RETHINKING ANTICIRCUMVENTION'S INTEROPERABILITY POLICY

Aaron K. Perzanowski[†]

Draft – September 6, 2008

Forthcoming UC DAVIS LAW REVIEW

ABSTRACT

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 a narrow textual focus on software-to-software interoperability render those safeguards largely ineffective.

Subjecting restrictions on interoperability to antitrust scrutiny, and the resulting mandatory disclosure of technical information, is one approach to holding anticircumvention law in check. But a number of considerations suggest antitrust is a poor tool for lessening the DMCA's impact on interoperability. Whether characterized as tying, denial of essential facilities, or refusal to deal, the use of anticircumvention law to impede interoperability is unlikely to consistently trigger antitrust enforcement. In part, the limits on the ability of antitrust to address the impact of the DMCA stem from its deference to the legislative process. Antitrust rarely interferes with the exercise of legitimately acquired IP rights.

Rather than relying on antitrust to limit the DMCA's restriction of interoperability, this Article proposes a solution that addresses that restriction at its source. Expanding the DMCA's existing interoperability exemption would create an environment more hospitable to interoperable technologies. But in order to preserve the protections the DMCA offers copyright holders, this expanded exemption must disaggregate restrictions on the use of interoperable software and devices from the restrictions on access and copying that Congress intended to enable. The former could be ignored only to the extent the latter are respected.

---

† 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, Fred von Lohmann, and the participants of the 2008 Intellectual Property Scholars Conference at Stanford Law School for helpful comments on earlier drafts.

INTRODUCTION

In our networked environment, questions of interoperability loom large. The ability of information, products, and services from a variety of providers to work together is often key to commercial success and an increasingly important component of consumer expectations.[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 limit interoperability accordingly.[3]

---

[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 the importance of flexible personal use to consumers).

[2] Posting of Brad Stone to Bits, http://bits.blogs.nytimes.com (June 2, 2008, 4:33 EST) (discussing Facebook Platform and Google's Open Social); 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).

[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, March 6, 2008, http://www.pcworld.com/article/143210.

The degree and character of available interoperability depends in part on law. The legal regulation of interoperability can take a range of forms that vary not only in the extent to which they favor interoperability, but also in the degree to which they intervene with private market-driven decisions. At the extremes, legal rules could either forbid or require interoperability. On the other hand, the law might reflect a non-interventionist sentiment, leaving decisions 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 to determine the circumstances under which interoperability is achieved. 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 achieve interoperability. It argues that the anticircumvention provisions of the DMCA unnecessarily inhibit interoperability and calls for a legislative solution to reconcile the legitimate interests of copyright holders with the need for increased freedom to interoperate.

Part I defines interoperability and examines its implications for innovation, competition, and accessibility. Although the impact of interoperability is not uniformly positive in every circumstance, and individual firms sometimes have strong incentives to oppose it, promoting or at least permitting interoperability is a reasonable policy objective. This conclusion is consistent with the treatment of interoperability in intellectual property law generally. The interoperability policy that emerges from trade secrecy, copyright, and patent law permits—and occasionally promotes—interoperability in most circumstances.

The DMCA's departure from this interoperability policy is addressed in Part II. In short, the DMCA prohibits acts of reverse engineering necessary to develop interoperable products and bans the distribution of technologies that interact with works protected by technological measures. To its credit, Congress recognized the DMCA's potential impact on interoperability and enacted a statutory exemption—§ 1201(f)—intended to limit its negative effects. But courts have consistently misinterpreted its 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 of the failure of the DMCA's internal safeguards to adequately protect interoperability, competitors, consumers, and regulators have increasingly turned to other legal doctrines to vindicate unauthorized interoperability. Part III describes the efforts in the United States and Europe to rely on antitrust and competition principles to limit the impact of anticircumvention law by mandating disclosure of interoperability information. This Part expresses skepticism about the role of antitrust in restraining the protections offered by the DMCA. First, taking the controversy surrounding the tight integration of Apple's iPod portable player and

iTunes download store as a useful hypothetical, there are good reasons to question the ability of standard antitrust theories to reach allegedly anticompetitive enforcement of the DMCA. Second, the deference typically afforded in antitrust analysis to legitimately acquired intellectual property rights suggests that the first response to any unwanted affects of the DMCA should be a retooling of the scope of its protections.

Part IV outlines a rethinking of the DMCA's approach to interoperability. By broadening § 1201(f), the DMCA's scope can be narrowed 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 offers an approach that disaggregates such restrictions from control over playback technologies, striking a balance between promoting interoperability and empowering copyright holders.

I. INTEROPERABILITY

This Part sets out to answer three preliminary questions about interoperability. First, what is it? Second, why is it valuable? And third, to what extent does traditional intellectual property doctrine regulate it?

To summarize, interoperability is a relationship between two or more systems by which they exchange usable information. Interoperability is valuable because, on the whole, it promotes innovation, competition, and access, each of which gives rise to more concrete benefits for consumers and society generally. Partly in recognition of these benefits, intellectual property law has largely avoided any direct regulation of unauthorized efforts to achieve interoperability, leaving market forces to determine whether such efforts are pursued. Some intellectual property rules, most notably copyright's favored treatment of reverse engineering, represent explicit efforts to promote interoperability. And IP directly interferes with efforts to interoperate only under limited circumstances.

A. Defining Interoperability

Interoperability is the ability of a system to work in conjunction or otherwise interact with another system.[4] With respect to information and communication technologies, interoperability takes on a more specific, but consistent, meaning—the ability of two systems to exchange information and to make use of the information exchanged.[5] Although both technical and legal definitions of interoperability vary in

[4] MERRIAM WEBSTER ONLINE, http://www.merriam-webster.com/dictionary/interoperability ("ability of a system ... to work with or use the parts or equipment of another system").

[5] *See* URS GASSER & JOHN PALFREY, BREAKING DOWN DIGITAL BARRIERS: WHEN AND HOW

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 that system and another. 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. A system that exhibits interoperability in one context is likely to be non-interoperable in others. Second, interoperability is not binary, but rather a matter of degree.[6] The extent to which two systems interoperate is a function of both how much information they share and the degree to which that information can be utilized. Complete seamlessness in the exchange and use of information between two systems is difficult to achieve, but interoperability does not demand perfection.

Because it is both relational and gradated, interoperability is a flexible, context-sensitive descriptor of a variety of interactions. But 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 flows in both directions. Interoperability, therefore, can embrace both bidirectional and unidirectional information exchanges, raising the related question of how interoperability is achieved. It could come about as the result of cooperation between two or more systems, or from a unilateral decision by the designers of a single system to interoperate with another.

Indeed, both systems in a potential exchange of information can take steps either to facilitate or frustrate interoperability. As a result, the heavy lifting in an

---

ICT INTEROPERABILITY DRIVES INNOVATION 4, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/interop-breaking-barriers_1.pdf ("the ability to transfer and render useful data and other information across systems (which may include organizations), applications, or components."); INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE STANDARD COMPUTER DICTIONARY: A COMPILATION OF IEEE STANDARD COMPUTER GLOSSARIES (1990) ("the ability of two or more systems or components to exchange information and to use the information that has been exchanged."); 17 U.S.C. § 1201(f) ("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 ("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 ("the ability to exchange information and mutually to use the information which has been exchanged."); European Interoperability Framework for Pan-European eGovernment Services Version 1.0, http://europa.eu.int/idabc/en/document/3761 ("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.").

[6] 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 that they exchange.").

interoperable relationship can be done at either end of that exchange.[7] A system encourages interoperability through the use of open, unencrypted, or easily reverse engineered file formats, data structures, and communications protocols. These design choices yield outputs that potentially interoperable 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.[8] When systems share information in ways that impede interoperability, a heavy burden falls to those attempting to make use of that information. In order to do so, developers must either reverse engineer or license the necessary information. But reverse engineers often contend with both technical complexity and intentional obfuscation that renders their efforts more difficult.

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.[9] Likewise, commentators sometimes speak of the role of data interoperability.[10]

A system is "a collection of components organized to accomplish a specific function or set of functions."[11] 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. But while program-level interoperability does not require much of a conceptual leap, data interoperability might pose a more significant hurdle. Data does not immediately lend itself to being characterized as sharing and using information in the same way as computer programs.

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.[12] So while data may be passed from one

---

[7] 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, in effect, render those two systems interoperable with each other.

[8] 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.

[9] *See, e.g.*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INFORMATION TECHNOLOGY VOCABULARY: FUNDAMENTAL TERMS (1993) ("[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.").

[10] *See, e.g.,* Stacy Baird, *The Government at the Standards Bazaar*, 18 STAN. L. & POL'Y REV. 35 (2007) (discussing need for data interoperability in the 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.").

[11] IEEE, *supra* note 5.

[12] *See* R.L. Ackoff, *From Data to Wisdom*, 16 J. APPLIED SYSTEMS ANALYSIS 3 (1989).

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.

But this view of data as a passive participant in the exchange of usable information can be contrasted with another way of thinking about data. This view recognizes that the line between program and data is often not clearly defined.[13] Just as programs 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 can be shared 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? Since Pages does not interact directly with Word, characterizing the relationship as program-to-data interoperability could be a more helpful conceptual tool. But regardless of which characterization more accurately describes the role of data, both perspectives confirm that data, just like programs, can facilitate interoperability.

B. Valuing Interoperability

Although its intrinsic value is often apparent to users of technology—particularly in its absence—the value of interoperability is largely instrumental. Interoperability is typically celebrated because it fosters a host of socially desirable ends: innovation, competition, consumer choice, and accessibility, among others.[14] On the whole, these justifications for promoting interoperability hold true, even if they fail to capture all the nuances of its social impact.[15]

Interoperability encourages certain types of innovation, but can reduce incentives for others. Incremental innovation, the process of improving and

---

[13] *See* Allen Newell, *The Models Are Broken, The Models Are Broken!*, 47 U. PITT. L. REV. 1023, 1033 (1986) ("the boundary between data and program—that is, what is data and what is procedure—is very fluid."); MARTIN DAVIS, THE UNIVERSAL COMPUTER: THE ROAD FROM LEIBNIZ TO TURING 164-65 (2000) (describing the distinction between program and data as an illusion).

[14] *See* S. Rep. No. 105-190, at 32 (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 the concern of network neutrality advocates that a "reduction in interoperability would impair the environment for competition and innovation….").

[15] *See* GASSER & PALFREY, *supra* note 5, at 18.

extending existing technologies, benefits from the interaction with existing products that interoperability enables. Because it leverages prior innovative activity, incremental innovation typically requires less investment, spurring contributions from a wider variety and greater number of developers. But innovators who choose to create new technologies from the ground up rather than improve or extend existing products or platforms could be hampered by interoperability. First, the network effects that emerge from interoperable technologies could prove difficult to overcome, even for a superior offering.[16] 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.[17]

The effect of interoperability on competition is similarly complicated. In markets defined by interoperability, barriers to entry tend to be lower since new 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, a greater number and variety of available choices, and more freedom to exercise those options. But under some circumstances, interoperability can reduce competition. If a handful of firms agree to interoperate, but exclude newcomers from the resulting interoperable network, competition could suffer. Aside from such collusive behavior, interoperability also could discourage Schumpeterian competition. Although price and output competition would likely increase with greater interoperability, incentives for innovation-based competition to supplant the current market with a new paradigm would likely be lessened if competitors were free to interoperate. With less assurance of temporary monopoly rents, the investment associated with innovation-based competition poses greater risk.

Interoperability also promotes access. Information and services are more likely to find their way into more hands in markets that feature interoperability than those that do not, all other considerations being equal. 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 the dominant network.

Apart from these widespread policy implications, individual firms may have strong incentives to limit interoperability with their own offerings. Firms with large user bases and established reputations, in particular, are likely to oppose

---

[16] *See* Joseph Farrell & Garth Saloner, *Standardization, Compatibility, and Innovation*, 16 RAND J. ECON. 70, 71 (1985)

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

interoperability for two reasons.[18] First, interoperability tends to lower barriers to entry created by network effects.[19] Second, interoperability increases the relative value of competing products by enabling access to the dominant network.[20] Both of these effects favor less established firms over their larger rivals.

History offers no shortage of examples of efforts to resist interoperability.[21] 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.[22] Railroads offer another useful set of early examples. Czarist Russia's use of railroad gauges wider than those common in Europe was meant slow potential invaders,[23] a strategy shared by developers who rely on proprietary formats to limit access to their platforms.[24] In India, the British laid non-uniform tracks to regionalize trade,[25] a tactic not unlike the contemporary region coding of DVDs and video games to enable market segmentation.[26]

These examples suggest that the methods by which interoperable products and services are created matter. If interoperability requires agreements between competitors, incentives for radical innovation and Schumpeterian competition might be preserved. But the risk of collusive behavior and barriers to entry for incremental innovators would likely increase. On the other hand, legal rules than permit unauthorized efforts to achieve interoperability could have the opposite effect.

The overall impact of unauthorized interoperability is a fact-intensive question with no clear empirical answer.[27] To the extent unauthorized interoperability reduces incentives for radical innovation, but increases incentives for

---

[18] Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, AMERICAN ECON. REV. 424, 425 (1983).

[19] Farrell & Katz, *supra* note 17, at 611 (discussing tendency of network effects to increase barriers to entry.)

[20] Farrell & Saloner, *supra* note 16, at 71.

[21] Sometimes interoperability is opposed by third parties who reap the benefit of inefficiencies introduced by incompatibility. In 1853, an effort to replace the three gauges of railroad tracks in Erie, Pennsylvania with a uniform track width prompted bloody riots. Local workers who unloaded cargo, changed car wheels, and then reloaded cargo at the juncture of these incompatible gauges rightly feared unemployment. Achsah Nesmith, *A Long Arduous March Toward Standardization*, SMITHSONIAN MAGAZINE, March 1, 1985, at 83.

[22] Columbia and Victor records were interchangeable since 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 allowed Edison records to play on competing hardware. RANDALL STROSS, THE WIZARD OF MENLO PARK 219-220 (2007).

[23] JONATHAN BAND & MASANOBU KATOH, INTERFACES ON TRIAL 40-41 (1995).

[24] The Nintendo Gamecube console, for example, was designed to accept 3-inch game discs rather than standard 5-inch DVDs as a means to prevent use of unauthorized copies. Alex Pham & Jon Healey, *Games Prove a Hassle for Web Pirates*, L.A. TIMES, May 17, 2003, at C1.

[25] BAND & KATOH, *supra* note 23.

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

[27] *See* GASSER & PALFREY *supra* note 5, at 18.

incremental improvements, any estimation depends, in part, on the relative value of those species of innovation and the competition they encourage—values likely to shift over time and vary between industries. In addition, such an estimate depends on the differential between the incentives necessary to spur radical innovation and those currently provided by intellectual property rights. If the IP system generally over-incentivizes innovators, the reduction in incentives introduced by unauthorized interoperability could reduce deadweight loss. Suffice it to say, this Article will not resolve these questions.

As the discussion below describes, intellectual property law operates from the typically implicit, but occasionally explicit assumption that interoperability is beneficial and worth encouraging—or at least permitting—in most circumstances. Of course, allowing interoperability without granular consideration of its effect on innovative incentives threatens to introduce uniformity costs. But such costs are an inherent, if regrettable, aspect of uniform IP grants.[28] Nonetheless, intellectual property doctrine reflects some sensitivity to the potential downsides of interoperability. The reduced incentives potentially triggered by unauthorized interoperability are primarily a concern for patent law, which affords greater control over interoperable technologies than either trade secrecy or copyright.

C. Intellectual Property & 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, intellectual property 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, and 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 in part 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.

Trade secrecy 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 developed"[29]—as a legitimate means to obtain information

---

[28] See Michael W. Carroll, *One for All: The Problem of Uniformity Costs in Intellectual Property*, 55 AM. U.L. REV. 845 (2006).

[29] UNIF. TRADE SECRETS ACT § 1 cmt. 2; *see also* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) ("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 ("the process of extracting know-how or knowledge from a human-made artifact.").

about lawfully acquired products.[30] Without reverse engineering, developers would be unable to discover communications protocols, format specifications, and other program interfaces that enable interoperability.[31] But the favored status of reverse engineering is an outgrowth of fundamental limits on the scope of trade secret protection, rather than any express intent to encourage interoperability.

Likewise, longstanding limits on the scope of copyright protection create a legal environment hospitable to interoperability by minimizing the extent to which copyright regulates interoperable technologies. First, copyright does not grant exclusive rights in systems or their functional components, and excludes them from the scope of protection of otherwise protected subject matter.[32] By refusing protection for the very objects capable of interoperating, copyright avoids any direct regulation of interoperability.[33] The originality requirement[34] and the doctrines of merger and scènes à faire[35] likewise contribute to copyright's permissiveness

---

[30] UNIF. TRADE SECRETS ACT § 1 cmt. 2 (reverse engineering is proper if the product was acquired by "fair and honest means"); Restatement (Third) Unfair Competition 43 (1995); Kewanee Oil, 416 U.S. at 476 (recognizing reverse engineering as proper); Nat'l Tube Co. v. Eastern 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").

[31] *See, e.g.*, Secure Services Technology, Inc. v. Time and Space Processing, Inc., 722 F. Supp. 1354 (E.D. Va. 1989) (permitting the reverse engineering of secure facsimile machines to discover a the implementation of a communications protocol necessary for interoperability).

[32] *See* Baker v. Selden, 101 U.S. 99 (1879) (holding that copyright in a text describing a system of accounting did not extend to the system itself); *see also* Perris v. Hexamer, 99 U.S. 674, 675 (1878) (holding that the copyright in a map "marked with arbitrary coloring and signs" was not infringed by a map using a similar system). Congress codified Baker's holding in the Copyright Act of 1976. *See* 17 U.S.C. § 102(b).

[33] *See* Taylor Instrument Cos. v. Fawley-Brost Co., 139 F.2d 98 (7th Cir. 1943) (holding that a chart used as a component of an 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."); Brown Instrument Co. v. Warner, 161 F.2d 910 (D.C. Cir. 1947) (a chart that served as a component of a measuring device was ineligible for copyright protection); Lotus Dev. Corp. v. Borland Int'l, 49 F.3d 807, 815 (1st Cir. 1995) (holding that the menu command hierarchy of a spreadsheet application was a method of operation), aff'd by an equally divided Court, 516 U.S. 233 (1996).

[34] The originality requirement reinforces *Baker* by limiting copyright protection for the output of an unprotectable system. *See, e.g.*, 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 a competitor to use interoperable codes); Southco, Inc. v. Kanebridge Corp. (en banc), 390 F.3d 276,278 (3d Cir. 2004). (holding that serial numbers for identifying parts were characterized by "an utter absence of creativity," allowing distributors of interchangeable parts to utilize identical numbers); ATC Distrib. v. Whatever It Takes Trans. & Parts, Inc., 402 F.3d 700 (6th Cir. 2005); *but see* ADA v. Delta Dental Plans Ass'n, 126 F.3d 977 (7th Cir. 1997) (holding that a taxonomy of medical codes was original).

[35] Applied to computer programs, the merger and scènes à faire doctrines suggest that if a limited number of options exist to efficiently achieve a given function, 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 (2nd Cir. 1992)

regarding interoperability.

Aside from limiting the scope of its protection, copyright avoids interference with interoperability by limiting the exclusive rights copyright holders are granted and their ability to hold technology developers responsible for acts of infringement committed by their users. 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.[36] Simply put, copyright provides no exclusive right to read.[37] 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. And even if the use of such technologies gives rise to direct infringement by a user, limits on indirect liability insulate developers in most instances.[38]

But not all copyright rules favoring interoperability grow out of independent constraints on the scope of copyright protection. The reverse engineering privilege offers a more explicit recognition of 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.[39] This willingness to enlist the fair use defense to address threats to interoperability suggests that copyright not only tolerates interoperable technologies, but promotes them.

In many respects, patent law is consistent with the policy that emerges from trade secrecy and copyright. The creation of products that interoperate with patented inventions does not infringe unless it entails making, using, or selling that invention.[40] Although the Patent Act neither expressly prohibits nor permits reverse engineering,[41] exhaustion doctrine ensures that once a patented product is sold,

---

(holding that the merger doctrine precludes exclusive rights in structural choices dictated by efficiency); *id.* at 710 (analogizing programming constraints dictated by external hardware compatibility and interoperability requirements to those recognized by the scènes à faire doctrine).

[36] *See* Stover v. Lathrop, 33 F. 348, 349 (U.S. Court of Appeals 1888) ("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.").

[37] *But see* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENTM'T L.J. 29 (1994) (arguing that an expansive reading of the reproduction right in the digital environment could lead to copyright holder control over the act of reading and other personal uses).

[38] Indirect liability enables copyright holders to exert control over the distribution and use of interoperable technologies that give rise to enduser infringement under three circumstances: first, if the technology at issue is incapable of substantial non-infringing use, Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984); second, if the developers of that technology encourage or induce enduser infringement, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd. 545 U.S. 913 (2005); or third, if those developers possess the legal right and practical ability to control end-user infringement and enjoy a direct financial benefit from such infringement, Perfect 10, Inc. v. Amazon.com, 508 F.3d 1146 (9th Cir.2007).

[39] *See infra* Part II.A.

[40] *See* 35 U.S.C. §§ 271.

[41] *Id.* (defining patent infringement and omitting any reference to acts reverse engineering).

purchasers are free to use it.[42] Such use could include reverse engineering to achieve interoperability. Software-based inventions, however, introduce some additional worries since reverse engineering may entail copying or "making" the invention rather than merely using it.[43] Patents pose the greatest threat to 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 a license.[44]

Even acknowledging the role patents sometimes play in controlling interoperability, traditional intellectual property law infrequently interfered with unauthorized attempts to achieve interoperability. But as discussed in the next Part, the DMCA embodies a very different approach.

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."[45] Reflecting these fears, two World Intellectual Property Organization treaties called for "adequate legal protection" against the circumvention of technological protection measures ("TPM").[46] Ostensibly to implement its treaty obligations, Congress enacted the DMCA in 1998.[47]

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.[48] The

---

[42] *See* United States v. Univis Lens Co., 316 U.S. 241 (1942).

[43] Julie E. Cohen & Mark A. Lemley, *Patent Scope and Innovation in the Software Industry*, 89 CALIF. L. REV. 1 (2001) (stating that reverse engineering a computer program by decompilation likely constitutes an infringing "making").

[44] *See, e.g.*, Atari Games Corp. v. Nintendo of Am., Inc., 30 U.S.P.Q.2d (BNA) 1401 (N.D. Cal. 1993) (holding that the development of an interoperable product infringed an interface patent); *see also* Pamela Samuelson, *Are Patents on Interfaces Impeding Interoperability?* (manuscript on file with author) (explaining that "patents for interfaces is because such patents can be very powerful in conferring on their owners an exclusive right to control the development not only of competing but also of complementary products.").

[45] *See* S. Rep. No. 105-190, at 2 & 8.

[46] WIPO Copyright Treaty, art. 11; WIPO Performances and Phonograms Treaty, art. 18.

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

[48] 17 U.S.C. § 1201(a)(3)(B) & (b)(2)(B). These two varieties of TPMs often overlap in practice,

statute regulates both circumvention—the act of decrypting an encrypted work, or otherwise disabling, removing, or avoiding a technological measure[49]—and trafficking—the manufacture, distribution, sale, or offering to the public of devices, tools, or technologies that enable circumvention.[50] With respect to access controls, both the act of circumvention and the trafficking in circumvention technologies are prohibited. Trafficking in technologies that circumvent copy controls is likewise banned, but the act of circumventing a copy control is not. However, such acts may nonetheless constitute copyright infringement.

This Part considers the impact of these prohibitions on interoperability. Because it enables broad rights-holder control over interoperable technologies, the DMCA deviates from the traditional treatment of interoperability in intellectual property law. Recognizing the DMCA's potential impact, Congress enacted a statutory exemption—§ 1201(f)—to limit the extent to which anticircumvention law disturbed existing interoperability policy. But the effectiveness of this exemption has been undermined. First, courts have misinterpreted several of its basic requirements, encouraging overreaching claims sounding far from 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 fully safeguard interoperability.

A. The 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. But because of the breadth of its prohibitions, the DMCA gives rise to a number of unintended consequences, including its impact on interoperability.[51] Rather than allow or encourage 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. Developers who enable interoperability with works restricted by TPMs without permission, however, face potential liability.

---

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) (a TPM is a 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) (a TPM is a copy control if the copying allowed "is not particularly useful").

[49] 17 U.S.C. § 1201(a)(3)(A).

[50] *Id.* § 1201(a)(2) & (b)(1). The trafficking bans apply to devices: (1) primarily designed for circumvention; (2) with only limited commercially significant uses aside from circumvention; or (3) marketed for use in circumvention. *Id.*

[51] *See* ELECTRONIC FRONTIER FOUNDATION, UNINTENDED CONSEQUENCES: FIVE YEARS UNDER THE DMCA (April 2006), http://www.eff.org/files/DMCA_unintended_v4.pdf.

The restraints on unilateral efforts to achieve interoperability are threefold. First, the DMCA discourages the creation of unauthorized interoperable products by interfering with certain acts of reverse engineering. The DMCA's circumvention ban functions at its core as a bar against the reverse engineering of products containing effective access controls.[52] In order 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.[53]

Second, the DMCA adversely affects interoperability by prohibiting the distribution of interoperable products. In order to interoperate with a work that incorporates an effective TPM, a product must include code that functions as the equivalent of the information or process that enables access or copying of the protected work. Otherwise, it would lack the ability to exchange information with the TPM-protected system. But products designed to access or copy a work protected by an effective TPM are subject to the trafficking ban. So the distribution of a product that interoperates with a work protected by a technological measure could constitute an independent violation of § 1201. Finally, the DMCA discourages interoperability by exposing the users of such technologies to liability. By utilizing a tool or device that relies on acts of circumvention to establish interoperability, endusers themselves could violate the circumvention ban.

In short, creating, using, or distributing products that interoperate with works restricted by effective TPMs may violate the circumvention or trafficking bans. As a result, in the absence of any applicable defense, the DMCA entitles copyright holders, TPM developers, or mere licensees to prevent the emergence of interoperable products so long as the minimal effectiveness requirement is satisfied.

This potential for control over interoperable technologies represents a marked departure from the treatment of interoperability under earlier intellectual property doctrine. By yielding power over the development and distribution of products that interface with TPM-protected works, the DMCA results in control on par with the patent grant in its power over interoperable technologies.[54] But unlike a patent, which must satisfy the comparatively exacting standards of novelty and non-obviousness, an effective TPM must only restrict access and copying in the ordinary

---

[52] 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).

[53] *Id.* § 1201(a)(3)(A).

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

course of operation.

B. The Interoperability Exemption

The DMCA's potential restraint of interoperability did not go unnoticed during the congressional debate.[55] Software industry groups argued that the DMCA would undermine *Sega v. Accolade*, a case decided just six years earlier that vindicated the reverse engineering of software programs. [56] In response, Congress enacted § 1201(f) in order preserve the right to reverse engineer for interoperability purposes.

In *Sega*, the Ninth Circuit held that the creation of intermediate copies of a computer program during reverse engineering was protected as a fair use when undertaken to isolate unprotected program elements.[57] 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.[58] Sega sued, maintaining that the intermediate copying of its code in the reverse engineering process was an act of infringement.

The Ninth Circuit agreed with Sega that intermediate copying of software programs was a *prima facie* violation of the reproduction right.[59] But recognizing that reverse engineering—and the attendant intermediate copying—was "the only means of gaining access to [] unprotected aspects of the program" necessary to achieve interoperability, the court held that Accolade's copying was fair.[60] While acknowledging that other legitimate interests could justify reverse engineering, *Sega* unambiguously identifies interoperability as a value worthy of promotion.[61] Other courts followed suit, holding that copying necessary for reverse engineering is fair.[62]

---

[55] 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* 17 U.S.C. § 1201(d)-(j). In addition, the DMCA permits the Librarian of Congress to recommend temporary exemptions from the circumvention ban for specific classes of copyrighted works if their non-infringing use has been aversely affected. *Id.* § 1201(a)(1)(B).

[56] Sega Enters. v. Accolade, Inc., 977 F.2d 1510, 1527 (9th Cir. 1992).

[57] *Id.* at 1527.

[58] *Id.* at 1515.

[59] *Id.* at 1519.

[60] *Id.* at 1520.

[61] *Id.*

[62] *See also* 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."); Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596, 598 (9th Cir. 2000) (holding that intermediate copying necessary to reverse engineer the BIOS of the Sony Playstation in order to "gain access to [its] unprotected functional elements."); *but see*

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 rudimentary protection measure to thwart the use of unlicensed games on its Genesis console.[63] But, six years before the DMCA, Accolade had no legal obligation to respect that restraint.[64] Developers understandably viewed a broad anticircumvention right as a threat to the freedom to interoperate that *Sega* endorsed.

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 the enactment" of the DMCA.[65] 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.[66]

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; (6) the identification and analysis does not constitute infringement.[67] Section 1201(f)(2) allows the development and use of technologies that enable circumvention to the extent necessary to achieve interoperability.[68] Further, any information lawfully acquired or tools lawfully developed can be distributed for the sole purpose of enabling interoperability.[69]

Compaq Computer Corp. v. Procom Technology, 908 F. Supp. 1409, 1416 (W.D. Tex. 1995).

[63] Sega, 977 F.2d at 1528.

[64] *Id.*

[65] S. Rep. No. 105-190, at 32 (citing Sega v. Accolade, 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. 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. J.L. & ARTS 137, 149 n.35 (1999) (suggesting that § 1201(f) might not embrace all reverse engineering permitted under prior law).

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

[67] 17 U.S.C. § 1201(f)(1). The language and basic requirements of § 1201(f) borrow heavily from Article 6 of the EU Software Directive. *See* Council Directive 91/250/EEC, 1991 O.J. (L 122) 42 (EC).

[68] *Id.* § 1201(f)(2).

[69] *Id.* § 1201(f)(3).

Early § 1201 litigation demonstrated that Congress's concern over 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.[70] 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.[71] 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.

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—not only from reduced console sales, but from decreased licensing revenue—as consumers and game developers defected to the PC platform.[72] 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.

But Sony's anticircumvention theory was deeply flawed. First, since the game data could be freely read by standard CD-ROM drives, it is far from clear that the Playstation authorization code functioned as an effective access control.[73] Second,

---

[70] *See* Complaint, Sony Comp. Entmt. Inc. v. Connectix Corp., No. 99-cv-003900; Complaint, Sony Computer Enter v. Bleem, LLC, No. 99-cv-01590; *see also* Jonathon Band & Taro Isshiki, *The New Anti-Circumvention Provisions in the Copyright Act: A Flawed First Step*, 3 CYBER. LAW. 2 (1999).

[71] The Connectix and Bleem emulators were developed for the Mac and Windows operating systems respectively. In order to achieve interoperability, Connectix reverse engineered the copyrighted Playstation BIOS, and act ultimately deemed a fair use by the Ninth Circuit. *See* Sony Comp. Entmt. Inc. v. Connectix Corp., 203 F.3d 596, 609 (9th Cir. 2000).

[72] Tellingly, after losing its copyright infringement suit against Connectix, Sony purchased the company and discontinued its emulation software rather than implement support for the Playstation authorization code. Phillip Michaels, *Emulation Sensation: Microsoft Buys Virtual PC from Connectix*, MACWORLD, May 2003, at 25.

[73] 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 223, May 19, 2000, http://www.copyright.gov/1201/hearings/1201-519.pdf

the "no mandate" provision of the DMCA freed the emulators of any obligation to comply with the Playstation authentication code if it was not an effective TPM.[74] Finally, Sony filed its complaints during the initial two-year moratorium on enforcement of the DMCA's circumvention ban.[75] Not surprisingly, Sony ultimately chose not to pursue its § 1201 claims.[76]

Assuming Sony could have overcome these threshold obstacles,[77] the emulator cases would have provided an opportunity for courts to apply § 1201(f) under 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 Genesis console.[78]

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 sole the purpose of obtaining information necessary to render Playstation games interoperable with independently created emulators. And since these acts of reverse engineering did not constitute infringement, so long as the interoperability information was not readily available, § 1201(f)(1) would have permitted circumvention. Moreover, the distribution of the emulator software—assuming it enabled acts of circumvention—would have been privileged so long as the sole purpose of its distribution was facilitating interoperability.

Unfortunately, the first case to analyze § 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 non-licensed players from decrypting and playing DVD movies.[79] 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.[80]

(Testimony of Jonathan Hangartner).

[74] *See* 17 U.S.C. § 1201(c)(3).

[75] *Id.* § 1201(a)(1)(B).

[76] Sony continued its litigation against Connectix and Bleem on other theories. *See* Sony Comp. Entm't Inc. v. Connectix Corp., 203 F.3d 596, 609 (9th Cir. 2000); Sony Comp. Entm't, Inc. v. Bleem, LLC, 214 F.3d 1022 (9th Cir. 2000).

[77] Sony eventually succeeded in enforcing Playstation access controls under the DMCA. Sony Comp. Entm't, Inc. v. GamerMasters, 87 F. Supp. 2d 976 (N.D. Cal. 1999) (enjoining the vendor of the Game Enhancer, a device that allowed players load games intended for foreign markets). Notably, Sony offered no proof that the Game Enhancer enabled infringement, only that it interfered with Sony's market segmentation strategy. *See also* Sony v. Divineo, 457 F. Supp. 2d 957 (N.D. Cal. 2006) (granting summary judgment against defendants who trafficked in Playstation modification chips).

[78] Connectix, 203 F.3d at 609 (9th Cir. 2000).

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

[80] *Id.* at 218.

The *Reimerdes* court offered expansive readings of the DMCA's liability provisions and narrow interpretations of its various defenses, among them § 1201(f).[81] 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 computer programs, not copyrighted works generally.[82] Since CSS restricted access to movies stored on DVDs, not computer programs, § 1201(f) was inapplicable. 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. 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.[83] 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.[84] 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 interoperability could be invoked as a pretext for circumvention aimed at infringement. But 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 misreads the statute.

Second, the court misconstrued the limits on distribution of interoperability information and circumvention tools under § 1201(f)(3). The court claimed that the statute permitted dissemination of information obtained through reverse engineering, but not the means of circumvention used to obtain such information, ignoring the plain language of § 1201(f).[85] The court also erred in imposing a blanket rule against the public distribution of exempted tools and information.[86] 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 satisfied.[87] A

---

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

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

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

[84] Reimerdes, 82 F. Supp. 2d at 218.

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

[86] Reimerdes, 111 F. Supp. 2d at 320.

[87] The court claimed that § 1201(f) permits the sharing of interoperability information only by one who acquires that information. As discussed *infra*, such a limit could prevent publication of

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.

Given the looming issues of interoperability in many DMCA disputes, § 1201(f) has been the subject of surprisingly little judicial analysis. Only a handful of published opinions make reference 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, emboldened plaintiffs to test the bounds of their control over interoperable products.

C. The Durable Goods Cases

Early DMCA litigation focusing on entertainment content, while arguably protecting legitimate copyright interests, evinced some desire on the part of plaintiffs to interfere with interoperable technologies.[88] But as consumer electronics manufacturers began to enforce TPMs incorporated in their products, any pretense of protecting against the threat of free-riding Internet infringers 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, a manufacturer of laser and inkjet printers, was among the first to adopt this tack. Like many printer manufacturers, Lexmark sold printers cheap, but charged a premium for ink cartridges. In order 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 would use the cartridge only once and return it to Lexmark.[89] Lexmark employed a TPM intended to prevent refilled prebate cartridges from interoperating with its printers.[90]

Lexmark alleged that Static Control Components ("SCC"), creator of the SMARTEK chip, which mimicked Lexmark's authentication sequence, was trafficking in a circumvention device.[91] According to Lexmark, the operation of its printers relied on the Printer Engine Program ("PEP"). If a non-Lexmark cartridge

---

interoperability tools and information for a variety of purposes, including academic research.

[88] *See* Burk, *supra* note 54, at 561-565 (discussing anti-competitive uses of the DMCA); Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1110-1111 (2003) (same).

[89] Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 530 (6th Cir. 2004). This agreement took the form of a shrink-wrap license on the cartridge packaging. *Id.* Non-prebate cartridges, which were not subject to this restriction, could be purchased at a higher price. *Id.*

[90] 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. If the codes matched, the printer accepted the cartridge and operated normally. If the authentication sequence failed, the printer would not operate. *Id.* at 530.

[91] *Id.* at 530-31.

was installed, the authentication sequence would fail, rendering those portions of the PEP that enabled printer functionality inaccessible. The SMARTEK chip bypassed this control and allegedly enabled unauthorized access to the PEP.[92]

Although the District Court granted Lexmark's request for a preliminary injunction,[93] the Sixth Circuit regarded Lexmark's argument with palpable skepticism, questioning whether § 1201 applied to its technology at all. The court concluded it did not. According to the court, access to the PEP was not controlled by the authentication sequence, but by the purchase of a Lexmark printer because the PEP was not encrypted or otherwise protected against literal copying.[94] Since the authentication sequence did not meaningfully control access to the code, "the DMCA [did] not apply."[95]

In *Chamberlain Group v. Skylink*, the Federal Circuit faced a similar theory.[96] Chamberlain manufactured the Security+ garage door opener ("GDO") system, which utilized a "rolling code" to sequentially modify the signal used by Chamberlain's remote transmitter to activate the GDO.[97] Skylink marketed universal remotes designed to interoperate with a variety of GDO systems, including the Security+ line.[98] Chamberlain filed suit, alleging that Skylink's universal transmitter violated the DMCA's anticircumvention provision. On Chamberlain's theory, access to the copyrighted code that operated its Security+ GDOs was protected by the rolling code system. 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.[99]

On appeal, the Federal Circuit agreed that Chamberlain customers possessed an "inherent legal right to use" the software embedded in their GDOs.[100] Perhaps more importantly, the court held that in order 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."[101] Since consumers were entitled to access the GDO software, Chamberlain was unable to

---

[92] *Id.*

[93] 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.

[94] 387 F.3d at 546-47.

[95] *Id.*

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

[97] *Id.* at 1183.

[98] 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.

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

[100] 381 F.3d at 1202.

[101] *Id.*

prove "the critical nexus between" the access facilitated by Skylink's device and the protection of a legitimate copyright interest.[102]

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. Although 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, how such permutations would be analyzed remains to be seen.[103] *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 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,[104] 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] product[s] in conjunction with competing products."[105] Such power, in turn, could "create monopolies of manufactured goods"[106] that relied on the DMCA to provide "broad exemptions from [] the antitrust laws."[107]

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 or thoroughly analyzed its application.[108] The district court in *Chamberlain* made no mention of § 1201(f), and the Federal Circuit declined

---

[102] *Id.* at 1203.

[103] 387 F.3d at 551-52 (Merritt, J., concurring).

[104] Storage Tech. v. Custom Hardware Eng'g, 421 F.3d 1307 (Fed. Cir. 2005).

[105] Chamberlain, 381 F.3d at 1201.

[106] Lexmark, 387 F.3d at 551.

[107] Chamberlain, 381 F.3d at 1203

[108] *See* Brief *Amicus Curiae* of Computer & Communications Industry Association, Chamberlain Group, Inc. v. Skylink Techs., 381 F.3d 1178 (Fed. Cir. 2004), No. 04-1118; Brief *Amicus Curiae* of Electronic Frontier Foundation, Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004), No. 0305400.

to reach the issue.[109] Since the court was satisfied that Chamberlain could not prove a *prima facie* violation of § 1201, the failure to delve into an affirmative defense offers little cause for criticism.[110] But clarification of the defense, particularly in light of *Reimerdes*, would have been welcome.

Lexmark offered some clarification of the independent creation requirement of § 1201(f), even if only *dicta*. The Sixth Circuit explained that independent creation only requires proof of originality; the new program must not infringe the protected program.[111] 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.[112] But in the end, *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."[113]

Although both courts were reluctant to reach the issue, *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. And 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.[114] 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

---

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

[110] The court continued this silence on § 1201(f) in Storage Tech. v. Custom Hardware. 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. 2004 U.S. Dist. LEXIS 12391 (D. Mass., July 2, 2004). Although it reversed the infringement holding, the Federal Circuit saw no need to revisit the interoperability question.

[111] Likewise, since the Toner Loading Program was not protected, its copying did not constitute infringement under § 1201(f)(3). 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.

[112] Lexmark, 253 F. Supp. 2d at 970.

[113] 387 F.3d at 522.

[114] *See* 17 U.S.C. § 1201(f)(1).

is precisely the sort of inquiry the Ninth Circuit undertook in *Sega*, the case § 1201(f) was expressly intended 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 non-interoperable 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 in order 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*. And while they articulated meaningful outer boundaries on the scope of § 1201 and staved off two attempts to restrict interoperable technologies, *Lexmark* and *Chamberlain* may have more effectively curbed further efforts to leverage the DMCA as a tool for restricting interoperability if they had 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

Lexmark and *Chamberlain* have been rightly praised for resisting the expansive interpretation of the DMCA embodied in *Reimerdes*,[115] 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. But 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).

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 on the hope of profits from expensive ink, mobile phones are often subsidized by service charges recouped over the life of the phone.[116] As a result,

---

[115] *See, e.g.*, Niva Elkin-Koren, *Making Room for Consumers Under the DMCA*, 22 BERKELEY TECH. L.J. 1119, 1132-34 (2007); Burk, *supra* note 54, at 571 ("The *Chamberlain* and *Lexmark* opinions radically change the trend begun in *Reimerdes*….").

[116] Tim Wu, *Wireless Carterphone*, 1 INT'L J. COMMS. 398-99 (2007).

providers have strong incentives to limit the availability of interoperable services.

Mobile phones include a number of programs responsible for various functions, including firmware that controls the ability to connect to a cellular network. Phones sold to endusers are typically configured to connect only to one carrier's network.[117] Carriers rely on a variety of TPMs to prevent users from accessing and reconfiguring firmware to allow connections to competing networks.[118] 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.[119] In other cases, phones are unlocked by deleting the firmware—and the associated TPM—and replacing it with new firmware that enables connectivity.[120]

TracFone is a vendor of prepaid mobile phones, which it sells at a loss.[121] 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.[122] TracFone has filed a series of lawsuits alleging violations of § 1201 by vendors that unlocked and resold its phones.

As the Register of Copyrights recognized in the 2006 DMCA Anticircumvention Rulemaking,[123] 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 holder."[124] Since unlocking is a non-infringing use, mobile phone firmware was exempted from the circumvention ban so long as unlocking occurs for the sole purpose of lawfully connecting to a wireless network.[125]

But this exemption has not deterred TracFone from continuing its aggressive pursuit of those who unlock its handsets. Indeed, TracFone has prevailed in a string

---

[117] *See* Comments of the Wireless Alliance & Robert Pinkerton 4, http://www.copyright.gov/1201/2006/comments/granick_wirelessalliance.pdf

[118] *Id.* at 7 (discussing the variety of technological means used by carriers).

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

[120] *Id.*

[121] TracFone Wireless, Inc. v. GSM Group, Inc., 2008 WL 2215059, *1 (S.D. Fla. May 15, 2008).

[122] *Id.*

[123] *See* 17 U.S.C. § 1201(a)(1)(C) (empowering the Librarian of Congress to exempt classes of copyrighted works from the anticircumvention ban to the extent it interferes with non-infringing use of those works).

[124] Recommendation of the Register of Copyrights 50-51 (November 17, 2006), http://www.copyright.gov/1201/docs/1201_recommendation.pdf.

[125] *Id.*

of recent § 1201 cases, only one of which even considered the mobile phone exemption.[126] There the court denied a motion to dismiss notwithstanding the exemption because the complaint alleged that defendants' purpose was not solely wireless network connectivity, but included reselling unlocked phones.[127]

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. It was intended to exclude circumvention by those seeking access to ringtones, video content, and other copyrighted works stored on mobile phones.[128] Although the mobile phone exemption should have prevailed over TracFone's circumvention theory, the exemption offered no colorable defense to its trafficking claim.[129] 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.[130] Instead, it hopes to protect its business model and pricing scheme from competitive forces by preventing consumers from connecting to interoperable networks. But 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 holds 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 access to the underlying work is enabled as a result.[131] 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

---

[126] *See* TracFone Wireless, Inc. v. Sol Wireless, No. 05-23279 (S.D. Fla. Feb. 28, 2006) (entering stipulated Final Judgment enjoining unlocking); TracFone Wireless, Inc. v. Dixon, 475 F. Supp. 2d 1236 (M.D. Fla. 2007) (granting unopposed permanent injunction on the basis of both circumvention and trafficking claims); TracFone Wireless, Inc. v. Bitcell Corp., 2008 U.S. Dist. LEXIS 41955 (S.D. Fla. May 28, 2008) (entering consent judgment and permanent injunction); GSM Group, 2008 WL 2215059.

[127] GSM Group, Inc., 2008 WL 2215059 at *1.

[128] *See supra* note 119, at 44-46. (Testimony of Steven Metalitz).

[129] Although the Copyright Office can exempt certain works from the ban on circumvention, its rulemaking authority does not extent to the prohibition on trafficking in circumvention devices or services. 17 U.S.C. § 1201(a)(1)(E); *see also* Aaron Perzanowski, *Evolving Standards and the Future of the DMCA Anticircumvention Rulemaking*, 10 J. INTERNET L. 1 (2007).

[130] *See supra* note 124.

[131] 17 U.S.C. § 1201(a)(3)(A) (including "remov[al]" of a TPM among the acts considered circumvention).

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.[132] But TracFone's success suggests that the limits those cases impose are sufficiently unclear to justify settlement by multiple defendants, even if its claims are ultimately flawed on the merits.

Section 1201(f) offer unlockers another plausible defense. Although unlocking enables interoperability with communications networks, those networks are composed not only of base stations and radio signals, but also software that controls network communications. So the practical effect of unlocking is interoperability between mobile phone firmware and other independently created programs. But without guidance from established precedent, courts may be reluctant to apply § 1201(f) to facts that appear, on the surface, far from those Congress anticipated. 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* were decided, the Eighth Circuit affirmed the most extensive and deeply misguided analysis of § 1201(f) to date. While *Reimerdes* introduced considerable uncertainty, *Davidson & Assocs. v. Jung* and the district court opinion it affirmed threatened to fundamentally undermine § 1201(f) through their consistently hostile misinterpretation of the statute.[133]

Davidson involved Blizzard, the developer of several multi-player PC games. Blizzard offered an online matchmaking service, Battle.net, that 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.[134]

A group of Blizzard enthusiasts, frustrated with certain shortcomings of Battle.net, developed an alternative matchmaking service that interoperated with Blizzard games.[135] The bnetd project reverse engineered the protocols used by Blizzard games to communicate with Battle.net and developed a functionally

---

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

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

[134] Davidson, 422 F.3d at 635 n.2 & 3.

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

equivalent server and software that allowed players to connect to it.[136] But since bnetd lacked access to Blizzard's database of CD keys, it was unable to ensure that all players used legitimate copies of Blizzard games.[137]

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.[138] Bnetd raised § 1201(f) as one of its defenses, arguing that any circumvention of Blizzard's access controls occurred to enable reverse engineering meant to render the bnetd server software interoperable with Blizzard games, and likewise, any tools it distributed that facilitated circumvention were likewise intended to enable interoperability.[139]

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. Here the district court appeared to confuse the basic elements of a § 1201 violation with the requirements of the interoperability defense, stating that "the statute [] only exempts those who obtained permission to circumvent the technological measure."[140] Of course, if bnetd had permission, an affirmative defense would be unnecessary.

Second, the court found that the sole purpose of the bnetd's circumvention was not to enable interoperability, but "to avoid the anti-circumvention restrictions of the game and to avoid the restricted access to Battle.net."[141] 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.[142] 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 information bnetd sought was used solely to create a program that interoperated with Blizzard's games. Whether bnetd distributed the resulting

---

136 *Id.* at 636.

137 *Id.*

138 Premising DMCA liability on access to "Battle.net mode" was problematic. Neither the District Court nor the Eight 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.

139 334 F. Supp. 2d at 1183.

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

141 *Id.* at 1186.

142 *Id.* at 1185-86.

program for free or for profit, with closed or open source is of little consequence.

Indeed, only the first of the court's reasons points to any plausible basis to doubt bnetd's purpose.[143] 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 sole purpose was not interoperability but the encouragement of infringement. But the evidence 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.[144] 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 concluded 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.[145] But this functional equivalence simply suggests that bnetd was successful in its attempt to enable interoperability. By counting this fact against bnetd, the court 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 "the resulting product [] be a new and original work, in that it may not infringe the original computer program."[146] 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).[147] 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.

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 since unauthorized copies of Blizzard games could be played on the

---

143 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.

144 *See* Letter from Cindy A. Cohn to Rod Rigole, March 11, 2002, http://www.eff.org/pages/eff-letter-blizzard-vivendi.

145 334 F. Supp. 2d at 1185.

146 S. Rep. No. 105-190, at 32 ("must be a new and original work, in that it does not infringe the original computer program.").

147 334 F. Supp. 2d at 1187.

bnetd server.[148] 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. But if "infringement" referred to § 1201 violations, qualifying for the interoperability defense would be a logical impossibility.

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 rights under § 106. Unless bnetd's reverse 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 *Davidson* district court's struggle to make sense of the basic elements of § 1201(f), coupled with the Eighth Circuit's disinterest in an independent analysis, leaves developers of interoperable technologies in an unenviable position. Aside from the Sixth Circuit's non-binding 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. But judicial misinterpretation explains only part of the failure of § 1201(f). As discussed below, Congress's choice to limit the exemption's scope to computer programs ensures that not all interoperable technologies are insulated 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 non-interoperable products are not privileged under § 1201(f).[149] Nor are researchers who investigate the operation of TPMs, their effectiveness, and their implications for security and privacy.[150]

---

[148] 422 F.3d at 642.

[149] H.R. Rep. No. 105-551 Part II, at 43 ("If a person makes this information available for a purpose other than to achieve interoperability... then such action is a violation of this Act.")

[150] Sections 1201(g) and (j) could apply in some, but not all, such circumstances. 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 (2007).

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."[151] As a result, interoperable products that make use of technologically protected entertainment content or other works are open to attack under the DMCA, regardless of whether or not those products create any additional risk of infringement.

The disparity in the treatment of these two classes of interoperable technologies is the result of two problematic distinctions. First, it 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.

First, 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 illustrates the difficulty 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.[152]

Real obtained a preliminary injunction against Streambox, developers of the VCR, an application that mimicked the secret handshake in order to interoperate with RealServer. The court found that the handshake served as an effective access control, one the VCR circumvented by mimicking RealPlayer.[153] But to what did the handshake control 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. In order to prevent access to RealMedia files, Real simultaneously limited access to the RealServer software.

The *Streambox* litigation also illustrates the second problematic distinction at work in § 1201(f). Because the VCR ignored Real's "Copy Switch," a bit of code that reflected copyright holder preferences about enduser copying, Streambox could have faced difficulty in establishing that interoperability was its sole purpose under

---

[151] H.R. Rep. No. 105-551 Part II, at 33; *see also* Samuelson & Scotchmer, *supra* note 29, at 1635 n.289 (noting that § 1201(f) does not extend to program-to-data interoperability).

[152] RealNetworks, Inc. v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889, *6 (W.D. Wash. Jan. 18, 2000).

[153] *Id.* at *18-19.

§ 1201(f).[154] 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 the RealPlayer and presented precisely the same risk of infringement. Because the handshake restricted access to entertainment content, § 1201(f) would have been unavailable.[155]

The unavailability of § 1201(f) in such circumstances ignores the role of data in enabling interoperable relationships, hampering § 1201(f)'s ability to fully accommodate interoperability.[156] 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 to use the information which has been exchanged"—reflects an undue focus on program-level interoperability.[157] Under Congress's definition, computer programs exhaust the class of potentially interoperable objects. Therefore, access to works other than programs is unnecessary to achieve interoperability. 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. Second, the software industry, the primary proponents of § 1201(f), had finite influence and focused its efforts on maintaining the ability to access other programs for reverse engineering, an ability central to prevailing industry practices. Data interoperability presented a less pressing concern.

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

---

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

[155] Section 1201(f) could be read to permit circumvention of TPMs that simultaneously control access to both entertainment content and the software necessary for its playback. But such a reading is hard to square with the bright line drawn between these two classes of works in the legislative history. Instead, it seems that Congress did not intend to enable the circumvention of controls applied to entertainment content, even if access to those files facilitated interoperability.

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

[157] 17 U.S.C. § 1201(f)(4).

indirectly in a computer in order to bring about a certain result."[158] But 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. First, the interoperability exemption was explicitly intended to preserve *Sega*, which permitted the reverse engineering of video games—works that straddle the line between computer programs and digital entertainment content. Second, files distributed in TPM-restricted formats exhibit program-like characteristics. Those files contain functional instructions distinct from the movies or music they contain—instructions that control the ability of other programs or devices to interoperate.

Ultimately, the distinction between data interoperability and program interoperability cannot justify the stark differences it creates in the scope of DMCA protection between firms that prevent interoperability by restricting access to their programs and those that restrict access to data. 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.[159] Real's competing download service utilized its own Helix technology. Because the only digital rights management ("DRM") technology supported by the iPod is Apple's FairPlay, music purchased from Real could not be transferred to the iPod.[160] 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.[161] Apple declined.[162] 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.[163] Real touted Harmony as a boon for "compatibility, choice, and quality" that "follow[ed] in a well-established tradition of

---

[158] 17 U.S.C. § 101.

[159] *See* Eric Bangeman, *Apple passes Wal-mart, now #1 music retailer in U.S.*, ARS TECHNICA, April 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.

[160] 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.

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

[162] *Id.*

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

fully legal, independently developed" interoperable technologies.[164] Apple responded by accusing Real of "adopt[ing] the tactics and ethics of a hacker to break into the iPod" and threatened both legal action under the DMCA and technological intervention to disrupt Harmony.[165]

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.[166] Nonetheless, Real eventually achieved iPod interoperability. But 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.[167]

Because Apple never filed suit against Real, it never clearly articulated its DMCA theory. Since Harmony did not allow Real customers to access music purchased from iTunes, an allegation that Real trafficked in a tool that enabled unauthorized access to such 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 on basis of the Federal Circuit's nexus requirement. Likewise, a court could have held that users were authorized to access the iPod's software by virtue of purchasing the device. In short, a DMCA theory premised on unauthorized access to the iPod faced substantial difficulties.

Apple's more plausible DMCA claim would have alleged that Real's reverse engineering during the creation of Harmony circumvented FairPlay, resulting in unauthorized access to iTunes music. If such circumvention occurred,[168] *Lexmark* and *Chamberlain* likely would have offered Real little help. As a result, it would have relied on § 1201(f), a defense Real stressed in its response to Apple's threats. Although Real's reverse engineering was intended to enable interoperability between RealPlayer and the iPod, a § 1201(f) defense was unlikely to succeed since FairPlay primarily restricted access to entertainment content.

---

[164] *Id.*

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

[166] John Borland, *Apple fights RealNetworks' 'hacker tactics'*, CNET, Dec. 14, 2004, http://news.cnet.com/2102-1027_3-5490604.html. This response is consistent with Apple's approach to tools like Hymn and Playfair, which enabled users to remove FairPlay DRM from iTunes tracks.

[167] 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.

[168] Real claimed that Harmony was developed using only publicly available information, suggesting that circumvention was unnecessary. Indeed, Harmony may have been created by reverse engineering existing FairPlay circumvention tools.

As Real's struggle to enable interoperability with a system that relied heavily on TPM-protected entertainment content illustrates, the DMCA implicates not only safeguards against potential copyright infringement, but markets for distribution and playback technologies as well. Apple's emerging dominance in both of those markets only underscored the inability of § 1201(f) to contain the risk to interoperability posed by the DMCA. As a result, proponents of interoperability began to turn to other legal theories to restrain the DMCA.

III. ANTITRUST & INTEROPERABILITY

Because the DMCA is ill-equipped to fully address the interference with interoperability it enables, consumers, competitors, and regulators have looked to antitrust 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. Although antitrust remedies—notably, mandatory disclosure of technical information—could facilitate interoperability, antitrust may not offer an ideal set of tools for correcting the DMCA's impact. First, reliance on TPMs to impede interoperability, whether characterized as tying, denial of essential facilities, or refusal to deal, appears unlikely to consistently trigger antitrust enforcement. Second, antitrust typically defers to the scope of legitimately acquired intellectual property rights, rather than second guessing them.[169] Given the breath of the DMCA's protections, antitrust is unlikely to disturb their enforcement.

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 in order to

[169] Reliance on antitrust to enable interoperability has practical implications as well. To the extent 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 value of a robust public domain. *See* Herbert J. Hovenkamp, *Innovation and the Domain of Competition Policy* 16 (forthcoming ALA. L. REV. (2008)), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1091488. 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 Comms. 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 courts 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 Intellectual Property Policy*, 103 COLUM. L. REV. 534, 551-52 (2003) (arguing that the speed of reverse engineering self-help renders it preferable to an antitrust conduct remedy).

enable the development of competing and interoperable products.[170] The cases against Microsoft in the United States 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 APIs.[171] In Europe, Microsoft was required to disclose protocol specifications that enabled interoperability between Windows and work group server operating systems.[172]

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.[173] 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.[174] 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.[175]

Since 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*

---

[170] *See, e.g.*, Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d 1255, 1291 (N.D. Ala. 1998) (granting preliminary injunction requiring the disclosure of technical information), vacated on other grounds, 195 F.3d 1346 (Fed. Cir. 1999); *see also* In the Matter of Xerox Corp., 86 F.T.C. 364 (1975) (requiring licensing of patents and the disclosure of related know-how); In the Matter of Silicon Graphics, Inc., 1995 FTC LEXIS 159 (requiring respondent to port computer games optimized for computing platforms and requiring the publication of APIs for interoperability purposes). 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. Rpt. (BNA) 65 (2003).

[171] 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, 231 F. Supp. 2d 144, 186-195 (approving settlement agreement containing provisions for mandatory disclosure of interoperability information); United States v. Microsoft, 2006 U.S. Dist. LEXIS 76862, *10-11 (D.D.C. Sept. 7, 2007) (Modified Final Judgment).

[172] Commission Decision, COMP/C-3/37.792, Article 5(a) (March 24, 2004); Microsoft Corp., T-201/04, 249 (CFI Sept. 17, 2007)

[173] For a detailed discussion, see 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 Center for Law and Technology (2005), http://works.bepress.com/mazziotti/1.

[174] *See* Conseil de la Concurrence, Decision No. 04-D-54, available at http://www.conseil-concurrence.fr/pdf/avis/04d54.pdf.

[175] *Id.*

Droits Voisins dans la Societe de l'Information ("Dadvsi") to implement the European Copyright Directive and, by extension, the WIPO Copyright Treaty.[176] 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.[177] Dadvsi also created the Regulatory Authority for Technical Measures to hear disputes over TPM interoperability, bypassing the FCA, which had endorsed Apple's DRM strategy.[178]

Apple dubbed the interoperability provisions of Dadvsi "state-sponsored piracy."[179] 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,[180] and his Norwegian counterpart found that iTunes imposed unreasonable terms and conditions on users, in part because of the absence of interoperability with other offerings.[181] Denmark, Finland, Germany, and Sweden also threatened action over Apple's restriction of interoperability.[182]

In the United States, 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 Department of Justice, expressed skepticism about the role of antitrust enforcement in promoting interoperability between Apple's offerings and those of its competitors.[183] Although U.S. antitrust authorities have declined to pursue enforcement actions against Apple, private plaintiffs have not. Three pending class action complaints allege that Apple's refusal to license its FairPlay DRM technology and its unwillingness to support

---

[176] Loi No. 2006-961. For a discussion of the debate leading to the enactment of Dadvsi, see Deana Sobel, *Note, A Bite out of Apple? iTunes, Interoperability, and France's Dadvsi Law,* 22 BERKELEY TECH. L. J. 267 (2007).

[177] Code de la Propriete Intellectuale, Article L. 331-5 and 331-7. 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.*

[178] Dadvsi, Article 14.

[179] Michael Geist, *Compatibility worries fuel battle over iPod law*, TORONTO STAR, April 17, 2006.

[180] Jan Libbenga, *Dutch Consumer Chief puts Apple through the Mill*, REGISTER, Jan. 25, 2007, http://www.theregister.co.uk/2007/01/25/dutch_out_of_tune_with_apple.

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

[182] *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; 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. 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. *Interesting signals from Apple regarding iTunes*, Feb. 8, 2007, http://www.forbrukerombudet.no/index.gan?id=11037506.

[183] Thomas O. Barnett, Interoperability Between Antitrust and Intellectual Property, http://www.usdoj.gov/atr/public/speeches/218316.pdf (Sept. 13, 2006).

competing DRM systems constitute anticompetitive conduct.[184] But as discussed below, there is good reason to doubt whether antitrust provides a reliable tool for curtailing the DMCA's impact on interoperability.

B. Questioning Antitrust Theories

In many respects, Apple is an attractive target for antitrust plaintiffs. It dominates the markets for both portable media players and licensed music downloads, commanding market shares above 70 percent in both sectors.[185] But even assuming that Apple has market power, it is far from clear that its DRM strategy violates U.S. antitrust law. Apple faces three potential antitrust claims: tying, monopolization, and attempted monopolization. The latter two claims could be premised on either essential facilities or more general refusal to deal grounds. As discussed below, all three of these theories face significant hurdles.

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."[186] A *per se* tying claim requires proof of a tie between two separate products offered by a defendant with sufficient economic power in the tying product market to anticompetitively affect a substantial volume of commerce in the tied market.[187]

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 in order to playback digital media. Neither of these scenarios present a tying arrangement in the classical sense. The sale of neither product is conditioned 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, and 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.[188] Tying can occur if a customer

---

[184] Slattery v. Apple, No. 05-0037; Tucker v. Apple, No. 06-04457; Somers v. Apple, No. 07-06507. 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.

[185] *Rhapsody to challenge Apple's iTunes with MP3 download service*, MAIL ONLINE, June 30, 2008, http://www.dailymail.co.uk/sciencetech/article-1030486.

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

[187] *Id.*

[188] *See id.*

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, 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. And iTunes customers who choose a device other than the iPod cannot play purchased music on a portable device. As a result Apple "refuses to accommodate those who prefer one without the other."[189]

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, the second largest digital music retailer, has sold DRM-free mp3 files since 1999.[190] Although eMusic's 3.5 million-track library focuses on independent labels, retailers including Amazon, Real, Napster, Microsoft, and Walmart offer DRM-free downloads from both independent and major labels.[191]

Similarly, the claim that Apple forces iTunes customers to buy an iPod in order 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.[192] Perhaps most importantly, in response to European critics and customers, Apple has replaced a sizable and growing portion of the Fairplay-restricted tracks in the iTunes catalog with DRM-free files that can be played on a host of portable devices.[193]

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.

---

[189] PHILLIP E. AREEDA & HERBERT HOVENKAMP, FUNDAMENTALS OF ANTITRUST LAW § 17.0i.

[190] About eMusic, http://www.emusic.com/about/index.html; eMusic and Yahoo! to Host Exclusive Web-Launch of 'They Might Be Giants' New MP3-Only Album July 19, July 15, 1999, http://docs.yahoo.com/docs/pr/release341.html.

[191] Kenneth Corbin, *Rhapsody Bets DRM-Free Downloads Can Foil iTunes*, INTERNETNEWS.COM, June 30, 2008, http://www.internetnews.com/ec-news/article.php/3756246.

[192] 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.

[193] Jacqui Cheng, *iTunes Plus DRM-free tracks expanding, dropping to 99 cents*, ARS TECHNICA, Oct. 15, 2007, http://arstechnica.com/journals/apple.ars/2007/10/15/itunes-plus-drm-free-tracks-expanding-dropping-to-99-cents.

2. Essential Facilities

Another line of attack against Apple's tight control over interoperability is the characterization of the iPod and iTunes store as facilities essential to potential competitors. 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.[194] Although the essential facilities doctrine developed out of early Supreme Court precedent,[195] the Court has recently cast doubt on its vitality.[196] Commentators have called for the doctrine's abandonment,[197] and even some of its supporters caution against its application to intellectual property.[198]

But assuming the doctrine represents a distinct monopolization theory—as most lower courts do—and that Apple has monopoly power in the relevant markets,[199] the essential facilities theory raises interesting questions. First, what is the essential facility to which Apple controls access? The answer depends on the competitor. 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, and manufacturers that want their devices to play the entire iTunes catalog must be able to decrypt FairPlay-protected tracks. Since Apple has refused to license FairPlay, with one exception,[200] these facilities have been off limits to its competitors.

An "indispensable requirement" of a monopolization claim premised on an essential facilities theory is the unavailability of access to that facility.[201] Here that element appears to be lacking. Online music retailers—including Apple's chief

---

[194] *See* MCI Comms. v. Am. Tel. & Tel. Co., 708 F.2d 1081, 1132-33 (7th Cir. 1982); Alaska Airlines, Inc. v. United Airlines, Inc., 948 F.2d 536, 542 (9th Cir. 1991) ("the 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.").

[195] *See* United States v. Terminal Railroad Ass'n, 224 U.S. 383 (1912); Otter Tail Power Co. v. United States, 410 U.S. 366 (1973).

[196] Trinko, 540 U.S. at 410 (suggesting that the Court has never recognized the doctrine).

[197] *See* Areeda, *supra* note 169; *but see* Brett Frischmann & Spencer Weber Waller, *Revitalizing Essential Facilities*, 75 ANTITRUST L.J. 1 (2008).

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

[199] *See* US v. Grinnell Corp., 384 US at 571 (87% market share is a monopoly); American Tobacco Co. v. United States, 328 US 781, 797 (1946) (more than two thirds of the market is a monopoly).

[200] 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, Motorola & Cingular Launch World's First Mobile Phone with iTunes, Sept. 7, 2005, http://www.apple.com/pr/library/2005/sep/07rokr.html.

[201] Trinko, 540 U.S. at 411 ("where access exists, the doctrine serves no purpose.").

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, in part because studies have demonstrated that protected content is equally vulnerable to widespread infringement.[202] Moreover, since Apple itself sells much of its catalog in an unrestricted format, non-iPod devices can play iTunes content. And since Amazon, Napster, and others offer extensive catalogs of DRM-free content at competitive prices, there is little reason to suspect that device manufacturers are truly dependent on access to iTunes, even if it were denied.

3. Refusal to Deal

A monopolization claim could also be premised on more general refusal to deal grounds. Under this theory, Apple's consistent refusal to license Fairplay to competing device manufacturers and download services constitutes anticompetitive conduct.[203] But courts are generally reluctant to interfere with the long recognized right to unilaterally refuse to deal with competitors.[204] Forced sharing of

---

[202] Tim Anderson, *How Apple is Changing DRM*, GUARDIAN, May 15, 2008, http://www.guardian.co.uk/technology/2008/may/15/drm.apple (claiming FairPlay has no effect on infringement).

[203] Apple's refusal to license FairPlay and the resulting tight integration of the iPod and iTunes could serve a number of pro-competitive 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*, 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 tightly 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* Jason Snell, *Inside Apple TV: what we know and what's new since last year's announcement*, MACWORLD, March 1, 2007 (discussing "the 'it just works' simplicity we've come to expect from Apple."); Julio Ojeda-Zapata, *Verizon's Chocolate phone isn't as sweet as an iPod*, ST. PAUL PIONEER PRESS, ("Apple's hot-selling music players are popular because they're so glitch-free and easy to use. They just work."). 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, April 2008, at 138.

[204] United States v. Colgate & Co., 250 U.S. 300, 307 (1919) (The 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 discretion as to parties with whom he will deal.").

competitively valuable assets may lessen incentives for investment and could lead to collusion among competitors.[205] Mandatory licensing of intellectual property rights presents additional difficulties. The power to exclude is the core of intellectual property rights, so antitrust enforcement that denies a rights holder the ability to exclude competitors is in tension with the intellectual property grant itself.[206] As a result, antitrust interferes with enforcement of IP rights or unilateral refusals to license only under narrowly defined circumstances.[207]

Courts have taken two approaches with respect to the refusal to license patents, both of which 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*.[208] Others have imposed a rebuttable presumption of legality.[209] However, intellectual property rights obtained by fraud or the subject of sham enforcement efforts are the proper focus of antitrust scrutiny.[210] Additionally, scrutiny is appropriate when rights holders rely on IP grants to "facilitate[] monopolization that extends beyond the scope of the intellectual property right itself."[211]

Applied to Apple's reliance on the DMCA to allegedly monopolize the portable player and digital download markets, this framework raises two questions. First, do the protections extended by the DMCA to copyright holders, TPM developers, and their licensees establish intellectual property rights that fall within this framework? And if so, does Apple's refusal to license FairPlay exceed the scope of its statutory rights?

The DMCA, which was enacted under Congress's commerce authority rather than its patent and copyright power, does not confer intellectual property rights in the strictest sense of that term. Nevertheless, it results in powers to exclude others from the use of technologies and content sufficiently similar to traditional intellectual property rights to suggest that the typical antitrust treatment of IP rights should inform analysis of the DMCA.[212]

The scope of the rights created by the DMCA is ambiguous. *Chamberlain* and *Lexmark* suggest that the use of TPMs to restrict interoperability and reduce

---

[205] Trinko 540 U.S. at 408 ("compelling firms to share the source of their advantage is in some tension with the underlying purpose of antitrust law…").

[206] *See* Hovekamp et al., *Unilateral Refusals to License in the U.S.*, in ANTITRUST, PATENTS AND COPYRIGHT: EU AND US PERSPECTIVES 17 (Francois Leveque & Howard Shelanski eds. 2005).

[207] 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 (1985). But no court has yet applied that rationale to a refusal to license intellectual property rights. Hovenkamp et al., *supra* note 206, at 35.

[208] *See* In re Indep. Serv. Orgs. Antitrust Litig., 203 F.3d 1322 (Fed. Cir. 2000).

[209] *See* Data General Corp. v. Grumman Systems Support Corp., 36 F.3d 1147 (1st Cir. 1994).

[210] *See* Walker Process Eqpt., Inc. v. Food Machinery Corp., 382 U.S. 172 (1965).

[211] Hovenkamp *et al.*, *supra* note 206, at 28.

[212] *But see* Chamberlain, 381 F.3d at 1203 ("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.").

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.[213] 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 from the scope of the DMCA. In the end, interference with interoperability, standing alone, is unlikely to place DMCA enforcement efforts beyond the statute's legitimate scope. Ultimately, since antitrust is unable to independently define the legitimate scope of the DMCA, it must defer to the rights created by Congress.

C. Deferring to the Scope of Intellectual Property Rights

Antitrust typically defers to valid exercises of legitimately acquired intellectual property rights. Without this degree of deference, antitrust would risk direct conflict with intellectual property doctrine since the rights to exclude that IP provides with one hand, antitrust could take away with the other. This deference acknowledges that antitrust is not well positioned to second-guess the scope of intellectual property grants established through the legislative process.[214] As one commentator explained, "courts cannot and should not try to use the antitrust laws to rein in what may appear to a judge to be excessive congressional grants of economic power through the intellectual property laws."[215]

This deference, however, does not mean that intellectual property 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 rely on their respective misuse doctrines to limit the extent to which those rights can be leveraged to gain control that exceeds the statutory grant.[216] 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 defined by Congress.[217]

---

[213] *See id.* (noting that Chamberlain did not bring a claim for copyright infringement); Lexmark, 387 F.3d at 548 (finding that the TLP was not protected by copyright and describing the PEP as "purely functional.").

[214] Hovenkamp, *supra* note 169, at 23 ("antitrust 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").

[215] David McGowan, *Innovation, Uncertainty, and Stability in Antitrust Law*, 16 BERKELEY TECH. L. J. 729, 781 (2001).

[216] *See* Burk, *supra* note 88, at 1114-1118.

[217] *See* Mark A. Lemley, *A New Balance Between IP and Antitrust*, 8 SW. J. L. & TRADE AMER. 237 (2007).

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 carefully circumscribe the legitimate bounds of the rights it confers to avoid harms to competition and innovation.[218]

Two cases decided by the European Court of Justice demonstrate the importance of both deference to IP rights and the resulting duty of intellectual property doctrine to appropriately define the limits of its exclusive rights. The *Magill* case arose when three Irish television broadcasters enjoined Magill's publication of a weekly listing of their programming schedules. Irish copyright law provided the broadcasters exclusive rights in their program listings, and each published its own weekly programming guide.[219] 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.[220]

Similarly, *IMS Health* addressed a refusal by IMS to license its "1860 brick structure"—a system for reporting German pharmaceutical sales data—to its competitor NDC.[221] 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.[222] When NDC's predecessor adopted the 1860 brick to distribute its own independently generated data, IMS claimed its copyright was infringed. After IMS obtained an injunction barring NDC from using the 1860 brick, NDC offered to license 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.[223]

The European approach to the relationship between intellectual property and competition law differs in important respects from the deference typical in the

---

[218] *See* Jonathan Zittrain, *The Un-Microsoft Un-Remedy: Law Can Prevent the Problem That It Can't Patch Later*, 31 CONN. L. REV. 1361 (1999) (arguing with respect to potential remedies in the Microsoft antitrust litigation that "the real answer lies 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.").

[219] *See* BBC v. Magill, I.L.R.M. 534 (1990).

[220] Radio Telefis Eireann v. Commission of the European Communities, E.M.L.R. 337 (1995).

[221] IMS Health v. NDC Health, 2004 E.C.R. C-418/01, 4 C.M.L.R. 28.

[222] *Id.*

[223] *Id.*

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 intellectual property rights are determined by individual member states.[224] Reconciliation of national IP regimes with the broader goals of "the free movement of goods" requires occasional subservience of intellectual property rights.[225]

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 free to reconsider existing IP rules. If intellectual property 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.

But perhaps more importantly, *Magill* and *IMS* show what happens when intellectual property fails to adequately account for its potential competitive impact. Although deference ensures greater clarity and more efficient adjudication, intellectual property 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.[226] Likewise, the 1860 brick structure—a system for organizing data—would be protected, if at all, by a patent in the United States.[227] Had the relevant intellectual property 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 appropriately tailor IP rights.[228]

Limits on IP rights, however, do more than avoid conflicts with antitrust law. The primary function of intellectual property is to create incentives for the creation and dissemination of new works. Even in fully competitive markets, the scope of IP

---

[224] *See* Radio Telefis Eireann, E.M.L.R. 337 at 25.

[225] *Id.*

[226] *See* Feist Publications, Inc., v. Rural Telephone Service Co., 499 U.S. 340 (1991).

[227] 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.

[228] 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.").

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.

Returning to the example of TPM-restricted digital music, imagine ten competitors that each offer integrated, non-interoperable systems for the purchase and playback of digital 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 non-interoperability 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. 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 improperly leverage the rights provided by the DMCA.[229] Timothy Armstrong has suggested that courts should more readily draw on fair use principles to create a body of judge-made fair circumvention law.[230] And 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.[231] Each of these proposals has substantial merit and would help address the many unintended consequences of the DMCA. But none specifically target the DMCA's interference with efforts to create unauthorized interoperable technologies. This Part offers a proposal that addresses that narrower concern.

---

[229] *See* Burk, *supra* note 88.

[230] Timothy K. Armstrong, *Fair Circumvention*, 74 BROOK. L. REV. (forthcoming 2008).

[231] 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 (2007).

A. Expanding § 1201(f) Without Undermining § 1201

Section 1201(f) reflects Congress's understanding that interoperability is a 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 non-copyright interests. In its effort to facilitate greater control over access to and copying of works, the DMCA reinforces both legitimate copyright holder interests and concerns entirely divorced from the statutory grant of copyright. In order 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.

In order to preserve the value the DMCA was intended to offer copyright holders while making room for interoperability, two changes are necessary. 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, recognizing the role data plays in enabling system-level interoperability. Second, legitimate copyright interests must be disaggregated from control over playback technologies that impede interoperability.[232] The nexus requirement articulated by the Federal Circuit in *Chamberlain* reflects this need to separate copyright and non-copyright interests in applying the DMCA's anticircumvention provisions. 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). Since the anticircumvention provisions restrict technologies that interact with TPM-

[232] Limiting the ability of TPM-providers to bring suit under the DMCA offers one rough means of separating legitimate copyright interests from efforts to restrict interoperability. *See* 17 U.S.C. § 1203(a) (providing a remedy to "any 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* 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.

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 a 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.

restricted works, a broad § 1201(f) could prove the exception that swallows the rule. If measures protecting copyrighted works could be circumvented to achieve interoperability with any device or program without further constraints, the liability provisions of § 1201 could be stripped of practical effect. 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. 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 copyrighted material Congress intended to bolster.

The current § 1201(f) requires potential circumventors to lawfully obtain a copy of a work, guaranteeing that only those who purchase, rent, or otherwise furnish some consideration in exchange for access are entitled to engage in circumvention.[233] But that requirement alone is insufficient since it does not secure against unauthorized post-sale 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 § 1201 was not intended to enable copyright holders to limit post-sale access to lawfully acquired copies of works.[234] And scholars have criticized the role persistent access controls play in restricting circumvention that may serve the public interest.[235] Nonetheless, copyright holders and TPM providers rely on such controls to restrict post-sale 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. Since users who download films from online rental services, for example, may be unwilling to simply 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. FairPlay, for example, permits users to access protected files on up to five computers, but no more.[236] By helping copyright holders and TPM providers define the bundle of rights consumers acquire, persistent access controls may ultimately

---

[233] *See* 17 U.S.C. § 1201(f)(1).

[234] H.R. Rep. No. 105-551 Part I, at 17-18 ("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 ….")

[235] *See* Reichman et al., *supra* note 231, at 1008-1009.

[236] *See* Apple iTunes Store, http://www.apple.com/itunes/store/music.html.

lead to competition on the basis of 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 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 such restrictions are respected, copyright holders and TPM providers should have no power to tether works to approved software or hardware.[237]

Imagine a TPM applied to digital video rentals that imposes two distinct restraints. First, it prevents access after the expiration of a 30-day rental period. Second, it refuses to allow access by unauthorized portable devices. Suppose device manufacturer wants to enable interoperability with rentals protected by this TPM. To qualify for exemption under the revised § 1201(f), the manufacturer must enforce the 30-day expiration date. Copyright holders would retain their power to define the scope of access, but could not dictate the playback platforms available to endusers.

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

---

[237] 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)(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 which has been exchanged.

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.[238] Where TPMs 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, since that 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.

Second, even if developers have the freedom to unilaterally interoperate 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. Limiting liability under the DMCA to permit unilateral efforts to achieve interoperability would bring anticircumvention's interoperability policy back in line with the treatment of interoperability in intellectual property 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 Congress was inclined to promote, rather than simply tolerate, unilateral interoperability, it could take a second, more active approach that provides disincentives against disruptive strategies. The ability to bring a circumvention or trafficking claim, for example, could be withheld 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 steps are taken to restore interoperability.[239]

Third, any legislative proposal addressing the adverse effects of the DMCA must confront the low likelihood of Congress revisiting the anticircumvention provisions. Several legislative efforts, led by Representatives Boucher and Lofgren,

---

[238] Jacqui Cheng, *If music DRM is dead, the RIAA expects its resurrection*, ARS TECHNICA, May 8, 2008, http://arstechnica.com/news.ars/post/20080508-if-music-drm-is-dead-the-riaa-expects-its-resurrection.html.

[239] 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.

attempted to lessen the DMCA's impact on non-infringing uses of copyrighted works, but failed to overcome the lobbying efforts of the entertainment industry.[240] 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. To the extent copyright holders are threatened by the control TPM-providers and device manufacturers like Apple wield over the pricing, distribution, and playback of digital content, increased freedom to interoperate may be viewed as a means to lessen that control without abandoning DRM altogether.[241] Since 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 enjoyed by copyright holders.

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 circumvention. Unlicensed players may prove easier to hack or 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 complete control over the approval of playback technology.[242] Indeed, since all DRM systems must ultimately allow consumers some degree of access to protected content, they are inherently susceptible to attack.[243] Sometimes this susceptibility is exploited by

---

[240] *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).

[241] *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).

[242] See Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOYOLA L.A. ENTM'T L. REV. 635 (2004).

[243] Bruce Schneier, *The Futility of Digital Copy Prevention*, CRYPTO-GRAM NEWSLETTER, May 15,

sophisticated reverse engineers, other times by enterprising teenagers.[244] Even the most sophisticated TPMs, those termed "unbreakable" by their developers, have fared poorly in the wild.[245]

The DMCA itself is a recognition of the technological weakness of the measures that restrict access and copying of publicly available copyrighted content. Since 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 effectively restrict unauthorized use in the absence of legal sanctions. Since 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). As discussed *supra*, in some circumstances interoperability could prove a net negative in terms of social welfare.[246] A rule that permits interoperability, the objection goes, suffers from uniformity costs unless it successfully separates beneficial interoperability from its harmful counterpart.

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 addressed by the revised § 1201(f)'s separation of copyright and non-copyright interests. By requiring interoperable technologies to adhere to restrictions on access and copying, the defense succeeds in filtering out those instances of interoperability most likely to create harm to copyright interests. As to the second, even assuming that interoperability reduces incentives to such a degree that innovation decreases—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 should not be expected to balance all innovative and creative incentives in isolation. Instead, it should be understood as more modest tool intended to preserve the existing incentive structures of copyright law. Moreover, it should be seen as a single component of the broader interoperability policy of intellectual property law.

2001, at 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.").

244 *See* Alex Eaton-Salners, *DVD Copy Control Association v. Bunner: Freedom of Speech and Trade Secrets*, 19 BERKELEY TECH. L.J. 269, 272 n.25 (describing the involvement of teenager Jon Johansen in the creation of DeCSS).

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

246 *See supra* Part I.B.

To the extent limiting interoperability is necessary to preserve incentives for radical innovation, those restrictions should be—and are— defined within the patent system, not the DMCA's anticircumvention provisions.

The expansion of § 1201(f) would convert the DMCA's treatment of interoperability from an aberration to a cohesive component of intellectual property's interoperability policy. Developers would regain the freedom to unilaterally create interoperable products, but copyright holders would retain the ability to restrict access and copying even within this interoperable environment.

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 that interfere with IP's longstanding tolerance of unauthorized unilateral interoperability. Ironically, this control over interoperability could hamper the further development of the very markets the DMCA was meant 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. And 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 scope of the DMCA offers the best hope for reestablishing the legitimacy of unauthorized interoperability. This approach recognizes the need for IP doctrine to carefully tailor 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. But the use of TPMs will undoubtedly continue in some markets. Their legal reinforcement, however, can and should accommodate the freedom to interoperate.