumventors to obtain a copy of a work lawfully, guaranteeing that only those who purchase, rent, or otherwise furnish some consideration in exchange for access are entitled to engage in circumvention.[262] However, that requirement alone is insufficient because it does not secure against unauthorized postsale copying, distribution, and access enabled in the name of interoperability.

Persistent access controls — TPMs that continue to restrict access after a user gains initial authorized access — are a controversial component of the DMCA landscape. The statute's legislative history explains that Congress did not intend § 1201 to enable copyright holders to limit postsale access to lawfully acquired copies of works.[263] Scholars have also criticized the role that persistent access controls play in restricting circumvention that may serve the public interest.[264] Nonetheless, copyright holders and TPM providers rely on such controls to restrict postsale access, and courts have expressed little hesitation about their enforcement.

Persistent access controls play a crucial role in rental-based models that rely on the ability to terminate access after a customer has acquired a fully functional copy of a work. Because users who download films from online rental services, for example, may be unwilling simply to delete those files once the rental period has expired, TPM-based mechanisms for enforcing the terms of such transactions may be desirable. Persistent access controls are also useful in fine-tuning access rights. Apple's FairPlay, for example, permits users to access protected files on up to five computers, but no more.[265] By helping copyright holders and TPM providers define the bundle of rights consumers acquire, persistent access controls may ultimately lead to competition based on the comparative value of greater or fewer restrictions. Absent judicial or congressional rejection of persistent access controls, a broadened interoperability exemption must account for the restrictions they impose.

To disaggregate the legitimate copyright interests reflected in TPMs from their potential to restrict interoperability for purposes unrelated to infringement, a revised § 1201(f) should be conditioned on

---

[262] *See* 17 U.S.C. § 1201(f)(1) (2006).

[263] H.R. REP. NO. 105-551, pt. 1, at 17-18 (1998) ("Paragraph (a)(1) does not apply to the subsequent actions of a person once he or she has obtained authorized access to a copy of a work . . . even if such actions involve circumvention . . . .").

[264] *See* Reichman et al., *supra* note 258, at 1008-09; *see also* JESSICA LITMAN, DIGITAL COPYRIGHT 83, 167, 170, 176 (2001) (noting extent to which persistent access controls restrict access to unprotected facts and ideas).

[265] Jobs, *supra* note 230.

compliance with those restrictions that do not directly implicate interoperability. Such restrictions include limits on the duration of access, instances of access, and number of copies a user is entitled to make. If interoperable developers respect such restrictions, copyright holders and TPM providers should have no power to tether works to approved software or hardware.[266]

Imagine a TPM applied to digital video rentals, which imposes two distinct restraints. First, it prevents access after the expiration of a thirty-day rental period. Second, it limits access to approved portable devices. Suppose an unapproved device manufacturer wants to interoperate with rentals protected by this TPM. To qualify for exemption under the revised § 1201(f), the manufacturer must

[266] A revised § 1201(f) that implements this approach is included below:

> (f) Interoperability.
>
> (1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a work may circumvent a technological measure that effectively controls access to that work for the sole purpose of identifying and analyzing information necessary to achieve interoperability with a computer program, if such information has not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title, and to the extent the interoperable computer program enforces any restrictions on the duration of access and the number of instances of access defined by the technological measure.
>
> (2) Notwithstanding the provisions of subsections (a)(1)(A), (a)(2), and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of a work with a computer program, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title, and to the extent the interoperable program enforces any restrictions on the duration of access, number of permitted instances of access, or number of permitted copies defined by the technological measure.
>
> (3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others solely for the purpose of enabling interoperability of a work with a computer program, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.
>
> (4) For purposes of this subsection, the term "interoperability" means the ability of a computer program and another work, including another computer program, to exchange information and use the information that has been exchanged.

enforce the thirty-day expiration date. Copyright holders would retain their power to define the scope of access, but could not dictate the playback platforms available to end users.

This proposal faces a number of potential objections from both sides of the interoperability debate. Proponents of increased freedom to interoperate will likely note that this approach does not maximize interoperability. As the major record labels have learned, interoperability is most prevalent in an environment in which TPMs are altogether absent. But while the music download market appears to be converging around a DRM-free standard, other markets are likely to retain DRM, at least in the short term. Licensed television and motion picture content, whether purchased or rented, remains subject to DRM, as does music obtained from most subscription services.[267] Where TPMs would continue to restrict access, the revised § 1201(f) would not give users the freedom to render content interoperable with any device or software they choose because such freedom would eliminate the DMCA's liability provisions altogether. Instead, the revised interoperability exemption outlined here gives developers the freedom to design products that interoperate with TPM-restricted content so long as they respect the material restrictions on access those TPMs were designed to enforce.

Even if developers have the freedom to interoperate unilaterally with TPM-protected systems, the possibility of technological interference by TPM providers could dissuade developers from investing in interoperable products. As Apple's reaction to Harmony demonstrates, TPM providers are well positioned to disrupt unwanted interoperability. A revised § 1201(f) could respond to this problem in at least two ways. First, it could do nothing. Allowing rights holders to interfere technologically with attempts to interoperate would bring anticircumvention's interoperability policy back in line with the treatment of interoperability in IP generally. Although trade secrecy, copyright, and patent all permit unilateral efforts to interoperate under appropriate circumstances, none impose obligations on rights holders to refrain from interfering with competitors' ability to interoperate.

To the extent that Congress was inclined to promote, rather than simply tolerate, unilateral interoperability, it could take a second,

---

[267] *See* Jacqui Cheng, *If Music DRM Is Dead, the RIAA Expects its Resurrection*, ARS TECHNICA, May 8, 2008, http://arstechnica.com/tech-policy/news/2008/05/if-music-drm-is-dead-the-riaa-expects-its-resurrection.ars; DefectiveByDesign.org, Apple Announces All Music on iTunes to go DRM-Free — No Word on Movies, TV Shows, Games, Audiobooks and Applications, http://www.defectivebydesign.org/itunes-drm-free (Jan. 8, 2009, 15:11 EST).

more active approach that provides disincentives against disruptive strategies. Congress could withhold the ability to bring a circumvention or trafficking claim, for example, from copyright holders or TPM providers that alter the operation of a technological measure for the primary purpose of interfering with interoperability. Such a rule might draw on the patent and copyright misuse doctrines, withholding protection until rights holders take steps to restore interoperability.[268]

Any legislative proposal addressing the adverse effects of the DMCA must also confront the low likelihood of Congress revisiting the anticircumvention provisions. Several legislative efforts, led by Representatives Boucher and Lofgren, attempted to lessen the DMCA's impact on noninfringing uses of copyrighted works, but failed to overcome the lobbying efforts of the entertainment industry.[269] Although the legislative outlook remains less than promising, there are reasons to suspect that the proposal offered here could overcome some of the difficulties facing broader reform efforts. Copyright holders feel increasingly threatened by the control TPM providers and device manufacturers like Apple wield over the pricing, distribution, and playback of digital content.[270] Increased interoperability offers one way to lessen that control without abandoning DRM altogether. Because the revised § 1201(f) separates the interests of copyright holders from those of TPM providers, it may increase competition among download services and playback devices without sacrificing the benefits of TPMs that copyright holders enjoy.

Nonetheless, copyright holders and TPM providers may object to expanding § 1201(f) for other reasons. First, they could maintain that interoperable playback devices and software, even those that faithfully adhere to limits on access and copying, could harm the long-term robustness of TPM systems, rendering them more susceptible to

[268] Proponents of interoperability would also be justified in noting that loosening the control the DMCA enables over interoperable technologies does not address all legal impediments to interoperability. End user license agreements and terms of service could continue to restrict reverse engineering and the creation of interoperable products. Likewise, patents will continue to play a role in restricting interoperability.

[269] *See* H.R. 1201, 110th Cong. (2007); H.R. 1201, 109th Cong. (2005); H.R. 107, 108th Cong. (2003); H.R. 5544, 107th Cong. (2002); H.R. 5522, 107th Cong. (2002); *see also* Calandrillo & Davison, *supra* note 19, at 383-89 (discussing unsuccessful legislative efforts to reform DMCA).

[270] *See* Jeff Leeds, *Free Song Promotion Is Expected from Amazon*, N.Y. TIMES, Jan. 14, 2008, at C1 (describing favorable treatment of Amazon's download service by record labels hoping to reduce Apple's market dominance).

circumvention. Unlicensed players may prove easier to hack, or may unintentionally expose decryption keys or other sensitive information.

The loss of control over playback technology could give rise to some potential threat to TPM robustness. If this risk were sufficient to undermine the value of TPMs generally, it could be addressed by an additional restriction on the availability of § 1201(f), one conditioned on a circumventor's reasonable steps to ensure the security of the original TPM or requiring that the resulting interoperable technology not substantially reduce the security of that TPM. But such conditions would greatly undermine the value of an expanded § 1201(f). The potential security risk posed by interoperable technology would prove a fact-intensive inquiry that would consistently extend potential litigation beyond summary judgment, imposing substantial costs on developers of interoperable technologies.

Any comparative analysis of TPM robustness would, of course, depend on the inherent security of a TPM on sanctioned playback platforms. As history demonstrates, every widely deployed DRM system has proven susceptible to circumvention, even when copyright holders and TPM providers exercised substantial control over playback technology.[271] Indeed, because all DRM systems must ultimately allow consumers some degree of access to protected content, they are inherently susceptible to attack.[272] Sometimes this susceptibility is exploited by sophisticated reverse engineers, other times by enterprising teenagers.[273] Even the most sophisticated TPMs, those termed "unbreakable" by their developers, have fared poorly in the wild.[274]

---

[271] *See generally* Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOYOLA L.A. ENT. L. REV. 635 (2004) (arguing that DMCA fails to reduce digital copyright infringement).

[272] *See* Bruce Schneier, *The Futility of Digital Copy Prevention*, CRYPTO-GRAM NEWSLETTER, May 15, 2001, http://www.schneier.com/crypto-gram-0105.html#3 ("This is the Achilles' heel of all content protection schemes based on encryption: the display device must contain the decryption key in order to work . . . . The end result will be failure. All digital copy protection schemes can be broken, and once they are, the breaks will be distributed . . . law or no law.").

[273] *See* Alex Eaton-Salners, DVD Copy Control Association v. Bunner*: Freedom of Speech and Trade Secrets*, 19 BERKELEY TECH. L.J. 269, 272 (2004) (describing involvement of teenager Jon Johansen in creation of DeCSS).

[274] *See, e.g.*, Cory Doctorow, *BluRay's BD+ DRM Broken, Boing Boing* (Mar. 21, 2008), http://www.boingboing.net/2008/03/21/blurays-bd-drm-broke.html (describing cracking of "unbreakable" BD+ protection scheme used on BluRay discs); Ed Felten, *AACS Plays Whack-a-Mole with Extracted Key* (May 1, 2007), http://www.freedom-to-tinker.com/?p=1152 (describing availability of encryption key used in AACS

The very enactment of the DMCA serves as recognition of the technological weakness of the measures that restrict access and copying of publicly available copyrighted content. Because code alone is incapable of preventing unauthorized use, legal prohibitions buttress technological controls. With or without an expanded § 1201(f), TPMs will continue to lack the robustness to restrict unauthorized use effectively in the absence of legal sanctions. Because the expanded § 1201(f) retains the legal enforcement mechanism crucial to the practical value of TPMs, any marginal decrease in their already low robustness is unlikely to offset the value of increased interoperability.

But the value of increased interoperability may raise an independent objection to an expanded § 1201(f). In some circumstances, interoperability could reduce incentives for certain innovative and competitive strategies.[275] Allowing interoperability without granular consideration of its effect on such incentives threatens to introduce uniformity costs.[276] An optimal rule, the objection goes, must separate beneficial interoperability from its harmful counterpart, otherwise any benefits to incremental innovation and static competition come at a cost to radical innovation and Schumpeterian competition.

Interoperability could be socially undesirable in two circumstances: first, if it harms copyright interests by enabling unauthorized access and copying to a degree that undermines incentives for creation and distribution; and second, if it harms incentives for competition and innovation. The first scenario is precisely the concern that motivated Congress to enact the DMCA. If the distribution platforms and playback devices used to access digital media cannot make good on their promise of technological control over user behavior, copyright owners may simply decline to invest in the creation of such content or to participate in insecure digital marketplaces. These concerns, putting aside their likelihood, would be addressed by the revised § 1201(f)'s separation of copyright and noncopyright interests. By requiring interoperable technologies to adhere to restrictions on access and copying, this statutory change would filter out those interoperable technologies most likely to harm copyright interests.

protection system employed on BluRay discs).

[275] *See supra* Part I.B.

[276] *See generally* Michael W. Carroll, *One for All: The Problem of Uniformity Cost in IP Law*, 55 AM. U.L. REV. 845 (2006) (explaining that uniform IP rights tend to provide insufficient protection to those who invest in costly innovations, while overprotecting those, who because of low innovation costs, require less incentive to innovate).

The second scenario contemplates a very different concern, one Congress never intended the DMCA to address. Without the added exclusivity provided by § 1201's restrictions on interoperable technologies, the worry goes, innovators like Apple will be less inclined to invest in developing products like the iPod.[277] Assuming that interoperability decreases incentives to a degree sufficient to reduce innovation — at best, an uncertain assumption — such incentives are beyond the goals of the DMCA and outside the scope of copyright policy generally. The DMCA's interoperability policy cannot balance all innovative and creative incentives in isolation. Instead, it should be understood as a more modest tool intended to preserve the existing incentive structures of copyright law. Moreover, it should be seen as a single component of IP's broader interoperability policy. To the extent limiting interoperability is necessary to preserve incentives for innovation, those restrictions should be, and are, defined within the patent system, not the DMCA's anticircumvention provisions. Any argument that the DMCA is necessary to spur innovation in playback technologies only reinforces the threat that § 1201 allows a back door to the more robust protections of patent law, evading its longstanding and more demanding requirements for exclusivity.

The DMCA currently affords a degree of control over interoperable technologies incongruous with the treatment of interoperability under traditional IP regimes. This control extends to any device or service incorporating a TPM that satisfies the trivial effectiveness requirement of § 1201. To limit the DMCA's broad protections, § 1201(f)'s exemption should be expanded to embrace the circumvention of TPMs protecting all classes of copyrighted works, not just computer programs. But the availability of this broadened exemption should be conditioned on a developer's adherence to other substantive restrictions on accessing and copying the underlying work. This expansion of § 1201(f) would convert the DMCA's treatment of interoperability from an aberration to a cohesive component of IP's interoperability policy. Developers would regain the freedom to create interoperable products unilaterally, but copyright holders would retain the ability to restrict access and copying even within this interoperable environment.

[277] The iPod, of course, was developed and released to overwhelming commercial success years before Apple sold a single DRM-protected song. So the need for the added exclusivity offered by the DMCA proved unnecessary to spur innovation in at least one instance.

## CONCLUSION

Congress enacted the DMCA to enable thriving online markets for copyrighted works by providing rights holders with tools to guard against unauthorized access and widespread infringement. Despite Congress's efforts, the DMCA also gave rise to broad powers over playback and distribution technologies, which interfere with IP law's longstanding tolerance of unauthorized unilateral interoperability. Ironically, this control over interoperability could hamper the further development of the very markets Congress intended the DMCA to foster. Likewise, restrictions on interoperability conflict with copyright's ultimate purpose — the dissemination and use of cultural works in the progress of science — by preventing authorized purchasers of copyrighted material from making use of those works.

Antitrust offers, at best, an imperfect means of redressing the DMCA's impact on interoperability. Not all interference with interoperability gives rise to cognizable competitive harms. In addition, the deference antitrust shows towards legitimately acquired IP rights requires rights holders to exceed the scope of their statutory grants before facing antitrust liability.

As a result, internal clarification and adjustment of the DCMA's scope offer the best hope for reestablishing the legitimacy of unauthorized interoperability. This approach recognizes the need for IP doctrine to tailor carefully the protections it offers and to take responsibility for their unintended consequences. The expansion of the § 1201(f) interoperability exemption outlined here addresses anticircumvention's impact on interoperability, but does so without ignoring the concerns over unauthorized access and copying that motivated the DMCA.

Ultimately, as copyright holders, content distributors, and device manufacturers have begun to realize, and as consumers have long understood, complete freedom to interoperate depends on the absence of technological restrictions on copyrighted works. The use of TPMs, however, will undoubtedly continue in some markets. Their legal reinforcement, however, can and should accommodate the freedom to interoperate.