BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 22 NUMBER 3 SUMMER 2007

TABLE OF CONTENTS

SYMPOSIUM: COPYRIGHT, DIGITAL RIGHTS MANAGEMENT TECHNOLOGY, AND CONSUMER PROTECTION

KEYNOTE ADDRESS: A DIFFERENT PERSPECTIVE ON DRM 971
By Commissioner J. Thomas Rosch

A REVERSE NOTICE AND TAKEDOWN REGIME TO ENABLE PUBLIC INTEREST USES OF TECHNICALLY PROTECTED COPYRIGHTED WORKS 981
By Jerome H. Reichman, Graeme B. Dinwoodie and Pamela Samuelson

NO PLACE LIKE HOME FOR MAKING A COPY: PRIVATE COPYING IN EUROPEAN COPYRIGHT LAW AND CONSUMER LAW 1061
By Natali Helberger and P. Bernt Hugenholtz

ENABLING COPYRIGHT CONSUMERS 1099
By Joseph P. Liu

MAKING ROOM FOR CONSUMERS UNDER THE DMCA 1119
By Niva Elkin-Koren

THE MAGNIFICENCE OF THE DISASTER: RECONSTRUCTING THE SONY BMG ROOTKIT INCIDENT 1157
By Deirdre K. Mulligan and Aaron K. Perzanowski

SUBSCRIBER INFORMATION

The *Berkeley Technology Law Journal* (ISSN 1086-3818), a continuation of the *High Technology Law Journal* effective Volume 11, is edited by the students of the University of California School of Law, Berkeley (Boalt Hall), and published four times each year (March, June, September, January) by the Regents of the University of California, Berkeley, Journal Publications, Boalt Hall School of Law, 313 Boalt Hall, University of California, Berkeley, CA 94720-7200. Application to Mail at Periodicals Postage Rate is Pending at Berkeley, CA 94704-9998, and at additional mailing offices. POSTMASTER: Send address changes to Journal Publications, 313 Boalt Hall, Boalt Hall School of Law, University of California, Berkeley, CA 94720-7200.

Correspondence. Address all correspondence regarding subscriptions, address changes, claims for non-receipt, single copies, advertising, and permission to reprint to Journal Publications Coordinator, 313 Boalt Hall, Boalt Hall School of Law, Berkeley, CA 94720-7200; (510) 643-6600; JournalPublications@law.berkeley.edu. Authors: see section entitled Information for Authors.

Subscriptions. Annual subscriptions are $65.00 for individuals, and $85.00 for organizations. Single issues are $27.00. Please allow two months for receipt of the first issue. Payment may be made by check, international money order, or credit card (MasterCard/Visa). Domestic claims for non-receipt of issues should be made within 90 days of the month of publication; overseas claims should be made within 180 days. Thereafter, the regular back issue rate ($27.00) will be charged for replacement. Overseas delivery is not guaranteed.

Form. The text and citations in the *Journal* conform generally to the UNITED STATES GOVERNMENT PRINTING OFFICE STYLE MANUAL (29th ed. 2000) and to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 18th ed. 2005). Please cite this issue of the *Berkeley Technology Law Journal* as 22 BERKELEY TECH. L.J. ___ (2007).

BTLJ ONLINE

The full text and abstracts of many *Berkeley Technology Law Journal* and *High Technology Law Journal* articles published in previous issues can be found at http://www.btlj.org. Our site also contains a cumulative index, general information about the *Journal*, selected materials related to

KEYNOTE ADDRESS: A DIFFERENT PERSPECTIVE ON DRM*

By Commissioner J. Thomas Rosch†

The timing for this conference is impeccable. The debate over Digital Rights Management—DRM—has reignited in the last six weeks thanks to Steve Jobs, the settlement of the Sony "root kit" case, and the release of Microsoft Vista. I think this public debate is a good thing.

The focus of the debate over DRM—and rightfully so—has been on the scope of copyright. I think I bring a slightly different perspective to DRM as someone who is focused on consumer protection and competition issues. As I look at the digital marketplace, I am not sure the bedrock consumer protection and competition principles that are deeply embedded in the Commission's case law need to be reworked. Yes, there are new problems—the recent *Sony* case is one example. However, I am not yet convinced that there is a need for new solutions in the form of new rules.

My goal today is to explore some of the consumer protection and competition issues with DRM and explain how those issues can be analyzed under existing Commission case law. Many of the issues have arisen in the context of digital music but I think the issues raised by DRM extend to a number of different markets—whether it be digital media and entertainment or the application of DRM in enterprises to secure sensitive or confidential information.

I. CONSUMER PROTECTION

DRM raises three distinct issues in my mind when it comes to the Commission's consumer protection mission. First, there are the disclosure obligations when selling DRM-encrypted materials. Second, there are the obligations to protect privacy, including confidential information about one's employees and customers. Third, there is a growing concern about unwanted software and the potentially harmful effects on consumers' computers. I believe that the Commission's traditional consumer protec-

---

* This speech was originally published on the Federal Trade Commission website at http://www.ftc.gov/speeches/rosch/Rosch-Berkeley-DRM%20Speech-Mar9-2007.pdf.

† Commissioner, Federal Trade Commission. The views stated here are my own and do not necessarily reflect the views of the Commission or other Commissioners. I would like to express my gratitude to Kyle Andeer, Elizabeth Delaney, Serena Viswanathan, and Holly Vedova, my attorney advisors, for their invaluable contributions to this paper.

tion principles, which have served us well in many different areas, apply with equal force to what I will call "consumer media" DRM. Technology has changed the playing field, but not the rules by which individual firms must play.

The Commission's recent settlement with Sony BMG is a good example.[1] In 2005, Sony began shipping compact discs with DRM software. That software did several things. First, it allowed the user to make only a limited number of digital copies and it also prevented consumers from "ripping" the music to common digital formats. Second, the digital music files were compatible with only Sony BMG and Microsoft portable devices—thus, for example, the consumer could not import that music into iTunes and play it on iPod devices. Third, the DRM software was loaded automatically onto a user's computer when the user played or burned a copy of an encrypted CD on that computer. However, the software included cloaking technology—frequently referred to as a "root kit"—that made it hard to remove from the system. At the same time, that technology left the user's computer vulnerable to external attack—in essence, it opened a backdoor for hackers. Finally, consumers had to use Sony's media player to play the music. That player would "phone home" to Sony's servers when a CD was played and it allowed Sony to monitor usage and serve ads.

The settlement focused on Sony's failure to adequately disclose the existence and effects of its DRM software and the unfair nature of Sony's installation practices. I think the case provides an excellent road map for the many consumer protection issues raised by DRM.

First, there is the failure to disclose the material limitations on consumers' use of the CD imposed by Sony's DRM technology. The Commission has long insisted that consumers be given adequate notice of the terms on which goods or services are being made available to them, including any material limitations.[2] Unless otherwise advised, I think consumers have the right to expect that their CDs come without copying limitations, and to expect that the music on those CDs will play on any device.

---

1. *In re Sony BMG Music Entertainment*, FTC File No. 062 3019 (posted for public comment Jan. 30, 2007) (consent decree), *available at* http://www.ftc.gov/os/caselist/0623019/index.htm.

2. *See Thompson Medical Co.*, 104 F.T.C. 648, 842-43 (1984), *aff'd*, 791 F.2d 189 (D.C. Cir.1986) (requiring simultaneous audio and visual disclosure of certain information); *see also* FEDERAL TRADE COMMISSION, FACTS FOR BUSINESS: DOT COM DISCLOSURES (2000), http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html ("If qualifying information is necessary to prevent an advertisement from being misleading, advertisers must present the information clearly and conspicuously.").

This position is not without precedent. Several years ago, when personal digital assistants were being touted as wireless communications devices, the Commission brought actions against the manufacturers of several handheld computers. We alleged the companies failed adequately to disclose that the devices could not actually access the internet wirelessly, unless the consumer also purchased additional equipment and services.[3] Likewise, with DRM, any material limitations of use rights (including, but not limited to, technological limitations such as an inability to use the media on another platform) must be clearly and conspicuously disclosed before a sale of those media is made.

Similarly, Sony did not inform consumers that its mandatory, proprietary media player would collect information from users' computers and use it to serve advertisements. I think consumers have the right to expect to be able to play their CDs on their computers, without being monitored and targeted with marketing. The Commission has challenged this type of conduct by adware purveyors,[4] and the same principles apply here. While this issue is not specific to DRM, it illustrates the potential risks for companies that may be tempted to piggyback marketing or other functions onto their DRM schemes. If piggybacking is material to consumers, and particularly if it is not expected in the context of the device or media, it must be disclosed. As a footnote, online behavioral targeting itself raises the specter of data collection and privacy violations. This is a hot topic that the Commission is closely following.

The third aspect of the *Sony* case that harkens back to established Commission cases is the undisclosed and irreversible downloading of software onto consumers' computers. We are entering a world where DRM may be implemented by way of software, hardware, or both. Regardless of how it is delivered, consumers must know what they are getting before they buy.

The Commission has brought actions against numerous distributors of spyware and adware; a common theme in these cases is that the companies surreptitiously loaded their software and made it difficult or impossible to

---

3. *In re Microsoft Corp.*, Docket No. C-4010 (issued May 17, 2001) (consent order), *available at* http://www.ftc.gov/os/caselist/c4010.htm; *In re Hewlett-Packard Co.*, Docket No. C-4009 (issued May 17, 2001) (consent order), *available at* http://www.ftc.gov/os/caselist/c4009.htm; *In re Palm, Inc.*, Docket No. C-4044 (issued Apr. 17, 2002) (consent order), *available at* http://www.ftc.gov/os/caselist/0023332/index.htm.

4. *In re Zango, Inc. et al.*, FTC File No. 052 3130 (issued Nov. 2, 2006) (consent order), *available at* http://www.ftc.gov/os/caselist/0523130/index.htm; *In re Direct Revenue, LLC et al.*, FTC File No. 052 3131 (issued Feb. 20, 2007) (consent order), *available at* http://www.ftc.gov/os/caselist/0523131/index.htm.

uninstall.[5] Sony's use of a root kit to hide its DRM software was a particularly egregious twist on that practice, made even more troublesome by the security vulnerabilities the software created. In all of these cases, the Commission has made clear that this conduct is unfair and illegal. Companies that employ DRM walk a fine line; obviously they need to ensure the viability of their mechanism in order to effectively protect their copyright. However, imposing it on consumers unilaterally without appropriate notice and consent, especially where it may have unintended effects, is problematic.

The story—at least from a consumer protection standpoint—is slightly different when one looks at the application of DRM technology in what I will call the "enterprise" sector. Here, I'm referring specifically to the use of DRM to authenticate users' rights to documents or information, particularly personal information. We have all heard the stories of the theft or inadvertent disclosure of sensitive information. By controlling access, "enterprise" DRM may be one tool that can be used in this battle to protect personal information and data. But, as we know, no DRM regime is completely hack-proof. It is likely, if not inevitable, that data breaches will occur, even with DRM-protected information.

The Commission has long insisted that when explicit or implicit representations are made to consumers and customers that their privacy will be protected—and those representations are readily found when consumers and customers entrust their confidential personal information to others—failing to make good on these representations amounts to deception under the FTC Act.[6] However, when it comes to protecting confidential personal information, the Commission's jurisprudence does not stop at disclosure requirements. Section 5 of the FTC Act prohibits "unfair," as well as "deceptive" acts and practices. The Commission has held that systemic or systematic shortfalls by custodians in protecting confidential personal information in their possession can be considered an unfair practice.

---

5. *FTC v. Seismic Entertainment Prods. Inc.*, Civ. No. 1:04-CV-00377-JD (D.N.H. Oct. 6, 2004) (complaint), *available at* http://www.ftc.gov/os/caselist/0423142/0423142.htm; *FTC v. Odysseus Marketing, Inc.*, Civ. No. 1:05-CV-00330-SM (D.N.H. Sept. 21, 2005) (complaint), *available at* http://www.ftc.gov/os/caselist/0423205/0423205.htm; *see also Zango* and *Direct Revenue*, *supra* note 4.

6. *FTC v. Toysmart.com, LLC*, Civ. No. 00-11341-RGS (D. Mass. filed Jul. 10, 2000) (complaint), *available at* http://www.ftc.gov/opa/2000/07/toysmart.htm; *In re Eli Lilly and Co.*, Docket No. C-4047 (issued May 8, 2002) (consent order), *available at* http://www.ftc.gov/os/caselist/0123214/0123214.htm; *In re Gateway Learning Corp.*, Docket No. C-4120 (issued Sept. 17, 2004) (consent order), *available at* http://www.ftc.gov/os/caselist/0423047/0423047.htm.

For example, the Commission obtained a $15 million settlement from the data broker ChoicePoint based in part on its unfair practices in failing to secure consumers' personal information, and has brought numerous similar cases.[7] It seems to me that this principle should apply to DRM when, because of a lack of reasonable procedures, a company fails to protect consumers or customers from theft or other misuse of their confidential personal information. In short, as to this use of DRM, I also think longstanding Commission principles and requirements governing liability are applicable.

I believe the Commission has the tools to handle many of the emerging consumer protection issues raised by DRM under its existing statutory authority to prohibit deceptive or unfair practices. The Federal Trade Commission Act has proven very adaptable to changing times. Therefore, at this point, I do not think that we need specific DRM legislation from a consumer protection standpoint. This is not to say, however, that I think the Commission has all the remedial tools it needs to deal with breaches of privacy or other harms attributable to defective DRM. I don't think those tools are adequate. More specifically, for most unfair or deceptive acts or practices, the Commission can and does seek equitable remedies, including consumer redress or disgorgement. In the *Sony* case, for example, consumers were offered refunds and reimbursement to repair any damage to their computers. In reality, however, much of the harm in the *Sony* case and similar cases—restricted use of lawfully purchased music, breaches of privacy, and unwanted intrusion into users' computers—is difficult to quantify monetarily. And, the companies responsible for the harms do not always have ill-gotten gains to disgorge. Consequently, either through Congressional action or through rulemaking action at the Commission, I would like to see the Commission armed with the authority to seek civil penalties in these types of cases.

II. COMPETITION

I would like to turn to some of the antitrust issues implicated by DRM.

---

7. *See United States v. ChoicePoint, Inc.*, Civ. No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006) (settlement), *available at* http://www.ftc.gov/os/caselist/choicepoint/choicepoint.htm; *see also In re CardSystems Solutions, Inc.*, Docket No. C-4168 (Sept. 5, 2006) (consent decree), *available at* http://www.ftc.gov/os/caselist/0523148/0523148.htm; *In re DSW, Inc.*, Docket No. C-4157 (Mar. 7, 2006) (consent decree), *available at* http://www.ftc.gov/os/caselist/0523096/0523096.htm; *In re BJ's Wholesale Club, Inc.*, Docket No. C-4148 (Sept. 20, 2005) (consent decree), *available at* http://www.ftc.gov/os/caselist/0423160/0423160.htm; settlement in *Gateway Learning*, *supra* note 6.

As is so often the case with software, interoperability is front and center in terms of the antitrust issues. Apple, Microsoft, Sony, and others have developed different DRM technologies to encrypt digital content. This has given some comfort to the copyright holders concerned with piracy. However these competing DRM standards limit interoperability—Microsoft's Zune is incompatible with Apple's iTunes. Undeniably, consumers would benefit from increased interoperability in the digital music marketplace—at least in the short term. The lack of interoperability—and Apple's market share—has led some to argue that antitrust should be brought to bear. However, I for one am not sure that antitrust—at least at this point in time—should be used to force these companies to make their products interoperable with their competitors.

Apple has sparked the most controversy largely because of the success of iTunes and iPod. Apple has sold over 90 million iPods since 2001 and over 2 billion songs on its iTunes Music Store—no one else comes close in either market. This success has led some to argue that Apple's tactics violate the antitrust laws.[8] Apple's refusal to license its DRM solution—FairPlay—to third parties and its refusal to use anything but FairPlay has meant that there is limited interoperability between Apple's products and competitors' products. This has made it difficult, if not impossible, for the average consumer—such as myself—to transfer music from iTunes to third party devices. It also means that it is difficult to play music encrypted with third party DRM on an iPod. However, iPod owners are not necessarily locked into iTunes for music—there are a number of other sources, including CDs and sites like eMusic, that do not encrypt their music files.

I do not know enough about the facts to make an assessment one way or the other about these investigations. I would note that there are some interesting parallels with the government's case against Microsoft. Microsoft's monopoly in operating systems was protected, at least in part, by a so-called "applications barrier to entry."[9] Under one theory of that case, Java and Netscape were a threat to Microsoft because those applications

8. For example, a class action complaint brought here in the Northern District of California alleges that Apple's strategy of "tying" the iPod and iTunes violates federal and California antitrust laws. Authorities in Europe are also looking into whether this practice violates their laws. The Norwegian Consumer Ombudsman ruled in January 2007 that Apple's closed system is illegal because the songs sold on iTunes, encoded with Apple's FairPlay DRM, cannot be played on any music device other than an iPod.

9. *United States v. Microsoft*, 253 F.3d 34, 55 (D.C. Cir. 2001). The "applications barrier to entry" was premised on the argument that it was costly and time consuming for independent software developers to write applications for more than one operating system. *Id.* Given the ubiquity of Microsoft's operating system, developers focused their energies on writing applications that would work with Microsoft's operating system. *Id.*

could erode that barrier to entry by making it easier to "port" applications between operating systems. The promise was that the development of these technologies—so called middleware—would allow developers to be agnostic when it came to operating systems. That would allow competing operating systems to flourish—Apple, Linux, and others would no longer be hampered by the "applications barrier to entry."

One could argue that iTunes' lack of interoperability creates a barrier to entry in the digital device market.[10] The iPod has been enormously successful with over 90 million units sold since its introduction several years ago. One theory is that consumers who have invested money in iTunes music for their iPods will be locked into Apple when it is time to replace their devices. They will not go with a competitive device because of the investment in iTunes music. An interesting theory, but one with some flaws—at least today.

For one, the market for these devices is still in its infancy—the market is continuing to grow and it is expected to for some time. In other words, there are still a number of consumers who have not purchased a device. Today there are a number of devices on the market—Toshiba, Microsoft, Sony, SanDisk, and iRiver to name a few. Apple may have the largest installed base today but it is unclear whether that will remain the case in the future. At the time of the government's Microsoft challenge the market was far more developed. Microsoft had an enduring decade-long monopoly in the operating system and there were few alternatives in the marketplace. I think it is too soon to say whether the lion's share of device customers will ultimately be locked into Apple's product. Second, studies suggest that the vast majority of music on iPods today is not purchased from iTunes. Rather, it comes from non-encrypted sources—largely compact discs—that can easily be ported to other devices.

---

10. The Berkman Center for Internet & Society at Harvard Law School has released a paper which describes the potential antitrust problem with Apple's strategy. It argues that:

> [Apple's strategy of making iTunes] exclusively compatible with iPod allows for the generation of noticeable entry barriers in the market of portable players and some barriers in the market of music downloading services. In so doing, this strategy ultimately reinforces Apple's price discrimination scheme, as Apple is able to fine tune prices more precisely to a consumer base that is more tightly linked to both products, and conveys information about intensity of usage or downloads more efficiently.

BERKMAN CENTER FOR INTERNET & SOCIETY, ITUNES: HOW COPYRIGHT, CONTRACT, AND TECHNOLOGY SHAPE THE BUSINESS OF DIGITAL MEDIA—A CASE STUDY 45 (June 15, 2004), *available at* http://cyber.law.harvard.edu/media/itunes.

Some have argued that the various stakeholders should coalesce around a marketplace standard for DRM. The Coral Consortium, Sun's DReaM project, and the Digital Media Project are three examples of ongoing standard-setting efforts in the DRM marketplace. Yet none of these efforts have made much headway on the problem. Standard-setting can be enormously beneficial to consumers. At the same time, some stakeholders are wary of participating in these efforts because they can be manipulated. We have seen that some seek to manipulate the standard-setting process in ways that implicate the antitrust laws and that ultimately may result in supra-competitive prices and/or sub-competitive quality that ultimately hurt consumers. The Commission's recent *Rambus* case is a case in point.[11]

Others have argued that the solution to the DRM question, at least in the music business, is to abandon DRM. The larger debate over DRM is one that is largely driven by the desire of the content providers to control their output (whether it is the entertainment and media companies concerned about piracy or enterprises concerned about the inadvertent disclosure of proprietary or confidential information). The internet has benefits for business and consumers alike but it has also created great uncertainty. Perhaps no market has seen more upheaval than the media markets. While the music labels have seen the greatest change to date, movie studios, television networks, book publishers, and video game publishers are not far behind. Today there are a number of different stakeholders all jockeying for position in the new landscape. The traditional players are trying to hold on to their power in this new medium. Those efforts raise some interesting antitrust questions.

In an open letter posted on Apple's website last month, Steve Jobs stated that his company would enthusiastically support a move away from DRM—at least in the market for digital music.[12] His letter, and the response to it, raise some interesting issues. He pointed the finger at the "Big 4" music labels—Warner Music Group, Sony BMG, EMI and Universal—as the reason Apple encrypts music. When it comes to digital music, the Big 4 have adopted similar strategies. According to Jobs and oth-

11. *In re Rambus Inc.*, Docket No. 9302 (issued Aug. 2, 2006) (opinion of the Commission and final order), *available at* http://www.ftc.gov/opa/2006/08/rambus.shtm. There the respondent engaged in deceptive practices respecting its patents and patent applications during a standard-setting process. *Id.* The result was incorporation of the respondent's intellectual property into two SDRAM standards and the respondent's illegal acquisition of monopoly power in violation of Section 2 of the Sherman Act. *Id.* The Commission imposed a ceiling on the royalties the respondent could exact in those circumstances. *Id.*

12. Steve Jobs, *Thoughts on Music*, APPLE.COM, Feb. 7, 2007, http://www.apple.com/hotnews/thoughtsonmusic.

ers, the music labels will not license their content to online music stores unless those "stores" promise to encrypt their "product" with DRM.

In fall 2005, as the music labels prepared to renegotiate their licenses with Apple, the labels talked publicly about a new "variable" pricing model for digital music. The heads of the labels complained publicly about Apple's standard 99 cent retailing model—a model followed by many other online stores. They wanted Apple to adopt a variable licensing strategy where "superstars" would be higher priced and at the same time music from new and emerging artists would be priced for less than 99 cents.[13] Soon after these public statements, the press reported that the Department of Justice and the New York Attorney General's office had launched independent investigations of the music companies.

I should emphasize that I have no inside knowledge as to the substance or status of these investigations. Press reports at the time suggested that these investigations were focused on possible violations of Section 1 of the Sherman Act by the music companies in the market for digital music downloads. For example, there was speculation that the authorities were looking at possible agreements relating to the prices charged to digital music distributors such as Apple, Microsoft, and Wal-Mart, the use of "most favored nation" clauses in music service contracts, and efforts by the music labels to influence retail prices.[14] If the music labels agreed on the prices they would charge companies like Apple that would be an obvious violation of Section 1. However, an agreement by the labels on a business

13. Edgar Bronfman Jr., speaking at an investor conference in New York, publicly aired the frustrations of music executives with the pricing structure of Apple's iTunes, the world's most successful digital music store. iTunes charges 99 cents a song and $9.99 for an album. Locking the prices at those levels isn't fair, Bronfman said, suggesting that variable pricing would be more equitable. "There's no content in the world that has doesn't have some price flexibility," Bronfman pointed out. "Not all songs are created equal. Not all albums are created equal." Arik Hesseldahl, *Why Apple Won't Up-Charge Downloads*, BUSINESS WEEK ONLINE (Sept. 29, 2005); *see also* Dan Sabbagh, *EMI in Push to Call the Tune with Apple over Pricing of Downloads*, THE TIMES (LONDON), (Nov. 17, 2005) ("Arguments over Apple's pricing have raged in recent months as two other top record companies, Warner Music Group and Sony BMG, have indicated that they want Apple to be more flexible. Only the largest company, Universal Music, part of Vivendi Universal, agrees with Apple that a simple pricing structure will help to develop the market.").

14. *See* Jennifer LeClaire, *Big Four Music Studios Subpoenaed in Digital-Music Pricing Probe*, TECHNEWSWORLD (Dec. 27, 2005); Ed Oswald, *DOJ Investigating Digital Music Prices*, BETANEWS (Mar. 3, 2006); *Feds Probe Online Music Companies: Justice Department Looking For Price Fixing In Burgeoning Industry*, CBS NEWS (Mar. 3, 2006), *available at* http://www.cbsnews.com/stories/2006/03/03/tech/main1366727.shtml?source=search_story.

model—for example, the adoption of a variable pricing scheme—could also violate Section 1. If there were hard core agreements, they might be viewed as horizontal price fixing or market division agreements that are illegal per se under the Sherman Act. By the same token, if and to the extent that uniformity is just the result of rivals monitoring and imitating each other, and there are no "plus" factors, that would probably not be considered illegal under the antitrust case law.

In sum, DRM technology may be relatively new. However, the "pure" consumer protection issues, as well as the antitrust issues, that are implicated are not new. Those who counsel firms involved in developing and/or using that technology will be well advised to be on top of the authorities defining the circumstances in which conduct may be unfair or deceptive or may violate Sections 1 or 2 of the Sherman Act.

A REVERSE NOTICE AND TAKEDOWN REGIME TO ENABLE PUBLIC INTEREST USES OF TECHNICALLY PROTECTED COPYRIGHTED WORKS

By Jerome H. Reichman[†], Graeme B. Dinwoodie[‡] & Pamela Samuelson[‡‡]

TABLE OF CONTENTS

I. **INTRODUCTION** 982

II. **CHECKS AND BALANCES IN THE ISP SAFE HARBORS AND ANTI-CIRCUMVENTION RULES** 988

A. ISP SAFE HARBOR PROVISIONS 989
B. ANTI-CIRCUMVENTION PROVISIONS 995
1. *The Sony Safe Harbor Was the Pre-DMCA Default Rule for Dual-Use Technologies* 996
2. *Technology Developers Criticized the White Paper's Anti-Circumvention Proposal* 1000
3. *Regulating Acts of Circumvention and Public Interest Uses of Technically Protected Works* 1002

III. **SETTING THE STAGE FOR A REVERSE NOTICE AND TAKEDOWN REGIME** 1009

A. THE DISSEMINATION TECHNOLOGY CASES: *NAPSTER*, *AIMSTER*, AND *GROKSTER* 1012
B. IMPLICATIONS FOR PUBLIC INTEREST USES OF TECHNICALLY PROTECTED CONTENT 1019
1. *Facilitating Public Interest User Groups Under Section 512* 1019

---

† Bunyan S. Womble Professor of Law, Duke Law School.

‡ Professor of Law, Chicago-Kent College of Law.

‡‡ Richard M. Sherman Distinguished Professor of Law, University of California, Berkeley School of Law (Boalt Hall).

This Article is based in part on a paper entitled "Digital Copyright: Third Party Liability and The Outer Limits of Protection," which Professor Reichman initially wrote and presented at a SOFTIC conference in Tokyo, Japan, in November 2005. The authors wish to thank Thomas Kearney and Assad Rajani for their valuable research assistance. Professor Reichman also gratefully acknowledges the support of the National Human Genome Research Institute and the Department of Energy (CEER Grant P50 HG003391, Duke University Center of Excellence for ELSI Research).

2. *How Public Interest Uses May Be Frustrated by Section 1201* 1022
C. THE LOCK-OUT TECHNOLOGY CASES: *CHAMBERLAIN*, *LEXMARK*, AND *STORAGETEK* 1024
1. *The Lock-out Technology Cases* 1025
2. *Broader Implications of the Lock-out Technology Cases* 1030
D. THE REVERSE NOTICE AND TAKEDOWN FRAMEWORK 1032
1. *The Basic Concept* 1032
2. *Illustrative Applications* 1034
3. *Other Considerations* 1037

IV. **REVERSE NOTICE AND TAKEDOWN AS A MODE OF IMPLEMENTING ARTICLE 6(4) OF THE EU COPYRIGHT DIRECTIVE** 1039

A. THE UNFULFILLED NORMATIVE COMMITMENT UNDERLYING ARTICLE 6(4) 1040
B. REVERSE NOTICE AND TAKEDOWN AS A MODE OF IMPLEMENTING ARTICLE 6(4) 1045
C. THE RELATIONSHIP BETWEEN REVERSE NOTICE AND TAKEDOWN AND ARTICLE 6(4) 1047
1. *Triggering an Entitlement to Relief* 1047
2. *Encouraging the Proper Role for Voluntary Arrangements* 1049
3. *Ensuring an Effective Ability to Engage in Privileged Uses* 1051
4. *Developing Appropriate Forms of Relief* 1053
D. BROADER PERSPECTIVES AND THE ROLE OF THE COMMISSION 1057

V. **CONCLUSION** 1058

I. INTRODUCTION

The WIPO Copyright Treaty (WCT), concluded in 1996, recognizes "the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information" in updating international copyright norms to respond to challenges arising from advances in information and communications technologies, including global digital networks.[1] The WCT implements this balance by affirming that existing exclusive rights, as well as exceptions to and limitations on those rights, can and should be applied to copyrighted works in

1. WIPO Copyright Treaty, Preamble, Dec. 20, 1996, WIPO Doc. CRNR/DC/94, *available at* http://www.wipo.int/documents/en/diplconf/distrib/pdf/94dc.pdf [hereinafter WCT].

digital forms.[2] Indeed, nations are free "to devise new exceptions and limitations that are appropriate in the digital network environment."[3]

The treaty also calls for nations to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights,"[4] although such rules should not impede acts that are "permitted by law" or otherwise beyond the authority of copyright owners.[5] The treaty gives no guidance, however, about how nations might implement this anti-circumvention norm so as to enable privileged and other public interest uses of copyrighted works.

While the WCT embodies a negotiated balance between copyright owners and users of digital works, the translation of this balance into the domestic laws of the United States (U.S.) and the member states of the European Union (EU) has not been fully successful.[6] When enacting the Digital Millennium Copyright Act (DMCA) of 1998 as the U.S. implementation of the WCT,[7] Congress achieved a reasonable balance of competing interests in its creation of safe harbors from copyright liability for internet service providers (ISPs) and other intermediaries for the infringing acts of others.[8] However, contrary to its apparent intention, Congress failed to achieve a similar balance of interests when establishing new rules forbidding circumvention of technical protection measures (TPMs) used by copyright owners to control access to their works and in regulating the

---

2. *Id.*, arts. 6-8; Agreed Statements Concerning the WIPO Copyright Treaty, statement concerning art. 1(4), Dec. 20, 1996, WIPO Doc. CRNR/DC/96 (published Dec. 23, 1996), *available at* http://www.wipo.int/documents/en/diplconf/distrib/pdf/96dc.pdf [hereinafter Agreed Statements]. The WCT also reflects an international consensus that nations are entitled "to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have been considered acceptable under the Berne Convention." *Id.*, statement concerning art. 10.

3. Agreed Statements, *supra* note 2, statement concerning art. 10.

4. WCT, *supra* note 1, art. 11. *See, e.g.*, Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369, 409-15 (1997) (discussing the evolution of the WCT anti-circumvention provision).

5. WCT, *supra* note 1, art. 11.

6. Maintaining a balance between the interests of copyright owners in having adequate protection for their works and the public in having access to and the freedom to use these works in non-infringing ways has long been a "bedrock principle" of U.S. copyright law and policy. *See, e.g.*, H.R. REP. NO. 105-551, at 18 (1998); Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1196 (Fed. Cir. 2004) (quoting legislative history of the DMCA).

7. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (anti-circumvention rules codified at 17 U.S.C. § 1201).

8. 17 U.S.C. § 512 (2000).

manufacture and distribution of technologies primarily designed or produced to enable circumvention of copyright-protective TPMs.[9]

Although the EU followed the U.S. lead in adopting DMCA-like rules that forbid circumvention and trafficking in circumvention tools,[10] it diverged from the U.S. approach by explicitly requiring member states to fulfill a normative commitment to ensuring that certain public interest uses can be made of technically protected works. Article 6(4) of the EU Copyright Directive provides that member states must take "appropriate measures" to ensure that right holders enable lawful users of copyrighted works to exercise certain exceptions or limitations provided for by national law, even when the works in question are technically protected.[11] Unfortunately, the Directive contains some limits that seemingly undermine this commitment,[12] and like the WCT, it provides little guidance about how member states might achieve this goal. National implementations of this Directive thus far have not, in our judgment, adequately facilitated public interest uses of technically protected content nor fulfilled the normative commitment to parity in the ability to exercise exceptions and limitations.[13]

The resulting imbalance in U.S. and EU member state anti-circumvention rules harms legitimate interests of the public in making fair uses, privileged uses, and other non-infringing uses of copyrighted works (which collectively we deem to be "public interest uses" of copyrighted

---

9. 17 U.S.C. § 1201 (2000). Part II will discuss various limitations on and exceptions to the DMCA anti-circumvention rules, including authorization of the Library of Congress to develop new exceptions and limitations; it will also show that these do not accomplish the needed balance.

10. Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, art. 6, 2001 O.J. (L 167) 10 [hereinafter Copyright Directive]. This Directive is more restrictive than the DMCA in at least two ways. First, it bans all acts of circumvention, not just circumventions of access controls. *Compare id. with* 17 U.S.C. § 1201(a)(1)(A). Second, it lacks a set of built-in exceptions and limitations such as those in the DMCA. *Compare* Copyright Directive, *supra*, art. 6, *with* 17 U.S.C. § 1201(c)-(j).

11. Copyright Directive, *supra* note 10, art. 6(4). We recognize that other commentators have been more skeptical than we are about the will to carry through with this normative commitment. *See, e.g.*, Severine Dusollier, *Exceptions and Technological Measures in the European Copyright Directive of 2001—An Empty Promise*, 34 IIC 62 (2003); INST. FOR INFO. LAW, UNIV. OF AMSTERDAM, STUDY ON THE IMPLEMENTATION AND EFFECT IN MEMBER STATES' LAWS OF DIRECTIVE 2001/29/EC ON THE HARMONISATION OF CERTAIN ASPECTS OF COPYRIGHT AND RELATED RIGHTS IN THE INFORMATION SOCIETY, FINAL REPORT 73 (2007) [hereinafter COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY].

12. *See infra* notes 312-315 and accompanying text.

13. *See id.; see also infra* notes 351-357 and accompanying text.

works).[14] We believe that practical judicial and administrative measures can and should be devised to implement the spirit of the WCT in both the U.S. and EU without reopening the contentious debates that engulfed the process leading up to enactment of the DMCA and the EU Copyright Directive. To this end, we propose adoption of a "reverse notice and takedown" procedure to help achieve some of the balance in anti-circumvention rules that the WCT endorsed, but which implementing legislation has thus far failed to deliver.[15] Under this regime, users would be able to give copyright owners notice of their desire to make public interest uses of technically protected copyrighted works, and right holders would have the responsibility to take down the TPMs or otherwise enable these lawful uses.

We call this a "reverse notice and takedown" process because, in an inversion of the notice and takedown procedure first developed through common law adjudication about ISP liability for wrongful acts of users,[16]

---

14. Numerous commentators have noted the imbalance of the DMCA anti-circumvention rules and their deleterious effects on fair, privileged, and other non-infringing uses of copyrighted works. *See, e.g.*, Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J. L. & TECH. 49 (2006); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354 (1999); Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J. L. & TECH. 41 (2001); Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462 (1997); Jacqueline D. Lipton, *Solving the Digital Piracy Puzzle: Disaggregating Fair Use from the DMCA's Anti-Device Provisions*, 19 HARV. J. L. & TECH. 111 (2005); Tricia J. Sadd, *Fair Use as a Defense Under the Digital Millennium Copyright Act's Anti-Circumvention Provisions*, 10 GEO. MASON L. REV. 321 (2001); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Rules Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999); Jane C. Ginsburg, *The Pros and Cons of Strengthening Intellectual Property Protection: Technological Protection Measures and Section 1201 of the U.S. Copyright Act*, (Columbia Law Sch. Pub. Law & Legal Theory Working Paper Group, Paper No. 07-137, Feb. 1, 2007), *available at* http://ssrn.com/abstract=960724.

The imbalance in the DMCA rules is at least partly attributable to the entertainment industry's success in analogizing the bypassing of TPMs to "breaking and entering" someone's home. *See, e.g.*, *WIPO Copyright Treaties Implementation Act and On-Line Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2180, Hearings Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. (1997) (testimony of Robert W. Holleyman II, President, Business Software Alliance) ("H.R. 2281 makes illegal the act of circumvention . . . in the same way that criminal laws make illegal the act of breaking and entering into a home or warehouse.").

15. *See infra* Sections III.B-C.

16. Religious Tech. Ctr. (RTC) v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995). *Netcom* opined that internet access and service providers

it is the user who will be giving notice and the content owner who will have a responsibility to take something down. A reverse notice and takedown regime would achieve for the anti-circumvention rules a comparable symmetry to the balance embedded in the ISP safe harbor rules. It would also effectuate the nascent, but not fully realized, legislative intent to permit public interest uses of technically protected digital content, while at the same time protecting copyright owners against circumvention of TPMs that would facilitate or lead to massive infringements.[17]

The Article will demonstrate that a reverse notice and takedown mechanism is best understood as a principle capable of numerous implementations. In the U.S., the most likely way to achieve this goal is through judicial interpretation of the anti-circumvention rules through case by case adjudication. It was, after all, the judicial branch that introduced the fair use doctrine into U.S. law and also pioneered the notice and takedown rules to govern ISP liability. In the heated political climate in which the DMCA was enacted, the measured analysis developed in *Netcom* was invaluable in shaping ISP liability rules. Unfortunately, no similarly careful judicial assessment was available in the late 1990's to guide Congress about how to achieve an appropriate balance in the anti-circumvention rules. We believe that courts in the U.S. can and should be enlisted in bringing about a balanced approach for dual-use circumvention technologies akin to that developed for the dual-use technologies and services of ISPs. Recent decisions, moreover, provide a theoretical base upon which this case law evolution could occur.

In the EU, by contrast, member states could implement a reverse notice and takedown regime in the course of fulfilling their obligations under the Copyright Directive, including Article 6(4), which requires them to

---

were not liable for user infringements unless and until they had received notice about the existence of infringing materials on their sites and failed to investigate and take infringing materials down. *Id.* at 1373-76. (The *Netcom* decision is discussed *infra* notes 36-42 and accompanying text.) This notice and takedown approach was later legislatively adopted in the U.S. and EU. Three of the four DMCA safe harbors for ISPs, for example, employ the judicially devised notice and takedown framework set forth in *Netcom*. *See* 17 U.S.C. § 512(b)-(d). (The fourth, section 512(a), creates a safe harbor for copies made in the course of transitory digital network transmissions for which notice and takedown is infeasible.) *See also* Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce in the Internal Market (Directive on Electronic Commerce), arts. 12-14, 2000 O.J. (L 178) 1, *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_178/l_17820000717en00010016.pdf [hereinafter E-Commerce Directive]. For a discussion of this Directive and a comparison with U.S. law, *see* Rosa Julia-Barcelo, *On-line Intermediary Liability Issues Comparing E.U. and U.S. Legal Frameworks,* 22 EUR. INTELL. PROP. REV. 105 (2000).

17. This proposal is developed in Section III.D.

ensure that users of technically protected works can exercise certain public interest exceptions. Although it is not possible in either the U.S. or the EU to write anti-circumvention rules on a completely blank slate, there is flexibility in the legal cultures of both entities to implement a reverse notice and takedown procedure to achieve needed balance in anti-circumvention regulations. Nations that have yet to implement the WCT may find our proposed reverse notice and takedown regime provides a far more balanced way to comply with the treaty than the approach being promoted by U.S. trade negotiators.[18]

Part II of this Article discusses the legislative history of the DMCA and the checks and balances embodied in its ISP safe harbor and anti-circumvention rules. It shows that the notice and takedown regime under section 512 has achieved a reasonable balance in the regulation of ISPs for wrongful acts of users, but that section 1201 lacks a similar balance. Certain caselaw interpretations of section 1201 have, moreover, made the DMCA anti-circumvention rules seem even more imbalanced than its express provisions require.[19]

Part III argues that a reverse notice and takedown regime would provide a needed balance in the U.S. anti-circumvention rules and shows that there is sufficient flexibility in the existing U.S. legal framework for courts to fashion such a regime. Part IV argues that member states of the EU should likewise consider adopting a reverse notice and takedown regime as a sound way to effectuate the duty that the Copyright Directive imposes on them to ensure that users are able to enjoy copyright exceptions and limitations that have been granted under national laws, notwithstanding the use of TPMs to control access to and uses of copyrighted works.[20]

Because the EU imposed this duty, yet deferred to national judgments about how to fulfill it, EU member states would seem to have more flexibility to experiment with different ways to implement a reverse notice and takedown regime than the U.S. presently does. Part IV discusses some of the available options.

---

18. *See, e.g.*, Anupam Chander, *Exporting DMCA Lock-outs*, 54 CLEV. ST. L. REV. 205 (2006) (discussing imbalanced anti-circumvention rules that the U.S. has insisted on in trade agreements with several nations).

19. *See, e.g.*, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 324 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

20. Copyright Directive, *supra* note 10, art. 6(4).

II. CHECKS AND BALANCES IN THE ISP SAFE HARBORS AND ANTI-CIRCUMVENTION RULES

The WCT was the end product of an international conversation about updating copyright laws for the digital age that began when the Clinton Administration published its "White Paper" on Intellectual Property and the National Information Infrastructure in September 1995.[21] No checks and balances were built into that document. Among other things, the White Paper opined that internet service and access providers were and should be strictly liable for copyright infringement of their users on account of the temporary copies made in the random access memory of their computers.[22] ISPs were, in the White Paper's view, in a far better position to monitor and control user infringements than copyright owners.[23] The prospect of liability would give them strong incentives to ensure that their sites were not used for infringing purposes and to develop technologies to deter infringements.[24]

The White Paper also recommended legislation to outlaw technologies the primary purpose or effect of which was to bypass TPMs that copyright owners used to protect their works.[25] Without such protection, the drafters warned, copyright owners would not be willing to make their works available in digital form. The White Paper contemplated no public policy exceptions to or limitations on the proposed anti-circumvention rules, a strategy that generated considerable opposition and criticism.[26] This Sec-

---

21. *See* WORKING GROUP ON INTELLECTUAL PROP. RIGHTS, INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE (1995), *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf [hereinafter White Paper]. Imbalance in the White Paper's interpretation of digital copyright issues was widely noted at the time. *See, e.g.*, Peter Jaszi, *Caught in the Net of Copyright*, 75 OR. L. REV. 19 (1996); Leslie A. Kurtz, *Copyright and the National Information Infrastructure in the United States*, 18 EUR. INTELL. PROP. REV. 120 (1996); Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29 (1994); Charles McManis, *International Intellectual Property Protection and Emerging Computer Technology: Taking TRIPS on the Information Superhighway*, 41 VILL. L. REV. 207 (1996); Pamela Samuelson, *The Copyright Grab*, 4.01 WIRED 96 (1996).

22. White Paper, *supra* note 21, at 114-24. The White Paper analyzed ISP liability based on temporary copies made in random access memory of computers as direct infringements of copyright. The White Paper discussed contributory and vicarious liability in a different section. *Id.* at 109-14.

23. *Id.* at 117.

24. *Id.* at 117-18.

25. *Id.* at 230-34.

26. *See, e.g.*, JESSICA LITMAN, DIGITAL COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET 122-65 (2001) (discussing the controversy). *See also supra* note 21.

tion will discuss the different ways that Congress responded to criticisms of the White Paper's proposed ISP and anti-circumvention liability rules.

A. ISP Safe Harbor Provisions

Congress had already begun to consider whether ISPs should be liable for wrongful acts of their users, such as libelous postings on bulletin board services, at the time the White Paper was published.[27] In 1996, as part of a telecommunications regulation reform measure, the telecom industry got a broad grant of immunity from liability for user wrongs.[28] The industry successfully argued that imposing liability on ISPs for wrongful acts of which they were unaware was unfair and unwise. Requiring them to monitor their sites for wrongful activity would not only interfere with user privacy and freedom of expression interests, but it would also increase dramatically the cost of internet access.

Self-regulation was deemed a more effective way to create incentives for ISPs to ensure that their sites were being used for lawful purposes.[29] At the copyright industry's insistence, Congress carved out an exception to the Communications Decency Act's (CDA) immunity provision for intellectual property violations.[30]

---

27. The ISP immunity provision was first introduced in Congress on Aug. 4, 1995. *See* 141 CONG. REC. H8468-69 (daily ed. Aug. 4, 1995). Prior to this, the caselaw on ISP liability for tortious acts of users was mixed. *Compare* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (rejecting a defamation claim against CompuServe because it did not monitor user postings) *with* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995) (refusing to dismiss a lawsuit similar to *Cubby* because, by monitoring some user postings for harmful speech, Prodigy had shown it could monitor for defamation as well). The telecommunications industry became concerned that it would routinely be held liable for wrongful acts of users insofar as it policed its sites for any reason. The telecom industry lobbied hard for Congressional preemption of decisions such as *Stratton Oakmont*. The House Conference report makes clear that "[o]ne of the specific purposes of [the immunity provision] is to overrule . . . decisions which have treated such providers and users as publishers or speakers of content that is not their own." H.R. REP. NO. 104-458, at 94 (1996) (Conf. Rep.).

28. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56. Title V of this Act was the Communications Decency Act. The immunity provision is now codified at 47 U.S.C. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information provider.").

29. The rationale for this grant of immunity is discussed in *Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997).

30. 47 U.S.C. § 230(e)(2). The Ninth Circuit has recently ruled that this limitation on CDA immunity applies only to federal intellectual property laws. *See* Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 768 (9th Cir. 2007) (applying CDA immunity provision to state right of publicity claims).

Having won a broad grant of immunity in the first round of the fight over ISP liability for wrongful acts of users, the telecom industry believed that, by advancing the same arguments used to gain immunity under the CDA, it could persuade Congress to reject the White Paper's contention that that industry should be held strictly liable for copyright infringements.[31] ISP technology platforms were, moreover, "dual-use" technologies, in the sense that they could be as easily used for lawful as for unlawful purposes. Under the Supreme Court's decision in *Sony Corp. of America v. Universal City Studios, Inc.*, ISP platform technologies seemed to qualify for the safe harbor that *Sony* carved out for technologies having substantial non-infringing uses.[32]

The telecom industry's chances for averting the strict liability rule proposed in the White Paper were substantially enhanced by two pre-DMCA developments. One was the *Netcom* decision, which rejected the White Paper's strict liability theory against ISPs.[33] A second was an international repudiation of a similar proposed strict liability rule for internet intermediaries that the U.S. had initially supported at the diplomatic conference that produced the WCT.[34] An Agreed Statement on the treaty further clarified that "mere provision of physical facilities for enabling or making a communication does not in itself amount to communication" under the treaty.[35] ISPs could accordingly point to the international consensus against a strict liability rule when arguing for a more balanced approach before Congress.

The *Netcom* decision was a pivotal development in the legislative drama that spawned the DMCA safe harbors.[36] In response to the copyright owner's direct infringement claim against Netcom, the alleged infringer's Internet access provider, Judge Whyte identified the question in

---

31. *See supra* text accompanying note 29 for the rationale for the CDA immunity.

32. Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 442 (1984).

33. Religious Tech. Ctr. (RTC) v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1370 (N.D. Cal. 1995).

34. The Clinton Administration had supported a draft treaty provision under which ISPs would have been strictly liable for temporary copies of infringing materials passing through their computers. *See* Samuelson, *supra* note 4, at 383-92 (discussing debate over ISP liability at the WIPO diplomatic conference).

35. Agreed Statements, *supra* note 2, statement concerning art. 8.

36. *RTC*, 907 F. Supp. at 1364-66. Litigation ensued after Dennis Erlich, a former minister of the Scientology religion turned vocal critic, posted portions of the writings of L. Ron Hubbard in the alt.religion.scientology Usenet newsgroup. RTC, owner of the relevant copyrights, sued Erlich, Thomas Klemesrud (the operator of a bulletin board service (BBS) on which Erlich had made the postings), and Netcom (the Internet access provider for Klemesrud's BBS), for copyright infringement. *Id.* at 1366.

the case as "whether possessors of computers are liable for incidental copies automatically made on their computers using their software as part of a process initiated by a third party."[37] Judge Whyte decided that RTC's direct infringement theory was an unreasonable interpretation of copyright law because it would logically lead to imposing liability on owners of "every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer."[38] Before an Internet access provider could become directly liable, there needed to be proof of "some element of volition or causation," proof "which is lacking where a defendant's system is merely used to create a copy for a third party."[39]

Although Judge Whyte also agreed with Netcom that it should not be held contributorily liable for Erlich's infringement before receiving notice about this risk, he took issue with Netcom's assertion that RTC's notice of Erlich's infringement was "too equivocal given the difficulty in assessing whether registrations are valid and whether a use is fair."[40] While "a mere unsupported allegation of infringement by a copyright owner may not automatically put a defendant on notice of infringing activity," Judge Whyte declared, "Netcom's position that liability must be unequivocal is unsupportable."[41] Upon receipt of a proper notice, Judge Whyte thought that Netcom should have a duty to investigate the claim of infringement and to take the material down if the claim was valid. Failure to do so

---

37. *Id.* at 1368. In support of its direct infringement claim, RTC relied upon the White Paper; the Ninth Circuit's decision in *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), which held that temporary copies of copyrighted works made in the random access memory of computers were infringing reproductions of the works unless authorized by the copyright owner or the law, *id.* at 518; and *Playboy v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993), which held the operator of a BBS directly liable for infringing copies of Playboy bunny pictures that users had uploaded to and downloaded from the BBS. The White Paper had also relied upon *MAI* in support of its view that making temporary as well as permanent copies of works in digital form were copyright-significant acts and upon *Frena* in support of its view that ISPs were directly liable for user infringements. *See* White Paper, *supra* note 21, at 64-69, 120.

38. *RTC*, 907 F. Supp. at 1369.

39. *Id.* at 1370. Judge Whyte also granted Netcom's motion for summary judgment on RTC's vicarious liability claim. Although the judge was skeptical of Netcom's claim that it lacked the ability to supervise and control users' postings, the vicarious claim was unsustainable because Netcom had not received any direct financial benefit from user infringements. *Id.* at 1375-77.

40. *Id.* at 1373. "To require proof of valid registration would be impractical and would perhaps take too long to verify, making it impossible for a copyright holder to protect his or her works in some cases. . . ." *Id.*

41. *Id.* at 1374.

amounted to a substantial contribution to user infringement that, if proven, would justify contributory infringement liability.[42]

Two of the DMCA safe harbors are codifications of the *Netcom* ruling: section 512(a) exempts service providers from liability for incidental copies made in the course of network transmission of digital content on behalf of users;[43] and section 512(c) exempts copies made in storing information for users except when providers have received proper notice of infringement from the copyright owner and failed to investigate the charges and remove infringing materials.[44] Congress also created safe harbors for caching of digital content to enable faster service to users and for information locating tools (e.g., search engines) that might connect users to infringing materials.[45] The information storage, caching, and information location tool safe harbors have notice and takedown requirements akin to those articulated in *Netcom*.[46]

The DMCA safe harbors represented a major victory for telecom and internet industry groups, given that powerful copyright industry groups had wanted service providers held strictly liable for infringing acts of users. Other legislative concessions to ISPs included: a specification of what constitutes adequate notice from copyright owners before the duty to investigate arises;[47] a counter-notice regime so that users can ask to restore information initially taken down in response to a complaint of infringe-

---

42. *Id.* at 1374-75. There being a triable issue of fact on the adequacy of RTC's notice to Netcom and the reasonableness of Netcom's response, the latter's motion for summary judgment on the contributory infringement claim failed. *Id.* The White Paper had not considered a notice and takedown regime as a way to balance competing interests in ISP liability cases.

43. 17 U.S.C. § 512(a).

44. *Id.* at § 512(c).

45. *Id.* at § 512(b) (caching safe harbor), § 512(d) (information location tool safe harbor). As mentioned above, the EU found notice and takedown to be a balanced approach to ISP liability in its E-Commerce Directive, which, like the DMCA, provides a safe harbor for transmission, caching, and information storage. It has no counterpart, however, to section 512(d). E-Commerce Directive, *supra* note 16, arts. 12-14.

46. 17 U.S.C. §§ 512(b)(2)(E)(i), (c)(1)(A), (d)(1)(A).

47. *Id.* at § 512(c)(3). The Ninth Circuit gave this requirement some teeth in a recent secondary liability case:

> In order to substantially comply with sec. 512(c)(3)'s requirements, a notification must do more than identify infringing files. The DMCA requires a complainant to declare, under penalty of perjury . . . that he has a good faith belief that the use is infringing.. . . Permitting a copyright holder to cobble together adequate notice from separately defective notices . . . unduly burdens service providers.

Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 761-62 (9th Cir. 2007).

ment;[48] an immunity for taking information down based on a good faith belief that such action was proper;[49] limitations on injunctive relief;[50] and a clarification that service providers were not obliged to monitor their sites for infringing materials.[51]

Copyright industry groups obtained some concessions as well. ISPs could rely on the safe harbors only if they had adopted and reasonably implemented policies to terminate repeat infringers, and if they accommodated standard technical measures that might be developed in the future for the protection of digital copyrighted works.[52] ISPs were obliged to publicly designate an agent to whom notices of infringement could be sent.[53] The DMCA also authorized copyright owners to seek subpoenas to require service providers to disclose names and other identifying information about ISP subscribers whom copyright owners alleged were infringers.[54]

The DMCA safe harbors have generally been efficacious in run-of-the-mill copyright infringement cases involving users and their ISPs.[55] Copyright owners have incentives to monitor Internet sites for infringing materials and to provide appropriately detailed information to ISPs so that the infringing material can be taken down. Copyright owners are deterred from sending false or overreaching notices of infringement not only by provisions of the DMCA that penalize wrongful notices,[56] but also by the prospect of "bad" publicity and judicial sanctions if they send improper or

48. 17 U.S.C. § 512 (g)(2)-(3).

49. *Id.* at § 512(g)(1).

50. *Id.* at § 512(j)(1)-(2).

51. *Id.* at § 512(m).

52. *Id.* at § 512(i). *See Perfect 10, Inc.*, 481 F.3d at 758-64 (discussing the reasonable implementation requirement).

53. 17 U.S.C. § 512(c)(2).

54. *Id.* at § 512(h). *But see* Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) (holding RIAA not authorized to obtain subpoena identifying information as to file-sharers whose communications Verizon transmitted; section 512(h) allows subpoenas as to section 512(c) storage of information, not as to section 512(a) transmissions of information).

55. *See, e.g.*, Christian C.M. Beams, *Note: The Copyright Dilemma Involving Online Service Providers: Problem Solved . . . For Now*, 51 FED. COMM. L.J. 823, 846 (1999); Heidi Pearlman Salow, *Liability Immunity for Internet Service Providers—How Is It Working?*, 6 J. TECH. L. & POL'Y 31, 49-50 (2001).

56. 17 U.S.C. § 512(f). This provision has some teeth, as is illustrated by *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004) (sanctioning electronic voting technology firm for knowing misrepresentations when giving notice to an ISP to take down allegedly infringing materials).

overreaching notices.[57] ISPs have incentives to cooperate with copyright owners in the notice and takedown process and to terminate repeat infringers lest they forfeit the safe harbors provided by the DMCA.

While there is some empirical evidence that ISPs are perhaps quicker than they should be to take materials down upon receipt of notice and that the counter-notice procedures are too rarely invoked,[58] ISPs and copyright owners have generally adapted to conducting businesses within the framework of the notice and takedown regime of the DMCA safe harbors.[59] Viacom's pending copyright infringement lawsuit against YouTube will test how secure the DMCA safe harbors really are,[60] but it will not be surprising if the court tells Viacom that it should take its complaint to Congress, as Viacom is essentially trying to achieve through litigation what the copyright industry was unable to obtain from Congress in 1998.[61] Leaving aside the Viacom lawsuit, the past decade of experience with the DMCA notice and takedown regime suggests that a relatively balanced and workable solution to this particular dual-use technology problem has been found.[62]

---

57. *See, e.g.*, Free Speech Battle Over Online Parody of 'Colbert Report,' http://www.eff.org/news/archives/2007_03.php#005176 (Mar. 22, 2007) (challenging Viacom notice and takedown demand as to parody available on YouTube).

58. *See, e.g.*, Jennifer Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621 (2006). For examples of notice and takedown letters that have had chilling effects on users, see http://chillingeffects.org/copyright/.

59. *See, e.g.*, Kevin M. Lemley, *Comment: Protecting Consumers From Themselves: Alleviating the Market Inequalities Created by Online Copyright Infringement in the Entertainment Industry*, 13 ALB. L.J. SCI. & TECH. 613, 620 (2003).

60. *See* Complaint, Viacom Int'l, Inc. v. YouTube, Inc., No. 07 Civ. 2103 (S.D.N.Y. Mar. 12, 2007). For contrasting perspectives on this lawsuit, *see, e.g.*, Lawrence Lessig, Op-Ed, *Make Way for Copyright Chaos*, N.Y. TIMES, Mar. 18, 2007, at sec. 4, page 12, *available at* http://www.nytimes.com/2007/03/18/opinion/18lessig.html?ex=1182139200&en=41732111a3c5e994&ei=5070; Douglas G. Lichtman, *The Case Against YouTube*, L.A. TIMES, Mar. 20, 2007, at A19, *available at* http://www.latimes.com/news/opinion/la-oe-lichtman20mar20,0,7632194.story.

61. *See, e.g.*, CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544 (4th. Cir. 2004) (rejecting copyright owner arguments for intermediary liability as having been resolved by DMCA safe harbors).

62. *See, e.g.*, Beams, *supra* note 55, at 841; Tim Wu, *Does YouTube Really Have Legal Problems?*, SLATE, Oct. 26, 2006, http://www.slate.com/id/2152264/ (arguing that "the content industry actually likes section 512 more than anyone will admit"). *See also* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 397 (2005) (praising the balance of the notice and takedown rules).

B. Anti-circumvention Provisions

In addition to endorsing a strict liability rule against ISPs, the White Paper anticipated that many copyright owners would find it desirable to use technical protection measures (TPMs) for digital media products or services intended for distribution via global digital networks; yet, it also recognized that clever technologists could build tools to bypass these TPMs, which would thereby render digital works vulnerable to infringements.[63] To offer greater security to technically protected content, the White Paper recommended enactment of a ban on technologies, "the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent" technical measures used by copyright owners to protect their works.[64]

The White Paper offered very little policy analysis in support of this ban.[65] It dismissed as misguided expressions of concern about the effects of anti-circumvention rules on the public domain and on fair and other privileged uses of copyrighted works.[66] Clinton Administration officials also proposed that a virtually identical provision should be included in the WCT.[67]

---

63. White Paper, *supra* note 21, at 230.

64. The White Paper's proposal was:

> No person shall import, manufacture or distribute any device, product, or component incorporated into a device or product, or to offer or perform a service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without authority of the copyright owner or the law, any process, treatment, mechanism, or system which prevents or inhibits the exercise of any of the exclusive rights under section 106.

Id., Appendix 1 at 6.

65. The White Paper did state:

> The Working Group finds that prohibition of devices, products, components, and services that defeat technological methods of preventing unauthorized use is in the public interest and furthers the Constitutional purpose of copyright laws. Consumers of copyrighted works pay for the acts of infringers; copyright owners have suggested that the price of legitimate copies of copyrighted works may be higher due to infringement losses suffered by copyright owners. The public will also have access to more copyrighted works if they are not vulnerable to the defeat of copy protection systems.

Id. at 230.

66. *Id.* at 231-32.

67. *See* Samuelson, *supra* note 4, at 409-15 (discussing proposed WIPO treaty anti-circumvention provision).

1. *The Sony Safe Harbor Was the Pre-DMCA Default Rule for Dual-Use Technologies*

The radical nature of the White Paper's proposed anti-circumvention rule can best be appreciated by contrasting it with the safe harbor for technologies with substantial non-infringing uses set forth in *Sony Corp. of America v. Universal City Studios, Inc.*[68] *Sony* was the first case to consider whether copyright owners could hold technology developers indirectly liable for user infringements on the ground that the primary purpose or effect of the challenged technologies was to facilitate unauthorized copying of copyrighted works.[69]

Universal sued Sony for contributory infringement in 1976, shortly after Sony introduced the Betamax video tape recorder (VTR) to the market, claiming that Sony knew that the primary use of its Betamax machines would be to make unauthorized, and hence infringing, copies of copyrighted works, such as movies shown on broadcast television.[70] Indeed, Sony's advertisements encouraged the public to purchase its VTRs in order to copy favorite programs.[71] In 1981, the Ninth Circuit Court of Appeals ruled in Universal's favor, on the grounds that making copies of copyrighted television programs, even for time-shifting purposes, was direct infringement, and that Sony had knowingly contributed to that infringement because the primary use of Betamax machines was to make such copies.[72] In 1984, the Supreme Court reversed, holding that time-shift copying of TV programs was fair use and that Sony was not liable for contributory infringement on account of the substantial non-infringing uses to which the Betamax machines could be put.[73]

Justice Stevens, writing for the Court in *Sony*, observed that the only theory on which Sony could be held liable was "that [it has sold] equipment with constructive knowledge that its customers may use that equip-

---

68. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984). The White Paper did not mention that its anti-circumvention rule would partially overturn the *Sony* safe harbor for technologies with substantial non-infringing uses. The White Paper mischaracterized *Sony* as a case in which the absence of a market for home-taping had led the Court to conclude that time-shift copying of television programs was fair use. White Paper, *supra* note 21, at 79.

69. For a well told history of the lawsuit, *see generally* JAMES LARDNER, FAST FORWARD: A MACHINE AND THE COMMOTION IT CAUSED (rev. ed. 2002).

70. *Sony*, 464 U.S. at 459.

71. *Id.*

72. Universal City Studios, Inc. v. Sony Corp. of Am., 659 F.2d 963, 971-72 (9th Cir. 1981).

73. *Sony*, 464 U.S. at 447-56.

ment to make unauthorized copies of copyrighted material."[74] There was, however, "no precedent for imposition of [secondary] liability on such a theory,"[75] nor any basis in the copyright statute.[76] Holding Sony liable on this theory was unwarranted, moreover, because of the significant effects it would have on other parties, including copyright owners who approved of time-shift copying of their programs by Betamax users, members of the public who wanted access to such technologies to make authorized and fair uses of them, and of course, Sony and other technology developers who wanted to make and sell these technologies.[77] "When a charge of contributory infringement is predicated entirely on the sale of an article in commerce that is used by the purchaser to infringe [an intellectual property right], the public interest in access to that article is necessarily implicated."[78]

Sony recognized that Congress had resolved a similar tension in patent law by imposing contributory liability on technology developers only when they made and sold devices that had been "especially made or especially adapted for use in an infringement of . . . a patent."[79] Congress had created a statutory safe harbor from contributory liability for dual-use technologies, that is, for "staple articles of commerce," which applies to technologies "suitable for substantial non-infringing use."[80] This safe harbor recognized a legitimate public interest in having the ability to access and enjoy staple articles for their non-infringing purposes.

---

74. *Id.* at 439.

75. *Id.*

76. Justice Stevens pointed out that U.S. copyright law "does not expressly render anyone liable for infringement committed by another." *Id.* at 434. Universal argued that "*Kalem* [*Co. v. Harper Bros.*, 222 U.S. 55 (1911)] stands for the proposition that supplying the 'means' to accomplish an infringing activity and encouraging that activity through advertisement are sufficient to establish liability for copyright infringement." *Sony*, 464 U.S. at 436. This was, Justice Stevens opined, a "gross generalization that cannot withstand scrutiny." *Id.*

77. *Id.* at 434-42.

78. *Id.* at 440. This statement was particularly significant because by the time the Court heard oral argument in *Sony* for the second time, 9.5 million American households had Betamax machines; under Universal's theory, virtually every Betamax user was a copyright infringer, and Sony's potential liability was vast. Counsel for Sony led off his oral argument with this fact. *See* Jessica Litman, *The* Sony *Paradox*, 55 CASE W. RES. L. REV. 917, 940 (2005). The potential for statutory damages for which Sony and/or owners of Betamax machines might be liable if Universal's theory was accepted was staggeringly large.

79. 35 U.S.C. § 271(c).

80. *Id.* For a highly informative discussion of the caselaw on the staple article of commerce rule, see 5 DONALD S. CHISUM, CHISUM ON PATENTS § 17.03 (2004).

Invoking an "historic kinship" between the copyright and patent laws,[81] the Court decided such a safe harbor was appropriate for copyright law as well as for patent law. "The sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement," *Sony* opined, "if the product is widely used for legitimate unobjectionable purposes."[82] Indeed, "it need merely be capable of substantial non-infringing uses."[83] Because the Betamax had substantial non-infringing uses for time-shift copying of television programs, the Court ruled that Sony could not be held secondarily liable for any infringing acts of users of these machines.[84]

In the twenty-some years since the *Sony* decision, information technology developers and the copyright industries have flourished.[85] The *Sony* safe harbor has been an important contributor to the success of both industries. Consumer electronics industry representatives speak of the *Sony* safe harbor as the "Magna Carta" for their industry.[86] Universal and other motion picture producers greatly benefited from the installed base of Betamax and other VTRs, which created opportunities for a wholly new lucrative market for copyrighted motion pictures, such as the sale of video cassettes of movies that could be played in VTR machines.[87] Many other new technologies, including notably the iPod, have similarly allowed both information technology and copyright industries to achieve mutual success.[88]

---

81. *Sony*, 464 U.S. at 439. For an argument that the Court was justified in borrowing this rule from patent law, see, for example, Brief of Amici Curiae of Sixty Intellectual Property and Technology Law Professors and US-ACM Public Policy Committee, to the U.S. Supreme Court in *MGM v. Grokster*, 20 BERKELEY TECH. L.J. 535 (2005) [hereinafter IP Professor Amicus Brief]. *But see* Peter S. Menell & David Nimmer, *Unwinding* Sony, 95 CAL. L. REV. 941, 985 (2007) (questioning the historic kinship justification).

82. *Sony*, 464 U.S. at 442.

83. *Id.*

84. *Id.* at 456.

85. *See, e.g.*, Pamela Samuelson, *The Generativity of* Sony v. Universal*: The Intellectual Property Legacy of Justice Stevens*, 74 FORDHAM L. REV. 1831, 1850-51 (2006) (discussing the legacy of *Sony*).

86. Litman, *supra* note 78, at 951. There is considerable support for the *Sony* safe harbor among academics as well as among technology developers. *See, e.g.*, IP Professor Amicus Brief, *supra* note 81; Brief of Intel Corp. as Amicus Curiae Supporting Affirmance, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (No. 04-480), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/20050301_intel.pdf [hereinafter Intel Amicus Brief]. However, there are also some critics. *See, e.g.*, Menell & Nimmer, *supra* note 81; Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J. L. & TECH. 395 (2003).

87. LARDNER, *supra* note 69, at 297-313.

88. *See, e.g.*, Intel Amicus Brief, *supra* note 86.

Although Congress has been persuaded on two occasions to deviate from the *Sony* safe harbor in very narrowly drawn circumstances,[89] it has rejected other legislative proposals aimed at giving copyright owners greater control over dual-use technologies.[90] Courts have also denied relief to some who sought to expand technology developer liability.[91] Yet, when presented with technologies lacking in substantial non-infringing uses, courts followed *Sony* and imposed liability for infringements thereby enabled.[92]

The White Paper had sought to establish a new rule for technology developer liability with respect to so-called circumvention technologies based on the "primary use" of the technology.[93] This approach resembled the technology developer liability rule that the Supreme Court rejected in *Sony* as too unbalanced. Soon after enactment of the DMCA, the entertainment industry commenced litigation against peer-to-peer ("P2P") file-sharing software developer Napster with the aim of overturning the *Sony* safe harbor for technologies with substantial non-infringing uses.[94] In cases against P2P file-sharing technology developers, the entertainment industry once again urged the courts to adopt a "primary use" theory of technology developer liability for user infringements.[95] Part III will discuss why the latter effort was unsuccessful, but for now, it suffices to say

---

89. *See* 17 U.S.C. § 1002 (prohibiting manufacture and sale of digital audio recording technologies unless they incorporate serial copy management technologies); 47 U.S.C. § 605(e)(4) (outlawing development and distribution of satellite cable decoder boxes). These narrow exceptions to the *Sony* safe harbor are discussed in Samuelson, *supra* note 85, at 1858-62.

90. *See, e.g.*, Nicholas E. Sciorra, *Note, Self-Help and Contributory Infringement: The Law and Legal Thought Behind a Little "Black Box,"* 11 CARDOZO ARTS & ENT. L.J. 905 (1993).

91. In *Vault Corp. v. Quaid Software, Ltd.*, 847 F.2d 255 (5th Cir. 1988), for instance, the maker of the Prolok copy-protection software sued Quaid, the maker of Ramkey software that bypassed Prolok, claiming Quaid was a secondary copyright infringer because the primary use of its software was likely to be making infringing copies of Prolok-protected software. The court invoked the *Sony* safe harbor as a basis for denying Vault's claim because Ramkey was a dual-use technology that enabled purchasers of software products to make lawful backup copies. *Id.* at 262.

92. *See, e.g.*, A&M Records, Inc. v. Abdallah, 948 F. Supp. 1449 (C.D. Cal. 1996) (imposing secondary liability because alleged non-infringing uses were insubstantial).

93. *See supra* note 25 and accompanying text.

94. *See* A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001), discussed *infra* Part III.A.

95. *See, e.g.*, Petition for a Writ of Certiorari at 15-20, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (No. 04-480) (interpreting *Sony* as a "primary use" case), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/20041008_Grokster_final_petition.pdf.

that the White Paper proposal for regulating technologies based on their primary purpose or use was a radical departure from the *Sony* safe harbor default rule in place since 1984.[96]

2. *Technology Developers Criticized the White Paper's Anti-Circumvention Proposal*

Information technology developers raised numerous concerns about the White Paper's proposed anti-circumvention rule in addition to objecting to its incompatibility with the *Sony* safe harbor for technologies with substantial non-infringing uses.[97] For one thing, the proposed provision was vague about what kinds of "processes" and "treatments" it was designed to protect. For another, its willingness to penalize technology developers based on "primary effect" meant that developers risked liability for what users did with the technology, rather than for what the technology had been designed to do. The proposed rule also lacked exceptions for legitimate acts, such as building tools to bypass TPMs for law enforcement, national security, or computer security research purposes. It could, moreover, be interpreted as outlawing the development of reverse engineering technologies to enable interoperability among computer programs.

The greatest concern of technology developers, however, was that the provision might be construed as imposing a duty on them to detect and enforce any TPM that copyright owners might use to protect their works in digital form. The most vigorous technology industry lobbying about anti-circumvention rules concentrated on getting statutory clarification that they had no obligation to design technologies to respond to copyright-protective TPMs.

The technology industry's opposition to the proposed anti-circumvention rule contributed to a stall in the initial legislative efforts in

---

96. Although the White Paper did not acknowledge that its proposal would have any impact on the *Sony* safe harbor, Marybeth Peters, the Register of Copyrights, did so in the course of the legislative debate that led up to the DMCA. *See WIPO Copyright Treaties Implementation Act and On-Line Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2180, Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. (1997) (statement of Marybeth Peters, the Register of Copyrights), *available at* http://www.copyright.gov/docs/2180_stat.html.

97. The technology industry objections to the White Paper proposed anti-circumvention rule are discussed at length in Samuelson, *supra* note 14, at 531-34, 546-57. Some in the technology industry, including the Business Software Alliance and its members, ultimately supported the DMCA anti-circumvention rules because they were more narrowly tailored than the White Paper proposal and because these developers sometimes use TPMs to control access to their works and did not want others to build tools to circumvent them.

1995 and 1996 to enact the White Paper's recommendation.[98] Another setback for copyright industry groups occurred in December 1996 when opposition to a White Paper-like ban on circumvention technologies caused it to be dropped from the final version of the WCT.[99] Many delegations at the WIPO diplomatic conference were concerned that the proposed anti-circumvention rule would chill development of dual-use technologies and impede fair and other non-infringing uses of copyrighted works and public domain materials.[100] To avert these undesirable effects, the treaty required only that contracting parties provide "adequate protection" and "effective remedies" against circumvention of TPMs,[101] which seemingly left the mode and extent of implementation of this norm to national discretion.

Congressmen Tom Campbell and Rick Boucher proposed to implement this treaty obligation in the U.S. with a minimalist anti-circumvention rule aimed at outlawing circumvention of a TPM for purposes of facilitating or engaging in infringing activities.[102] This bill was unacceptable to copyright industry groups, who favored adoption of a broad ban on circumvention technologies, akin to the proposal that had been rejected at WIPO, to serve as a standard for international implementation of the WIPO treaty's anti-circumvention norm.[103]

The Clinton Administration's post-treaty anti-circumvention proposal responded to technology industry concerns in several ways: by becoming more precise about the technical measures the rule was designed to protect;[104] by defining circumvention;[105] and by outlawing only technologies that were "primarily designed or produced" to circumvent TPMs, that had only limited uses other than for circumvention, or that had been marketed as circumvention tools.[106] It also contained an exception for national security and law enforcement activities.[107] Further lobbying led to the creation

98. *Id.* at 523.

99. *See* Samuelson, *supra* note 4, at 409-16 (discussing opposition to the proposed WIPO treaty anti-circumvention provision).

100. *Id.*

101. WCT, *supra* note 1, art. 11.

102. *See* H.R. 3048, 105th Cong. § 8 (1997).

103. *See, e.g.*, Chander, *supra* note 18, at 206-07 (discussing stronger than DMCA anti-circumvention rules being negotiated by the U.S. in free trade agreements with other nations).

104. 17 U.S.C. § 1201(a)(3).

105. *Id.*

106. *Id.* at § 1201(a)(2), (b)(1).

107. *Id.* at § 1201(e).

of exceptions for encryption research, computer security testing,[108] and reverse engineering to achieve interoperability.[109]

The technology industry also obtained the "no mandate" clause that had been its top priority. Section 1201(c)(3) provides that the law does not "require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological protection measure."[110] Given how hard the copyright industries fought against inclusion of any exceptions to section 1201—beyond that for law enforcement and national security activities—especially the "no mandate" rule, it is notable that technology industry objections led to substantial changes in the circumvention technology rules.

Still, it was a major victory for the entertainment industry that the DMCA anti-circumvention rules premised technology developer liability on a "primarily designed or produced" standard.[111] Copyright industry representatives were pleased with the DMCA also because, on its face, section 1201 did not appear to require any proof that the availability of a circumvention tool enabled copyright infringement or even created a grave risk of infringement.[112] The exceptions are, moreover, complex and ambiguous enough to be susceptible to dismissive interpretations.[113]

3. *Regulating Acts of Circumvention and Public Interest Uses of Technically Protected Works*

The most troubling part of the legislative history of the DMCA anti-circumvention rules was the manner in which Congress dealt with the

---

108. *Id.* at § 1201(g), (j).

109. *Id.* at § 1201(f).

110. *Id.* at § 1201(c)(3).

111. *Id.* at § 1201(a)(2)(A), (b)(1)(A).

112. For a discussion of numerous examples of ill effects arising from the overbreadth of the DMCA anti-circumvention rules, see ELECTRONIC FRONTIER FOUNDATION, UNINTENDED CONSEQUENCES: SEVEN YEARS UNDER THE DMCA (as updated Apr. 2006), *available at* http://www.eff.org/IP/DMCA/DMCA_unintended_v4.pdf [hereinafter UNINTENDED CONSEQUENCES].

113. *See, e.g.*, NATIONAL RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE 171-76 (2001) [hereinafter DIGITAL DILEMMA] (raising objections to the complexity and narrowness of the DMCA encryption research exception). Under the *Reimerdes* decision, a journal publisher could arguably be held liable for violating the DMCA anti-circumvention laws even if the author of an encryption research article it planned to publish qualified for the DMCA exception because the publisher is not itself an encryption researcher. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 320 (S.D.N.Y. 2000). *See* Pamela Samuelson, *Anti-Circumvention Rules: Threat to Science*, 293 SCIENCE 2028 (2001).

threat that TPMs posed for the public's ability to engage in fair and other non-infringing uses of copyrighted works protected by TPMs. As we shall see in Part IV, the EU implemented the WCT anti-circumvention norm by making a normative (if incomplete) commitment to ensuring that copyright exceptions and limitations on the scope of exclusive rights must be made as available when copyrighted works are protected by TPMs as when they are not.[114] No similar commitment is apparent in the DMCA rules, although there is ample, if somewhat equivocal, evidence that Congress had tried to assure itself through various measures that it was preserving opportunities for fair and other privileged uses of technically protected digital content.[115]

The initial threat that the White Paper posed to fair and other public interest uses of technically protected copyrighted works was somewhat indirect. The White Paper had not attempted to regulate the act of circumvention, but its proposal to ban circumvention technologies affected public interest uses insofar as circumvention tools were necessary to engage in such uses of content wrapped in TPMs.[116] From the standpoint of copyright owners, however, circumvention technologies that enabled fair or other public interest uses of technically protected works were dangerous because they were too likely to enable infringements. A broad ban on circumvention technologies was, they argued, necessary to protect against massive infringements.

It was not until 1997 that the Clinton Administration proposed a ban on the act of circumventing TPMs used by copyright owners to protect their works.[117] The bill distinguished between two types of TPMs: those used to control access to copyrighted works and those used to protect "a right of a copyright owner" in a work protected by copyright law.[118] Its sponsors did not explain why the bill distinguished between these two

---

114. *See infra* Part IV (discussing limits that have hampered the effectiveness of Article 6(4) in achieving this objective).

115. *See, e.g.*, 17 U.S.C. § 1201(c)(1), discussed *infra* notes 124-125 and 251-257 and accompanying text.

116. *See, e.g.*, Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089 (1998). Yet, perhaps building a circumvention tool for public interest purposes could be defended as authorized by the law, even if not by the copyright owner. *Id.* at 1142 n.200. If so, it might have been outside the White Paper's anti-circumvention ban, which recognized both sources of authority as relevant to the scope of the ban.

117. *See* H.R. 2281, 105th Cong. (1997).

118. The distinction between the two types of TPMs is evident in the bifurcation of the anti-tool rules. *See id.*, § 3. The DMCA, as enacted, has retained this distinction. *See* 17 U.S.C. § 1201(a)(2), (b)(1).

types of TPMs, nor why it proposed totally banning circumvention of access controls, but not of other TPMs.

A coalition of organizations, including libraries, educational institutions, and other nonprofit organizations raised concerns about the direct impact that such a ban would have on fair and other non-infringing uses of copyrighted works in digital form, on access to public domain materials, and on user privacy interests.[119] These concerns did not, however, arouse Congressional interest as much as concerns about overbroad ISP liability. This relative indifference may be explained in part perhaps because the lobbying clout of these nonprofits was minute in comparison with the heft of the copyright, telecom, and technology industries that lobbied about ISP liability. Furthermore, deployment of TPMs to protect copyrighted works was in its early stages, so concerns about impediments to fair and other privileged uses may have seemed speculative.[120]

Yet, if one knows where to look, there is considerable evidence of Congressional concern about enabling public interest uses of technically protected content. By regulating circumvention of access controls, but not of rights controls,[121] Congress decided, albeit implicitly, that circumvention for fair use and other public interest purposes should remain lawful. Congress also created three special public interest exceptions, including one for libraries, archives, and educational institutions to bypass TPMs to make a good faith effort to decide whether to buy the content protected by the TPM if circumvention was necessary to achieve this objective;[122] one that aims to protect user privacy interests implicated when content is protected by TPM; and one that buttresses parental control over minors.[123]

---

119. *See WIPO Copyright Treaties Implementation Act and On-Line Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2180, Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. (1997) (testimony of Robert Oakley; testimony of M.R.C. Greenwood).

120. The important role of the House Commerce Committee in inserting some balance in the anti-circumvention rules is related in Samuelson, *supra* note 14, at 541-43.

121. 17 U.S.C. § 1201(a)(1)(A). *See* Ginsburg, *supra* note 14, at 6 (noting that section 1201 "does not prohibit the act of circumventing a rights control"). Ginsburg believes that the decision not to regulate circumvention of rights controls was intended to leave room for fair uses of technically protected works. *Id.* at 10.

122. 17 U.S.C. § 1201(d).

123. *Id.* at § 1201(h), (i). These provisions are, however, a puzzlingly narrow response to concerns expressed about the anti-circumvention ban. *See, e.g.*, Samuelson, *supra* note 14, at 537-53 (explaining the undue narrowness of section 1201's exceptions); David Nimmer, *Puzzles of the Digital Millennium Copyright Act*, 46 J. COPYRIGHT SOC'Y 401 (1999), *available at* http://ssrn.com/abstract=208876.

A more general indication of Congressional concern about the impact of section 1201 on fair and other privileged uses can arguably be found in section 1201(c)(1), which states that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."[124] Some members of Congress who spoke about the anti-circumvention rules during the legislative debate over the DMCA seemed genuinely to believe this provision constituted a "savings clause" to enable fair and other privileged uses of technically protected copyrighted works.[125]

Finally, Congress established a triennial rulemaking process under which the Librarian of Congress (LOC) is directed to examine "the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research."[126] The Librarian is authorized to create new exceptions from the ban on circumvention to enable public interest uses of copyrighted works when users of certain classes of copyrighted works show they "are, or are likely to be . . . adversely affected" by the use of TPMs.[127]

Much contested is whether these provisions of the anti-circumvention rules meaningfully contribute to an adequate balance of public and private interests in the DMCA. The first decision to have considered this question was *Universal City Studios, Inc. v. Reimerdes*,[128] in which Judge Lewis Kaplan concluded that Congress had considered, and decided against, allowing circumventions for fair use or other privileged purposes. "If Congress had meant the fair use defense to apply to [anti-circumvention] actions, it would have said so. The decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate."[129]

In affirming an injunction against posting or linking to DeCSS, software designed to bypass the Content Scramble System (CSS) protecting DVD movies, the Second Circuit rejected the argument that section 1201(c)(1) was a "fair use savings" clause. The panel declared that this

---

124. 17 U.S.C. § 1201(c)(1).

125. *See, e.g.*, 144 CONG. REC. H7093 (daily ed. Aug. 4, 1998) (statement of Rep. Bliley) (indicating that the Commerce Committee understood the DMCA legislation to enable consumers to "exercise their historical fair use rights").

126. 17 U.S.C. § 1201(a)(1)(C).

127. *Id.*

128. 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

129. *Id.* at 322.

interpretation "is not only outside the range of plausible readings of the provision, but is also clearly refuted by the statute's legislative history."[130]

Both the trial court and the Second Circuit considered the triennial rulemaking and the narrowly drawn public interest exceptions to section 1201 as adequately accommodating fair use and other public interests pertaining to technically protected works.[131] Judge Kaplan characterized the argument that purchasers of DVD movies have the right to circumvent CSS so long as they do not infringe copyrights in DVD movies as "pure sophistry" and as "a corruption of the first sale doctrine."[132] According to Judge Kaplan, the DMCA anti-circumvention laws "fundamentally altered the landscape of copyright" as to technology provider liability.[133]

Seemingly without realizing it,[134] Judge Kaplan arguably also closed off another possible public interest safety valve in the DMCA by construing DeCSS as a tool for circumventing access controls. If CSS is indeed an access control, then bypassing it would violate section 1201(a)(1)(A). Insofar as TPMs, such as CSS, are deemed "access controls" within the meaning of section 1201, the public interest circumventions that the DMCA was supposed to accommodate by not regulating circumvention of non-access-control TPMs have arguably been foreclosed. Copyright owners have apparently recognized that they may be able to defeat some public interest limitations on the scope of the anti-circumvention rules by adopting persistent access controls as their TPMs of choice.[135]

Given the hostility that *Reimerdes* and *Corley* displayed toward fair use as a limitation on the scope of section 1201, the next most plausible candidate for an accommodation of public interest uses of digital content protected by TPMs would seem to be the LOC rulemaking procedure. However, this procedure is not a sufficient safety valve for several reasons.

---

130. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443 (2d Cir. 2001). *But see* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1200 (Fed. Cir. 2004) (regarding section 1201(c)(1) as a fair use savings clause).

131. *Reimerdes*, 111 F. Supp. 2d at 323; *Corley*, 273 F.3d at 443.

132. *Reimerdes*, 111 F. Supp. 2d at 317 n.137.

133. *Id.* at 324.

134. In discussing circumvention for fair use purposes, Judge Kaplan seemed to accept that technically sophisticated persons would be able to circumvent CSS to make fair uses of DVD movies without violating the DMCA rules. *Id.* at 388. Yet, his conclusion that CSS is an access control is inconsistent with his conclusion that technical sophisticates could make fair uses of DVD movies.

135. *See, e.g.*, R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anti-Circumvention Law?*, 18 BERKELEY TECH. L.J. 619 (2003).

First, it only occurs every three years, and any exceptions created only last for three years.[136] Second, it is largely focused on exempting classes of works rather than classes of uses, although classes of uses are more relevant when assessing public interest uses.[137] Third, proposals for exemptions can only be made during the rulemaking process, and a heavy burden of proof has been put on the proponent of any particular new exception to show adverse effects on privileged uses.[138] This contrasts sharply with the EU, which seems to place burdens on its member states and on copyright owners to ensure that privileged uses can be exercised, even when works are technically protected.[139]

Fourth, section 1201 does not authorize the LOC to create exceptions to the tool rules, only to the act of circumvention rule.[140] Without some way to obtain appropriate tools, circumvention privileges may not be meaningful. Fifth, the LOC has generally construed its rulemaking authority in a narrow manner.[141] For these reasons, we agree with the Electronic Frontier Foundation, a prominent civil liberties group, that "the DMCA

136. 17 U.S.C. § 1201(a)(1)(C)-(D).

137. *Id.*

138. *See* 17 U.S.C. § 1201(a)(1)(C); ELECTRONIC FRONTIER FOUNDATION, DMCA TRIENNIAL RULEMAKING: FAILING THE DIGITAL CONSUMER 3 (2005) [hereinafter EFF on Rulemaking], *available at* http://www.eff.org/IP/DMCA/copyrightoffice/DMCA_rulemaking_broken.pdf (explaining why ordinary consumers without copyright counsel are unlikely to be able to meet the onerous burden of proof established by the Copyright Office, but "[e]ven with expert assistance, the burdens imposed by the Copyright Office on participants often prove nearly insurmountable"). By focusing the inquiry on proof of adverse effects on non-infringing uses of classes of works, the DMCA makes it difficult to focus on particular uses, a more relevant criterion for fair use analysis. *See* Bill D. Herman & Oscar Gandy, *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121 (2006).

139. *See infra* Section IV.A.

140. *See* 17 U.S.C. § 1201(a)(1)(D); EFF on Rulemaking, *supra* note 138, at 2 ("[A]verage consumers denied access to circumvention tools are not able to make use of the 6 exemptions that have been granted."). One of us has argued that there should be an implied right to make a tool to enable a privileged party to make a privileged use of technically protected content. Samuelson, *supra* note 14, at 554.

141. *See, e.g.*, Diane Leenheer Zimmerman, *Adrift in the Digital Millennium Copyright Act: The Sequel*, 26 U. DAYTON L. REV. 279, 283-84 (2001). *See also* ALA, DMCA SECTION 1201—THE ANTI-CIRCUMVENTION RULE (as updated Dec. 22, 2005), http://www.ala.org/ala/washoff/woissues/copyrightb/dmca/dmcasection1201.cfm (characterizing the LOC exceptions as "narrow"); EFF on Rulemaking, *supra* note 138, at 7 (pointing out that the Copyright Office has given a narrower interpretation of fair use in the course of its rulemakings than courts and commentators have done).

triennial rulemaking is fundamentally unable to protect the interests of today's digital media consumers."[142]

In the latest rulemaking,[143] the LOC moved beyond the exemption of "particular class[es] of works"[144] and proposed an exemption focused on a particular type of use by a particular type of user. It created an exception so that media or film study professors could make compilations of clips from CSS-protected movies for use in teaching classes.[145] Much as the LOC deserves credit for this innovative interpretation of its section 1201 authority, this exemption seems to leave in the lurch everyone else who might want to make fair use clips of CSS-protected movies.[146] Many other fair use clips of technically protected content can easily be imagined, but only those who participate in a triennial rulemaking have a chance of having their fair use interests accommodated through the rulemaking process.

The LOC rulemaking procedure "is a kind of safety valve" for the DMCA anti-circumvention rules, but as Professor Ginsburg has recently concluded, "it may not let off enough steam."[147] Too many public interest uses of copyrighted works are being blocked by TPMs.[148] The checks and balances that Congress arguably embedded in the DMCA have not achieved the necessary balance.

A better balance among competing interests can be attained within the framework of the DMCA anti-circumvention rules.[149] Among the more

142. *Id.* at 1. *See also id.* at 8 (offering suggestions about how the LOC rulemaking could be improved); Aaron Perzanowski, *Evolving Standards & The Future of The DMCA Anticircumvention Rulemaking*, 10 J. INTERNET L. 1, 20-21 (April 2007) (discussing shortcomings of the DMCA rulemaking process).

143. 37 C.F.R. § 201.40(b)(1) (2007).

144. *See* 17 U.S.C. § 1201(a)(1)(B)-(C).

145. *See* 37 C.F.R. § 201.40. For a discussion of the latest rulemaking, see, for example, Ginsburg, *supra* note 14, at 12-17. Ginsburg notes that the film teacher exception "departs significantly from prior rule-makings." *Id.* at 12-13.

146. For example, an evidence professor might want to bypass CSS in order to take clips from movies about trials to show his class how to (and not to) make objections, while a psychology professor might want to make fair use clips of movies to demonstrate how mentally ill people are depicted. We are hopeful that a judge with a broad view of 17 U.S.C. § 1201(c)(1) might analogize these and similar fair use circumventions to the exemption granted by the LOC, but there is as yet no precedent for doing so.

147. Ginsburg, *supra* note 14, at 16.

148. *See, e.g.*, Armstrong, *supra* note 14, at 68; Benkler, *supra* note 14, at 420-27; Lipton, *supra* note 14, at 124-36; Perzanowski, *supra* note 142, at 17-18.

149. Professors Burk and Cohen have proposed requiring deployers of TPMs to make unlocking technologies available to enable fair uses by third party escrow agents. Burk & Cohen, *supra* note 14, at 65-67. Professor Lipton has proposed that the Copyright Office establish an administrative procedure to assist prospective fair users of TPM content. Lipton, *supra* note 14, at 124.

modest measures, courts could decide that persistent access controls, such as CSS, are not the kinds of "access controls" that section 1201(a) actually regulates, which would open up considerably more room for fair use circumventions.[150] They could also find in section 1201(c)(1) a statutory basis for excusing fair use circumventions.[151] They could, moreover, regulate abuses of section 1201 and abusive uses of TPMs through the anti-circumvention misuse doctrine first proposed by Professor Burk.[152] Courts could additionally interpret the DMCA anti-circumvention rules as inapplicable to any technology that does not pose serious risks of enabling copyright infringement.[153]

The stronger measure to achieve balance in the DMCA anti-circumvention regulations that we propose is the reverse notice and takedown regime discussed in the next part. It would not only permit circumvention to enable public interest uses of technically protected digital content, but it could provide a mechanism to help those who lack the technical expertise to perform public interest circumventions by themselves. In an appropriate case, prospective fair users, after unsuccessfully seeking voluntary cooperation from relevant copyright owners, could seek a declaratory judgment that circumvention for specific public interest purposes should be permitted. Courts in such cases could order copyright owners to cooperate with facilitating such circumventions, including, as necessary, providing the key to unlock the TPM that was inhibiting a particular privileged use to the prospective user or designating a circumvention service to facilitate this action.

III. SETTING THE STAGE FOR A REVERSE NOTICE AND TAKEDOWN REGIME

The idea for a reverse notice and takedown regime emerged as we reflected upon two groups of cases that have recently challenged the outer limits of protection for copyrighted works in the digital environment. Both have elicited considerable attention and controversy,[154] although most

150. *See, e.g.*, Reese, *supra* note 135, at 663-64.

151. *See, e.g.*, Ginsburg, *supra* note 14, at 21-22; Samuelson, *supra* note 14, at 539-45.

152. Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095 (2003).

153. The Federal Circuit opened up this possibility by its far-sighted decision in *Chamberlain Group, Inc. v. Skylink Technologies., Inc.*, 318 F.3d 1178 (Fed. Cir. 2004), discussed at length *infra* notes 241-258 and accompanying text.

154. *See, e.g.*, Matthew D. Brown et al., *Secondary Liability for Inducing Infringement After MGM v. Grokster: Infringement Prevention and Product Design*, 9 J. INTERNET L. 21 (Dec. 2005); Stacey Dogan, *Is Napster a VCR? The Implications of Sony for*

commentaries have not considered the two groups of cases in conjunction with one another. We, however, find in these sets of cases not only a deep symmetry, but the theoretical underpinnings for judicial evolution of a reverse notice and takedown regime that would permit and enable circumventions of technically protected copyrighted content for public interest purposes.

The first group of cases—*Napster*,[155] *Aimster*,[156] and *Grokster*[157]—considered whether online service providers and related software toolmakers who facilitated P2P file sharing of copyrighted sound recordings by a multitude of individual direct infringers should be held indirectly liable for their users' infringing acts. (We will call these the "dissemination technology cases.") Entertainment industry plaintiffs in these cases believed that the scale of infringements enabled by these technologies was so vast that courts would be willing to move away from the *Sony* safe harbor for technologies with substantial non-infringing uses in favor of a "primary use" test for technology/service developer liability under copyright law.[158]

As in the legislative debate that produced the DMCA, the entertainment industry dismissed as unimportant expressions of concern about the public's interest in access to these technologies and services for non-infringing purposes if the entertainment industry gained greater control over technology development.[159] Notwithstanding the many arguments and amicus briefs that the industry marshaled in favor of the primary use

---

Napster and Other Internet Technologies, 52 HASTINGS L.J. 939 (2001); Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement without Restricting Innovation*, 56 STAN. L. REV. 1345 (2004); Lipton, *supra* note 14.

155. A&M Records, Inc. v. Napster Inc., 239 F.3d 1004 (9th Cir. 2001).

156. *In re* Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003).

157. Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 545 U.S. 913 (2005).

158. *See* Brief for Motion Picture Studio and Recording Company Petitioners, Metro-Goldwyn-Mayer Studios v. Grokster Ltd., 545 U.S. 913 (2005) (No. 04-480), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/04-480_Petitioners_brief.pdf [hereinafter MGM Brief]. Recall that the Court had rejected, albeit only just barely so, a primary use test for indirect liability for copyright infringement in the *Sony* case. *See supra* note 73 and accompanying text. Section 1201 adopts a variant on the primary use test for circumvention technology liability. While in theory a "primary purpose or design" test, as in the DMCA, is more rigorous than the "primary use" test for which Universal argued in *Sony*, we are skeptical about how different they would be in practice, given that when a technology is primarily used for an illicit purpose, a challenger of that technology will almost certainly argue that the technology must have been designed to facilitate these illicit uses and that any testimony about beneficial purposes for the design are self-serving misrepresentations to avoid liability. *See* IP Professor Amicus Brief, *supra* note 81, at 559-61.

159. *See, e.g.*, MGM Brief, *supra* note 158, 18-20.

test,[160] the Supreme Court maintained a balanced approach to technology/service developer liability in *Grokster*. It preserved the *Sony* safe harbor for technology developers except as to those who actively induce copyright infringement.[161] As in *Sony*, the Court was attentive to the interests of the public in access to dual-use technologies for non-infringing purposes.[162]

In the second group of cases—*Chamberlain*,[163] *Lexmark*,[164] and *StorageTek*[165]—makers of technologies claimed that by embedding software access controls inside their products, they had obtained the right to control the market for replacement parts or repair services. (We will call these the "lock-out technology" cases.) The courts ultimately decided these cases by permitting third-party suppliers of parts or services to bypass the lock-out codes and provide competing parts or services, notwithstanding the amplified rights of copyright owners under the anti-circumvention provisions of the DMCA.[166] Judges in the lock-out cases could not accept the unbalanced interpretation of section 1201 that the plaintiffs had constructed on the foundation laid by *Reimerdes* and *Corley*.

Both groups of cases focus attention on the extent to which recent legislative efforts to bolster the protection of copyright owners operating in the digital environment have unduly narrowed or sacrificed the interests of users, follow-on improvers, competitors, and the public at large that were core components of pre-digital traditional copyright law. In practical terms, however, the two groups of cases affect the public interest at diametrically opposite ends of the spectrum of protected rights.

This Article will show that the dissemination technology cases have implications for public interest users who want to access copyrighted works for unauthorized but non-infringing purposes when the works in question have been surrounded by TPMs designed to prevent unauthorized uses. The dissemination technology cases also have implications for the

160. The many amicus briefs filed in support of MGM's appeal are available at http://www.eff.org/IP/P2P/MGM_v_Grokster/.

161. *Grokster*, 545 U.S. at 937.

162. *Id.* at 920 ("Given [their] benefits in security, cost, and efficiency, peer to peer networks are employed to store and distribute electronic files by universities, governmental agencies, corporations, and libraries among others.").

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

164. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

165. Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

166. Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-05 (2000).

right of public interest users to access technologies that enable lawful uses. These cases recognize both the legitimacy of user access to equipment that enables non-infringing uses and the need for incentives to persuade manufacturers to invest in and create innovative technology, such as P2P file-sharing software, that can enhance non-infringing uses of copyrighted works.[167] By articulating a theory that took the "bad" technology developers out of the picture, as the Supreme Court did with its active inducement rule in *Grokster*, the Court created a climate in which public interest uses could more freshly be assessed both generally and as they pertain to circumvention of TPMs.

The lock-out technology cases contribute further to this fresh approach by rejecting the plaintiffs' anti-competitive section 1201 claims as unsound and by importing balancing principles from copyright and patent law as essential to the proper interpretation of section 1201. Among other things, the courts in *Chamberlain* and *StorageTek* recognized the need to guard the public's interest in making fair and other non-infringing uses of technically protected content. The lock-out cases, in our view, set the stage for judicial development of the reverse notice and takedown procedure we endorse in this Article.

A. The Dissemination Technology Cases: *Napster*, *Aimster*, and *Grokster*

In approaching the dissemination technology cases and the controversies they have provoked, we offer some preliminary observations. First, there are very few privileged public interest uses directly at stake when consumers use P2P file-sharing technologies to download entire musical works and sound recordings without payment to authors, artists, and recording studios. Unless one believes that copyrights are an inherently illegitimate form of property, one cannot readily defend the limitless free-riding on copyrighted works that P2P file sharing has engendered in terms of traditional exceptions to copyright protection.[168]

---

167. *See, e.g.*, Lemley & Reese, *supra* note 154.

168. Some have argued that the public interest might better have been served by a liability rule than a property rule in response to the P2P file-sharing phenomenon, that is, by grant of a compulsory license to allow file sharing of copyrighted works for noncommercial purposes. *See, e.g.*, WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW AND THE FUTURE OF ENTERTAINMENT (2004); Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARVARD J. L. & TECH. 1 (2003); *see generally* J. H. Reichman, *Of Green Tulips and Legal Kudzu: Repackaging Rights in Subpatentable Innovation*, 53 VAND. L. REV. 1743 (2000) (theory of compensatory liability regime). This would have ensured that revenues would flow back

One may lament the demise of any equivalent of the first sale doctrine in the online environment,[169] and one may castigate record companies for clinging too long to outdated business models, without viewing the downloaders as principled defenders of the public interest. Had the DMCA not so shamelessly sacrificed the public interest provisions of copyright law on the altar of TPMs,[170] few copyright law professors would express so much alarm about the cases expanding third-party liability for contributory and vicarious infringement.[171]

What alarms the critics is precisely the potential capacity of the dissemination technology cases, if mishandled by the courts, to exacerbate the imbalance found in the the DMCA's anti-circumvention rules and thereby to further reduce the bona fide and legitimate rights of users, improvers, competitors, and the public at large. From this perspective, every expansion of third-party liability in this group of cases could potentially further inhibit the already limited range of public interest exceptions to copyright protection. Perhaps worst of all, it could further undermine the incentives to invest in technologies needed for the sharing of information goods for legitimate and important public-good purposes.[172]

The validity of these concerns must, however, be tested against the actual holdings in these cases. Napster, Aimster, and Grokster operated online services that supplied P2P technologies to enable users of their software to search for digital files of commercially distributed copyrighted works on other users' computers, connect directly to the other users' computers in order to make copies of the desired files, and transfer the copies to the requesting users' computers.[173] The principal defense of these P2P developers against charges of secondary liability for copyright infringement was that they qualified for the *Sony* safe harbor for technologies with

---

to the composers, performers, and producers of sound recordings while also ensuring that the works were widely distributed.

169. 17 U.S.C. §§ 106(3), 109 (2000).

170. *See, e.g.*, Litman, *supra* note 26, at 122-45.

171. *See, e.g.*, IP Professor Amicus Brief, *supra* note 81, at 556-57 (expressing concern about expansion of technology developer liability rules).

172. *See* Lemley & Reese, *supra* note 154, at 1354-56 (discussing problems of "dual-use" technologies that can be used in both non-infringing and infringing capacities).

173. A&M Records, Inc. v. Napster Inc., 239 F.3d 1004, 1011 (9th Cir. 2001). Napster differed from Aimster and Grokster in that its servers hosted indices through which users could directly search for specific files they wanted to download. *Id.* at 1012.

substantial non-infringing uses,[174] although Napster also raised two DMCA ISP safe harbor defenses.[175]

Napster's *Sony* defense characterized the downloading of MP3 files authorized by new artists, the sampling of songs users planned to buy if they liked them, and the archival copying of sound recordings users already owned as substantial non-infringing uses of its technology.[176] Because of the massive amounts of infringement taking place through use of these P2P services, the entertainment industry plaintiffs argued that the *Sony* safe harbor should not be available for services, or alternatively, that it should only be available if the primary use of the challenged technology was non-infringing, as in *Sony*.[177] Another reason to sue this P2P service was that "it was easier and more effective to shut down Napster than to sue the millions of people who illegally traded files on Napster."[178]

Napster was hardly a neutral ISP providing a vehicle for innocent transmissions of honest exchanges of information or opinions. Yet, it nonetheless claimed immunity under the section 512(a) safe harbor for internet transmissions initiated by others[179] and the section 512(d) safe harbor for information locating tools.[180] The courts in *Napster* rejected its statutory safe harbor defenses.[181] Although Napster's network was capable of some non-infringing uses, the fact remained that, as the Ninth Circuit observed, Napster knew or should have known that massive infringements were underway, and its business success depended on encouraging these

---

174. *See, e.g.*, Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263 (2002).

175. A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 919 n.4 (N.D. Cal. 2000); A&M Records, Inc. v. Napster, Inc., 2000 WL 573136, at *3 (N.D. Cal. 2000) [hereinafter Napster II].

176. *Napster*, 114 F. Supp. 2d at 916.

177. *Id.* at 916 & n.20. The primary use of the Betamax machine was to make copies of television programs for time-shifting purposes, a use that the Court held was fair. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 423-24 (1984).

178. Lemley & Reese, *supra* note 154, at 1349. Lichtman and Landes argue that suing third parties instead of the actual direct infringers can be efficient when the former, although only indirectly responsible, are "typically in a good position to either prevent copyright infringement or pay for the harm it causes." *See* Lichtman & Landes, *supra* note 86, at 409.

179. *Napster II*, at *6-*8 (ruling on Napster's section 512(a) defense).

180. *Napster*, 114 F. Supp. 2d at 919 n.24. Napster argued that absent notice from the copyright holder, it had no way of knowing which transfers were infringing transfers. Brief for Defendant-Appellant Napster, Inc. at 52, *A&M Records, Inc. v. Napster, Inc.* 114 F. Supp. 2d 896 (N.D. Cal. 2000) (Nos. 00-16401 and 00-16403), *available at* http://www.eff.org/IP/P2P/Napster/brief0818.pdf.

181. *Napster II*, *supra* note 175, at *6-*8 (rejecting a section 512(a) defense); *Napster*, 114 F. Supp. 2d at 919 n.4.

infringements.[182] In hindsight, Napster's claim to shelter under the *Sony* safe harbor was undermined by its active inducement of infringement, as the Supreme Court later phrased it in *Grokster*.[183]

The court in *Napster* seemed self-consciously to draw parallels between contributory infringement and the safeguards established for ISPs under section 512 by suggesting that a system operator could avoid liability by purging infringing materials when it knew or should have known about them.[184] Obviously, a true contributory infringer, such as Napster, had no interest in this safeguard.[185]

Perhaps the most interesting aspect of the *Napster* case was the district court's characterization of Napster's system as a potential barrier to entry for honest purveyors of downloaded music operating under a fee-based system.[186] Here, indeed, is a positive nexus to *Sony*,[187] because the Supreme Court's refusal to ban manufacture of VTRs owing to their substantial non-infringing uses removed an inchoate barrier to entry into the movie rental and cassette business.[188] This result became an unforeseen bonanza for film studios who made considerable revenues by selling movies to rental companies and to consumers. In contrast, the district court correctly perceived the opposite effect in the *Napster* case, and the growth of fee-based providers via iTunes and other systems in the aftermath of Napster's closure would seem to vindicate that thesis.[189]

---

182. *Napster*, 239 F.3d at 1020 n.5.

183. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 545 U.S. 913, 936-38 (2005).

184. The Ninth Circuit Court of Appeals stated that "if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement." *Napster*, 239 F.3d at 1021 (quoting Religious Tech. Ctr. (RTC) v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1374 (N.D. Cal. 1995)). The Ninth Circuit invoked *Sony*, where the Supreme Court held that if liability had to be imposed, "it must rest on the fact that they have sold equipment *with constructive knowledge* of the fact that their customers may use that equipment to make unauthorized copies of copyrighted material." *Id.* at 1020 (quoting Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 439 (1984) (emphasis added)). Although the Supreme Court in *Sony* did not clarify what could qualify as constructive knowledge, the Court in *Napster* found that the company had materially contributed to the direct infringement committed by end users, since it had provided them with "the site and the facilities" without which copyright violations could not have been committed. *Napster*, 239 F.3d at 1022-23.

185. *Id.*

186. *Napster*, 239 F.3d at 1016.

187. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

188. *See, e.g.*, LARDNER, *supra* note 69, at 297-313.

189. *See, e.g.*, IFPI, DIGITAL MUSIC REPORT 2007, at 4 (2007), *available at* http://www.ifpi.org/content/library/digital-music-report-2007.pdf ("Digital music sales

Aimster, like Napster, made loose, self-serving assertions about the capability of the relevant software system for non-infringing uses, but this was disingenuous coming from someone whose business knowingly depended on the highest possible volume of infringing uses.[190] By co-opting the instant messaging networks of other ISPs to enable file sharers to find each other and search each other's autonomous files, Aimster's contributory acts were more remote and indirect than Napster's.[191] But Aimster's business objectives depended largely on the volume of its infringing uses; its main business activity was to facilitate these same infringing uses; and it structured its computer architecture so as not to know anything about the specific acts of infringement it did its best to facilitate.[192] Club Aimster, furthermore, gave users access to the top forty songs on the charts for a mere $4.95 a month.[193]

Although the Seventh Circuit's *Aimster* decision expressed some concern about not unduly impeding substantial non-infringing uses under *Sony*, it also toyed with imposing potentially burdensome obligations on technology developers to build in infringement-inhibiting technological measures.[194] The force of this speculation has been greatly weakened by the doctrine of "actively inducing infringement," on which the Supreme Court finally settled in *Grokster*.[195] In hindsight, it seems that the Seventh Circuit in *Aimster* was really groping its way toward the doctrine of active inducement later recognized in *Grokster*.

In *Grokster*, the software system at issue provided a range of means by which users could search through the pools of shared files while connecting directly with each other, and without reference to any central index hosted by defendants.[196] Neither Grokster nor its co-defendant Streamcast "operated the network over which the users of their software connected

---

are estimated to have almost doubled in value worldwide in 2006, reaching an estimated trade value of around US $2 billion"). In 2006, Apple's iTunes accounted for nearly 6% of U.S. music sales, and generated about $1 billion in sales worldwide. Patrick Seitz, *Rock 'N' Roil: iTunes Reports Stir Up Investors*, INVESTOR'S BUS. DAILY, Dec. 14, 2006, at A04. Apple's revenue for "Other Music Product," which includes iTunes sales and iPod accessories, was $653 million for the second quarter of fiscal year 2007. APPLE INC., Q2 2007 UNAUDITED SUMMARY DATA (2007), *available at* http://images.apple.com/pr/pdf/q207data_sum.pdf.

190. *In re* Aimster Copyright Litigation, 334 F.3d 643, 651 (7th Cir. 2003).

191. *Id.* at 646.

192. *Id.* at 650.

193. *Id.* at 651-52.

194. *See id.* at 648.

195. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 545 U.S. 913, 948-49 (2005) (Ginsburg, J., concurring).

196. *See id.* at 920-22.

and exchanged files, and the [district] court emphasized the decentralized nature of those networks," in the sense that "no information is transmitted to or through any computers owned or controlled by the software makers."[197] The lower court also recognized that the software was capable of substantial non-infringing uses, including the authorized dissemination of copyrighted works and dissemination of unprotected works.[198] For the district court, and later the Ninth Circuit, the distance of the software providers from the sites of infringement and their lack of active knowledge of specific infringements was sufficient to shelter them from contributory liability under the *Sony* exception, given the potential non-infringing uses to which the software could be put.[199]

For the Supreme Court, however, Grokster and Streamcast had forfeited the safe harbor established in *Sony* for technologies with substantial non-infringing uses, which the Court had drawn from patent law. In *Grokster*, the Court drew upon another complementary patent law doctrine that disallowed the safe harbor if the defendant had actively induced copyright infringement.[200] Using this approach, neither the relative degrees of remoteness or of the material contribution in the three cases, nor the relative weights of some potential non-infringing uses—allegedly rising to a possible ten percent of all uses in *Grokster*—could vindicate a *Sony* defense if the underlying intent of the operation was to actively induce copyright infringement.[201]

---

197. Lemley & Reese, *supra* note 154, at 1364. In particular, the Ninth Circuit, quoting the District Court, explained: "[E]ven if the Software Distributors 'closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption.'" *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 380 F. 3d 1154, 1164 (9th Cir. 2004) (quoting Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 259 F. Supp. 2d 1029, 1041 (C.D. Cal. 2003)).

198. *See Grokster*, 545 U.S. at 935.

199. *Grokster*, 259 F. Supp. 2d at 1036 ("[T]he existence of substantial non-infringing uses turns not only on a product's current uses, but also on potential future non-infringing uses."); *Grokster*, 380 F.3d at 1161 ("[I]f the product at issue is capable of substantial or commercially significant non-infringing uses, then the copyright owner must demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement.")

200. *See Grokster*, 545 U.S. at 935.

201. In *Sony*, the Supreme Court explained that the application of the staple article of commerce doctrine required Betamax products to be capable of *commercially significant* non-infringing uses, meaning that VCRs should be capable of at least one potential legitimate use employed in a numerically significant manner. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442-43 (1984). The ultimate outcome of the case was deeply influenced by the Court's finding that unauthorized time-shifting was indeed a legitimate fair use.

While some contend that this resolution will unduly chill innovation in dual-use technologies,[202] we have a more optimistic assessment of what *Grokster* accomplished. The *Grokster* decision rejected several proposals to limit the scope of the *Sony* safe harbor. It did not, for instance, exclude services, as such, from the *Sony* safe harbor. It did not adopt any particular standard of intolerable infringing uses. Moreover, it did not adopt a "primary use" test for judging the lawfulness of dual-use technologies.[203] The Court preserved the safe harbor for technologies with substantial non-infringing uses and focused instead on evidence of actions that demonstrated active and intentional promotion of infringement, which disqualified the defendants from the shelter of copyright's variant on patent law's staple article of commerce limitation.[204]

The extent to which suppliers of dual-use technologies may still benefit from a *Sony* safe harbor remains to be worked out in future cases, and care must be taken not to impair or undervalue actual non-infringing uses where they occur in a good faith context. Over time, however, it has become clear that the recording industry cannot cling to obsolete business models that oblige consumers to purchase music they do not want, and that this industry cannot attain control over P2P technology. Rather, as the district court in *Napster* correctly foresaw, shutting down firms such as Napster effectively removed barriers to the entry of fee-based music distribution systems,[205] such as Apple's iTunes service. This arguably helped to support the formation of a new business model that may benefit consumers and competition in the long run.

As to the future prospects for non-infringing users of dual-use technologies in general, we cannot accurately evaluate them through the lens of cases dealing with bad faith active inducers of infringement. Moreover, when we try to envision such cases through a cleaner lens, the real barriers to entry will not lie so much in the weakness of the *Sony* safe harbor as in the potentially troublesome intersection between sections 512 and 1201 of the DMCA.[206]

---

202. *See, e.g.*, Rob Hof, *Larry Lessig:* Grokster *Decision Will Chill Innovation*, BUS. WEEK ONLINE, June 28, 2005, http://www.businessweek.com/the_thread/techbeat/archives/2005/06/larry_lessig_gr.html; Fred von Lohmann, *Remedying* Grokster, LAW.COM, July 25, 2005, http://www.law.com/jsp/article.jsp?id=1122023112436.

203. Pamela Samuelson, *Legally Speaking: Did MGM Really Win the* Grokster *Case?*, 48 COMM. OF THE ACM 19 (Oct. 2005), *available at* http://www.ischool.berkeley.edu/~pam/papers/CACM%20SCT%20decides%20MGM.pdf (pointing out that the Court rejected virtually all of MGM's proposed tests for liability).

204. *Id.*

205. *See* A&M Records, Inc. v. Napster Inc., 239 F.3d 1004, 1016 (9th Cir. 2001).

206. 17 U.S.C. §§ 512, 1201 (2000).

B. Implications for Public Interest Uses of Technically Protected Content

Our concern with dual-use technologies that impede non-infringing uses acquires considerably more traction the moment we try to envision the real life obstacles likely to be encountered by legally privileged non-infringing user groups who, by definition, advance some public interest consonant with, rather than antagonistic to, the goals of copyright protection. Here we are concerned with gaining access to copyrighted works in the digital environment in order to extract unprotectable subject matter, such as ideas and disparate facts; to make fair uses of protectable expressions, including research uses; and to exploit codified exceptions to, or limitations on, the bundle of exclusive rights.[207] Also of concern is access to works whose copyrights have expired but which cannot readily be located in public domain copies outside a given digitally controlled network.[208]

1. Facilitating Public Interest User Groups Under Section 512

By focusing on user groups whose typically nonprofit activities are thought to advance the public interest in education, research, science, and technological progress, we immediately dispel the atmosphere of mistrust arising from *Napster, Aimster* and *Grokster*, and allow courts to think positively about the need to balance public and private interests, as they traditionally sought to do in the pre-digital era.[209] Only when defendants begin to appear in a good faith posture can we really discern what is at

---

207. 17 U.S.C. §§ 102(a), 107-122 (2000).

208. *See, e.g.*, Jonathan Band, *The Google Print Library Project: A Copyright Analysis*, J. OF INTERNET BANKING AND COM., (Dec. 2005), *available at* http://www.policybandwidth.com/doc/googleprint.pdf. (discussing projects to digitize public domain and copyrighted works in major library collections). In theory, anti-circumvention liability should not lie for public interest users who bypass TPMs to gain access to public domain works. However, if publishers use the same TPM to protect copyrighted and public domain works, then any tool that would bypass this TPM will arguably be illegal under section 1201 because of the copyrighted material also being protected by it.

209. *Cf.* WCT, *supra* note 1, Preamble ("The contracting parties, . . . [r]ecognizing the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention . . . . ") We do not mean to suggest that educators, researchers, and the like are the only parties who should be eligible to make public interest uses of technically protected copyrighted works. Many commercial firms engage in fair and other privileged uses, and they too should qualify for the reverse notice and takedown regime. We focus on the nonprofit public interest users in order to make the more general case for the need for the reverse notice regime, as these users are generally perceived in a favorable light in copyright discourse.

stake when the courts make appropriate judgments about the public's interest in access to technologies capable of substantial non-infringing uses.

Of course, P2P systems such as Napster, Aimster and Grokster could not long survive in such an atmosphere because they depend, directly or indirectly, on benefits derived from infringing uses. Private foundations, public entities, and public-private partnerships have already found good reasons to establish P2P file-sharing networks to promote access to information goods for non-infringing public interest purposes. For example, Creative Commons has established such networks for specific subject matter groupings,[210] and scientific efforts to link databases in virtual archives through P2P technologies[211] are growing in number.[212] Science Commons, an affiliate of Creative Commons, has unveiled plans to vigorously employ such technologies in a number of major projects.[213]

These initiatives are likely to increasingly rely on P2P technologies to enable participants to access and share privately held materials, whether copyrighted or not, that have been voluntarily made available to advance the goals of the different user communities in question. Because such communities are, as a rule, loosely organized and administered, they cannot and should not be charged with the duties of policing the contents of materials made available to the community for copyright infringement. Fortunately, so long as such groups take pains to position their networks within the penumbra of section 512 of the DMCA, they can obtain all the sharing advantages of P2P systems while largely immunizing themselves from liability for copyright infringement by virtue of the "notice and takedown" procedures that this provision sets up.[214]

Moreover, section 512 procedures allow systems managers to vet any infringement claims lodged against participating contributors and to refuse

---

210. *See* Creative Commons, http://www.creativecommons.org.

211. *See generally* J. H. Reichman & Paul F. Uhlir, *A Contractually Reconstructed Research Commons for Scientific Data in a Highly Protectionist Intellectual Property Environment*, 66 LAW & CONTEMP. PROBS. 315 (2003) [hereinafter Reichman & Uhlir]; NAT'L RESEARCH COUNCIL, THE ROLE OF SCIENTIFIC AND TECHNICAL DATA AND INFORMATION IN THE PUBLIC DOMAIN (J. M. Esanu and Paul F. Uhlir, eds. 2003).

212. *See, e.g.*, Peter Dawyndt et al., *Contributions of Bioinformatics and Intellectual Property Rights in Sharing Biological Information*, 188 INT'L SOC. SCI. J. 249 (2006); Harlan Onsrud & James Campbell, *Big Opportunities in Access to "Small Science" Data*, DATA SCI. J., (2007). *See also* Science Commons, http://science.creativecommons.org (last visited July 20, 2007).

213. *See id.*; *see also* Abby Seff, *Will John Wilbanks Launch the Next Scientific Revolution?*, POPULAR SCIENCE (July 2007), *available at* http://www.popsci.com/popsci/technology/f8a1780809ed3110vgnvcm1000004eecbccdrcrd.html.

214. 17 U.S.C. § 512 (2000).

to comply with a takedown request if they choose to back their member's claim of privileged use against an outsider's claim of infringement.[215] Even in a worst case scenario, where the outsider's infringement claim ultimately prevails in a court of law, the public interest goals of the user community should encourage courts in this situation to narrowly tailor injunctions so as to avoid inhibiting any legitimate non-infringing uses.[216]

The "notice and takedown" modalities of section 512 thus make it possible to keep P2P networks running for nonprofit public interest purposes. Moreover, the "clean hands" legitimacy of the enterprise should at least ensure that no injunction otherwise affecting some infringing uses of the technology in question would shut down or impede such public interest initiatives. Nor is there anything in the Supreme Court's *Grokster* decision that creates an insuperable barrier to entry for launching these initiatives.[217]

Yet, once a public interest P2P file-sharing network is up and running, problems may arise insofar as the technology allows community members to link to external nonmember ISPs where copyrighted works have been deposited on conditions that restrict use or reuse of the material available there. A risk of conflict exists between the search potential of the software to enable non-infringing uses of posted material and the obligations of the service provider to respect the dictates of the copyright owners it hosts on its site. However, assuming that the service provider was covered by section 512 of the DMCA, this conflict could normally be resolved by "notice and takedown" provisions with which we are familiar.

Under section 512, all of the standard copyright exceptions and defenses are preserved even after the "notice and takedown" machinery superimposed upon them has been triggered. If the information locating tool triggers an objection from the copyright owner, the searcher can respond by asserting the non-infringing uses (e.g., fair uses) that he intends to make of the protected work in question. If the copyright owner acquiesces, the problem is solved. If not, the putative fair user can seek a declaratory judgment to remove the obstacle and vindicate the non-infringing use.

---

215. *Id.* at § 512(g).

216. Public interest uses of protected works might also be facilitated if courts made more use of the Court's suggestion about the appropriateness of damage awards instead of injunctions in close fair use cases. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 578 n.10 (1994).

217. Indeed, the opening section of the *Grokster* decision speaks in positive terms about P2P technologies. Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 545 U.S. 913, 920-21 (2005).

Clearly, these legal modalities would benefit from expeditious administrative procedures to promptly resolve such disputes at low cost, with deferred removal to courts only for specific issues that merited a full dress trial.[218] Our point is that, so long as we are dealing with traditional copyright defenses, section 512 of the DMCA poses no serious barriers to entry for our putative public interest initiative.

2. *How Public Interest Uses May Be Frustrated by Section 1201*

Serious problems may arise, however, when copyright owners surround information products available on their websites with technological fences specifically designed to thwart, for example, the search and sharing capabilities of the non-infringing, would-be public interest users.[219] TPM fences may initially prevent searchers from gaining access for the purpose of browsing contents in order to identify material of interest.[220] The same fences may then direct would-be non-infringing users to an electronic gateway, where electronic contracts of adhesion will condition entry on a waiver of all the users' rights that our putative searchers might otherwise put forward to justify access to and use of the information product in question.[221] The electronic fence will thus separate access from use. Insofar as section 1201(c) permits circumvention for privileged purposes,[222] this will arguably only kick in after lawful access has been gained. Yet, by then, user rights may have been abrogated by contract, and it may already be too late to hack through the electronic fence prohibited by section 1201.[223]

---

218. *See, e.g.*, Lemley & Reese, *supra* note 154, at 1410-25.

219. Firms that want to use TPMs to protect public domain works can, of course, take the precaution of attaching to any bulky ineligible matter, such as a noncreative database, some copyrightable fig leaf component, such as an explanatory introduction, in order to bring the collective work as a whole within section 102(a) of the Copyright Act and trigger the additional protections of section 1201 of the DMCA. For implications for science, see Reichman & Uhlir, *supra* note 211, at 376-79.

220. The DMCA provides an exemption from section 1201(a)(1)(A) for nonprofit libraries, archives, and educational institutions to bypass access controls "solely in order to make a good faith determination of whether to acquire a copy of that work." 17 U.S.C. § 1201(d). This exemption would not, however, apply if the purpose of the circumvention was to index the work or to extract unprotectable facts, ideas, or public domain materials from the technically protected work.

221. *See* J. H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PENN L. REV. 875 (1999). *See also* Burk, *supra* note 152 (discussing anti-circumvention misuse).

222. *See supra* notes 121-127 and accompanying text for a discussion of section 1201 and privileged uses.

223. 17 U.S.C. § 1201 (2000).

Ironically, this scenario inverts the situation found in cases such as *Napster*, *Aimster*, and *Grokster* where facilitators of mass infringements sought to hide behind potential non-infringing uses. Here, instead, bona fide non-infringing users risk being thwarted by copyright owners who use access control TPMs to disable privileged uses.

By using TPMs, copyright owners arguably gain the power to opt out of those parts of the copyright system they dislike. They can not only design TPMs to circumvent public interest uses, but can claim shelter behind section 1201 for doing so. Because some cases have construed section 1201 as abrogating fair use and other public interest exceptions as grounds for circumventing TPMs to extract non-infringing material, the public interest goals of the non-infringing user may be absolutely defeated by the TPM.[224] The DMCA does not explicitly allow circumvention for legally permissible purposes, although this would have been consistent with the WCT and seems to have been the intent of some in Congress.

From this perspective, section 1201 arguably functions as a form of "active inducement" to avoid the public interest exceptions embodied in the Copyright Act. Copyright owners employ TPMs and section 1201 protections in order to thwart infringing uses of their works. However, TPMs may protect against all unauthorized uses, both infringing and non-infringing. Although it is technically difficult to differentiate between these two classes of uses prospectively, firms could do more to facilitate some public interest uses of technically protected content if they chose to do so. There is as yet no incentive for copyright owners or TPM vendors to fine-tune TPMs to enable non-infringing uses.[225]

Thus, unless there is a way for section 1201 to be construed to recognize the legitimacy of access to enable non-infringing uses, the statute could become a one-way ratchet for attaining complete enclosure of digital content.[226] At the very least, it establishes a potential barrier to entry for some meritorious public interest initiatives of the kind envisioned above, and it tends to chill investment in developing viable dual-use technologies that could promote more efficient non-infringing uses.[227]

---

224. *See* Ginsburg, *supra* note 14.

225. One interesting experiment in designing TPMs with fair use in mind is the open source digital rights management technology that Sun Microsystems is developing for digital content that would enable many fair uses. *See* Gerard Fernando et al., *Project DReaM, An Architectural Overview* (Sept. 2005), http://www.openmediacommons.org/collateral/DReaM-Overview.pdf.

226. *Cf.* James Boyle, *The Second Enclosure Movement*, 66 L. & CONTEM. PROBS. 33 (2003).

227. *See* Lemley & Reese, *supra* note 154, at 1390.

The *Reimerdes* decision has unfortunately provided considerable ammunition for the gutting of the public interest balance in copyright law by setting forth a framework for analyzing section 1201 claims that, if followed in subsequent cases, excludes consideration of virtually all public interest concerns. Under Judge Kaplan's interpretation of section 1201, anti-circumvention liability arises: (1) if a copyright owner has adopted a TPM to control access to its copyrighted works (even if they are persistent access controls such as CSS); and (2) if an unauthorized person has developed a technology that bypasses this TPM (relying, if necessary, on an inference that if the defendant's technology bypasses the TPM, it must have been primarily designed or produced to do so).[228] Under *Reimerdes*, it is irrelevant whether copyright infringement has occurred (or was even possible) as a result of the availability of the circumvention tool. Nor does it matter whether the tool might enable consumers to tinker with a copyrighted work he or she has purchased.[229]

Harm to the copyright owner's interests is presumed from the fact of the violation.[230] In Judge Kaplan's view, Congress deliberately decided against permitting circumvention or making circumvention tools to enable fair or other public interest uses of technically protected digital content, and section 1201(c) provided no shelter for public interest uses once copyright owners have deployed technical locks on their content.[231]

C. The Lock-out Technology Cases: *Chamberlain*, *Lexmark*, and *StorageTek*

Although Congress seems to have thought the DMCA anti-circumvention rules would protect copyright owners from massive infringements,[232] it did not take long for some technology developers to realize that these rules, as interpreted in *Reimerdes*, were susceptible to use as a tool for defeating competition in the market for uncopyrightable products and services.[233] Technology developers Lexmark, Chamberlain, and Storage Technology Corp. ("StorageTek") relied on *Reimerdes* in claim-

228. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317-19 (S.D.N.Y. 2000). *See also* Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 217 (S.D.N.Y. 2000).

229. *Reimerdes*, 111 F. Supp. 2d at 314-16, 317 n.137.

230. *Reimerdes*, 82 F. Supp. 2d at 215.

231. *Reimerdes*, 111 F. Supp. 2d at 322-24.

232. *See* S. REP. NO. 105-190, at 8 (1998) (expressing concern about massive piracy as a reason for adopting anti-circumvention rules).

233. *See, e.g.*, Pamela Samuelson and Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1642-49 (2002) (predicting technology developer misuses of the DMCA rules).

ing that the DMCA's anti-circumvention rules conferred on them the right to control access, through digital lock-out codes, to software embedded in their products so as to prevent competitors from supplying after-market replacement parts or services.[234]

1. The Lock-out Technology Cases

Lexmark, a manufacturer of printers and toner cartridges, claimed that the authentication protocol (or digital handshake) component of copyrighted computer programs installed on chips in its printers and toner cartridges was an access control, the bypassing of which violated section 1201(a)(1)(A).[235] Because Static Control made chips designed and produced to bypass this access control, Lexmark charged it with violating section 1201(a)(2).[236] Static Control's customers were manufacturers of toner cartridges designed to work in Lexmark printers. The trial court, relying heavily on *Reimerdes*, issued a preliminary injunction against Static Control's manufacture of these chips.[237]

The Sixth Circuit eventually reversed, seemingly on the ground that the DMCA does not apply to digital fences limiting access to functional aspects of the printers.[238] The court's reasoning on the anti-circumvention

234. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004); Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004); Storage Tech. Corp. v. Custom Hardware, Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

235. *Lexmark*, 387 F.3d at 528-32. Static Control successfully challenged the validity of the copyright in the toner cartridge software because it was a short program with limited functionality and copying was necessary in order to make compatible cartridges capable of running on Lexmark machines. *Id.* at 535-42.

236. *Id.* at 531.

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

238. The court observed:

> In the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code's execution. For example, the encoded data on CDs translates into music and on DVDs into motion pictures, while the program commands in software for video games or computers translate into some other visual and audio manifestation. . . . The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or DVDs, 'using' or executing the Printer Engine Program does not in turn create any protected expression. Instead, the program's output is purely functional.

Lexmark, 387 F.3d at 548.

claim is, unfortunately, neither very coherent nor persuasive.[239] A concurring judge would more forthrightly have invoked the misuse doctrine, so as to "make clear that in the future companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods for themselves just by tweaking the facts of [a] case."[240]

Shortly after issuance of the preliminary injunction in *Lexmark*, a similar attempt was made to use the anti-circumvention rules to foreclose competition in the market for electronic garage-door opening (GDO) devices.[241] Skylink made a universal GDO that bypassed the digitized "lockout" (access control) components of programs Chamberlain had installed in its GDOs and transmitters. Chamberlain argued that the "plain language" of the DMCA and precedents such as *Reimerdes* and the lower court decision in *Lexmark* provided compelling support for its claim against Skylink.[242] The Federal Circuit strongly disagreed and upheld the lower court's grant of summary judgment to Skylink.

The *Chamberlain* decision is remarkable in several respects. A fundamental premise underlying the Federal Circuit's interpretation of section 1201 was its perception that Congress had intended the DMCA anti-circumvention rules to be balanced:

> The most significant and consistent theme running throughout the entire legislative history of the anti-circumvention and anti-trafficking provisions of the DMCA . . . is that Congress attempted to balance competing interests, and "endeavored to specify, with as much clarity as possible, how the right against anti-circumvention would be qualified to maintain balance between the interests of content creators and information users." H.R. Rep. No. 105-551, at 26 (1998). The Report of the House Commerce Committee concluded that § 1201 "fully respects and extends into the digital environment the bedrock principle of

239. *Id.* at 545-51. The court, for example, questioned whether the Lexmark authentication sequence was an access control within section 1201 by observing that purchase of a Lexmark printer allowed access to the program. *Id.* at 549-50. Because it was possible to access the toner cartridge program if one bought a printer and toner cartridge, the court questioned whether the sequence was an effective access control measure. *Id.*

240. *Id.* at 551.

241. Chamberlain Group, Inc. v. Skylink Techs., Inc., 292 F. Supp. 2d 1040 (N. D. Ill. 2003), *aff'd*, 381 F.3d 1178 (Fed. Cir. 2004).

242. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1186, 1192 (Fed. Cir. 2004).

> 'balance' in American intellectual property law for the benefit of both copyright owners and users."[243]

It consequently rejected the notion that the DMCA had created a new exclusive right in copyright owners to control access to their works.[244] Section 1201 should instead be viewed as providing copyright owners with a new cause of action when circumvention of access controls threatened their ability to enforce their exclusive rights under copyright law.

In its search for a more balanced interpretation of the DMCA, the court considered at length linkages between the anti-circumvention rules and rights conferred by copyright law:

> Statutory structure and legislative history both make clear that § 1201 applies only to circumventions reasonably related to [copyright] protected rights. Defendants who traffic in devices that circumvent access controls in ways that facilitate infringement may be subject to liability under § 1201(a)(2). . . . [D]efendants whose circumvention devices do not facilitate infringement are not subject to § 1201 liability.[245]

Without proof of a nexus between the availability of an allegedly unlawful circumvention tool and the existence, or grave threat, of copyright infringement, section 1201 liability should not be imposed.[246] Thus, it was relevant that:

> Chamberlain has not alleged that Skylink's Model 39 infringes its copyrights, nor has it alleged that the Model 39 contributes to third-party infringement of its copyrights. . . . Chamberlain urges us to conclude that no necessary connection exists between access and *copyrights*. Congress could not have intended such a broad reading of the DMCA.[247]

To the extent that *Reimerdes* said otherwise, the Federal Circuit disagreed.

---

243. *Id.* at 1195.

244. *Id.* at 1192-93. The Federal Circuit has thus rejected the views of some commentators that section 1201, in effect, created an exclusive right of access. *See, e.g.*, Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium,"* 23 COLUM. J. L. & ARTS 137, 140-43 (1999). *See also* Michael Landau, *Has the Digital Millennium Copyright Act Really Created a New Exclusive Right of Access?: Attempting to Reach a Balance Between Users' and Content Providers' Rights*, 49 J. COPYRIGHT SOC'Y U.S.A. 277, 286 (2001).

245. *Chamberlain*, 381 F.3d at 1195.

246. *Id.* at 1195-97.

247. *Id.* at 1197.

Under Chamberlain's interpretation of the DMCA, "the owners of a work protected *both* by copyright *and* a technological measure that effectively controls access to that work . . . would possess *unlimited* rights to hold circumventors liable under § 1201(a) *merely for accessing that work* even if that access enabled only rights that the Copyright Act grants to the public."[248] The Federal Circuit found this construction of the DMCA "problematic for a number of reasons."[249]

For one thing, Congress's exercise of its constitutional authority must be rational; yet, as construed by Chamberlain, section 1201(a) "borders on the irrational."[250] For another, its interpretation of section 1201(a) "would flatly contradict § 1201(c)(1)—a simultaneously enacted provision of the same statute."[251] It was consequently necessary to adopt "an alternative construction that leads to no such contradiction."[252]

Construing section 1201(a) as though it was concerned only with control over access, and not with rights protected by copyright law, would be "both absurd and disastrous."[253] It would "allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial 'encryption' scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products."[254] This would "allow virtually any company to attempt to leverage its sales into aftermarket monopolies," even though this would be unlawful under the antitrust laws and the copyright misuse doctrine.[255]

At least as problematic to the Federal Circuit were the implications of Chamberlain's interpretation of section 1201 for the rights of consumers to make fair uses:

> Chamberlain's proposed construction would allow copyright owners to prohibit exclusively fair uses even in the absence of any feared foul use. It would therefore allow any copyright own-

248. *Id.* at 1200.

249. *Id.*

250. *Id.*

251. *Id.* "A provision that prohibited access without regard to the rest of the Copyright Act would clearly affect rights and limitations, if not remedies and defenses." *Id.*

252. *Id.*

253. *Id.* at 1201.

254. *Id.* For analogous concerns about the need for courts to carefully manage boundaries between different modes of intellectual property protection, see *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141 (1989), which struck down Florida anti-plug mold law as contrary to patent law and policy.

255. *Chamberlain*, 381 F.3d at 1201.

> ers through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work—or even selected copies of that copyrighted work. Again, this implication contradicts § 1201(c)(1) directly. . . . Consumers who purchase a product have the inherent legal right to use that copy of the software. What the law authorizes, Chamberlain cannot revoke.[256]

Contrary to Chamberlain's contention, which relied on dicta from *Reimerdes*, "the DMCA emphatically did not 'fundamentally alter' the legal landscape governing the reasonable expectations of consumers or competitors; did not 'fundamentally alter' the ways that courts analyze industry practices; and did not render the pre-DMCA history of the GDO industry irrelevant."[257] The Federal Circuit consequently rejected Chamberlain's interpretation of section 1201 "in its entirety."[258]

The Federal Circuit had a second opportunity to consider the scope of the anti-circumvention rules in *StorageTek*.[259] StorageTek manufactures automated tape cartridge libraries for mass data storage. When StorageTek sells its tape libraries to customers, it licenses customers to use the functional code for managing the tape libraries but not the code to carry out maintenance functions.[260] Custom Hardware Engineering ("CHE") is an independent business that repairs data libraries manufactured by StorageTek. To enable it to carry out these repairs, CHE developed a program that bypassed a password protection scheme in the StorageTek maintenance code so that it could effectively intercept and interpret error messages generated by that program. Processing the error code information enabled CHE to diagnose and repair data libraries for StorageTek's customers. StorageTek claimed that CHE had violated the DMCA anti-circumvention rules.[261]

Relying on its analysis in *Chamberlain*, the Federal Circuit found no DMCA violation: "To the extent that [the defendant's] activities do not constitute copyright infringement or facilitate copyright infringement, StorageTek is foreclosed from maintaining an action under the DMCA.

---

256. *Id.* at 1202.

257. *Id.* at 1194.

258. *Id.*

259. Storage Tech. Corp. v. Custom Hardware, Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

260. *Id.* at 1309-10.

261. StorageTek also claimed copyright infringement. A majority of the Federal Circuit decided that the 17 U.S.C. § 117 safe harbor for computer maintenance services protected CHE's activities. *Storage Tech. Corp.*, 421 F.3d at 1311-18.

That result follows because the DMCA must be read in the context of the Copyright Act, which balances the rights of the copyright owner against the public's interest in having appropriate access to the work."[262] Even if activation of the maintenance code might violate the firm's contractual rights with customers, this unauthorized activation of the code could not violate the DMCA because the contractual rights "are not the rights protected by copyright law."[263] Without proof of a nexus between the rights protected by copyright law and the circumvention of the TPM, no violation of the DMCA anti-circumvention rules could occur.[264]

2. *Broader Implications of the Lock-out Technology Cases*

While this trio of cases—*Lexmark*, *Chamberlain* and *StorageTek*—reached the right results, they failed to consider a fundamental postulate of U.S. intellectual property law, namely, that the exclusive rights that copyright law confers cannot be used to defeat competitive uses of non-copyrightable functional products or features that are suitable for regulation under the more pro-competitive mandate of the patent laws.[265] This proposition, established by the Supreme Court in the 1880 landmark case of *Baker v. Selden* and extended by *Baker*'s progeny, stands for the necessity of maintaining a clear line of demarcation between industrial and artistic property laws.[266] Properly understood, *Baker v. Selden* authorizes intermediate copying of even an entire copyrightable work in order to extract the non-copyrightable functional elements, so long as the competi-

262. *Id.* at 1318. However, the *StorageTek* decision opens the disquieting possibility that a better-drafted contract could exclude the provision of competing repair services by express terms that this court would uphold. *Id.* at 1316-17.

263. *Id.* at 1319.

264. *Id.*

265. Baker v. Selden, 101 U.S. 99 (1880). *See, e.g.*, Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1993) (affirming the lawfulness of reverse engineering of copyrighted software to get access to interface information which was beyond the scope of copyright protection); Atari Games Corp. v. Nintendo of Am., Inc., 975 F.2d 832 (Fed. Cir. 1993) (accord).

266. *See generally* J. H. Reichman, *Computer Programs as Applied Scientific Know-How: Implications of Copyright Protection for Commercialized University Research*, 42 VAND. L. REV. 639, 649 n.288 (1989) (analyzing historical meaning of *Baker v. Selden* and criticizing commentators' misinterpretations, especially that of Melville Nimmer's treatise); Pamela Samuelson, *Why Copyright Law Does Not Protect Processes and Systems*, 85 TEX. L. REV. 1921, 1944-61 (2007) (demonstrating that Nimmer's interpretation of *Baker* is unsound).

tor's ultimate production avoids any unnecessary taking of protected expression.[267]

Unfortunately, some commentators have obscured the pristine meaning of *Baker v. Selden*,[268] which Professor Kaplan, among others, clearly understood.[269] There has been a regrettable tendency to treat *Baker* as merely endorsing a form of fair use in cases involving functional works[270] rather than as an independent and fundamental, perhaps even constitutionally based, subject matter requirement of the federal intellectual property system.[271] *Baker v. Selden*, properly understood, establishes fundamental limits on the ability of copyright owners to exercise control over the development of technologies because this would bypass the strictures of the patent law.[272] Because of this, the DMCA cannot override *Baker* and its fundamental policy prescriptions cannot be frustrated by the provisions of that Act.[273] There is, moreover, no legislative history suggesting that Con-

---

267. *See* Pamela Samuelson, Baker v. Selden: *Sharpening the Distinction Between Authorship and Invention*, *in* INTELLECTUAL PROPERTY STORIES 181, 181-92 (Rochelle Cooper Dreyfuss & Jane C. Ginsburg, eds. 2004) (discussing *Baker*'s repudiation of copyright protection for useful arts and its implications for the lawfulness of reverse engineering uncopyrightable technologies).

268. *See, e.g.*, 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT §§ 2.03, 2.18 (2006) (interpreting *Baker* narrowly).

269. *See* BENJAMIN KAPLAN, AN UNHURRIED VIEW OF COPYRIGHT 63-66 (1966). *See also* Reichman, *supra* note 266, at 649 n.288; Samuelson, *supra* note 266, at 1953-61; Lloyd L. Weinreb, *Copyright for Functional Expression*, 111 HARV. L. REV. 1149, 1175 (1998).

270. Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1993); Atari Games Corp. v. Nintendo of Am., Inc., 975 F.2d 832 (Fed. Cir. 1993).

271. U.S. CONST. art. I, § 8, cl. 8 (giving Congress power to "promote the progress of science and useful arts, by securing to authors and inventors exclusive rights for limited times for their *respective* writings and discoveries" (emphasis added)). *See also* J.H. Reichman, *Legal Hybrids Between the Patent and Copyright Paradigms*, 94 COLUM. L. REV. 2432 (1994) (discussing the fundamental premises of patent and copyright regimes).

272. Insofar as *Sony* held that technologies lacking in substantial non-infringing uses can be regulated by copyright law, even if technologies with substantial non-infringing uses cannot be, we regard *Sony* as consistent with *Baker*'s fundamental precepts.

273. We are concerned about whether federal appellate courts will vindicate the pristine meaning of *Baker v. Selden* or even perceive its critical importance for satisfactorily resolving this class of cases on more than an ad hoc, tentative grounds. We are also concerned about the Federal Circuit's tendency to defer in some cases to so-called "contractual" terms (regardless of the lack of meaningful assent by the "licensee") of mass-marketed products, which undermines our confidence in the staying power of that court as a check on abuses of public interest limitations on intellectual property rights. *See, e.g.*, Monsanto Co. v. McFarling, 363 F.3d 1331 (Fed. Cir. 2004) (enforcing "license" on bag of seeds sold to a farmer). Courts dealing with Lexmark or Chamberlain-like DMCA claims may find it useful to consider Professor Burk's intriguing theories of "anticircum-

gress intended to override *Baker* and its progeny in adopting the DMCA anti-circumvention rules.

The Federal Circuit deserves considerable praise for expressly recognizing that balance is a bedrock principle of intellectual property law and for developing a framework for interpreting section 1201 that enables courts to develop a balanced approach to interpretation of the DMCA's anti-circumvention rules insofar as copyright owners try to use them to block fair and other non-infringing uses of technically protected copyrighted works. Just as the court in *Netcom* rejected the White Paper's unbalanced and overly broad interpretation of the reproduction right,[274] courts interpreting section 1201 should reject *Reimerdes*' unbalanced and overly broad interpretation of section 1201 in favor of the framework set forth in *Chamberlain* and *StorageTek*, which we believe is far more consistent with the letter and spirit of the WCT and with Congressional intent in enacting the anti-circumvention rules.

D. The Reverse Notice and Takedown Framework

Building on the insights of *Chamberlain* and *StorageTek*, courts faced with public interest challenges to the DMCA anti-circumvention rules should follow *Netcom*'s lead by developing a notice and takedown approach to balancing the interests of copyright owners and the public.. A reverse notice and takedown procedure to enable privileged uses of technically protected works is consistent with section 1201. It would lower the barrier to entry for public interest users and reconcile the tensions between sections 1201(a) and 1201(c).

1. The Basic Concept

Under our proposal, any confrontation between the user community's efforts to make non-infringing uses of material available to the public on a website and the copyright owners' technological fencing under section 1201 could elicit a demand from the user group for a right to a limited bypassing of TPMs for legitimate purposes. For example, they might assert a need to index the material in question and extract specified components, in order to complete a specified non-infringing project. Copyright owners could be given fourteen days either to object to the limited circumvention or to allow it by silence, without prejudice. In case of denial, the user

---

vention misuse." Burk, *supra* note 152. This would avert the risk posed if the DMCA anti-circumvention rules allowed every product sold on the general products market to obtain 150 years of copyright protection behind digitized electronic fences that have nothing to do with the protection of literary and artistic works.

274. *See supra* note 33 and accompanying text.

group would be entitled to seek a declaratory judgment to vindicate its claim to an entitlement to circumvent a TPM for the purpose of engaging in the specified non-infringing use.

To become fully operational, this proposal would benefit from standardized procedures concerning the form in which notice should be given to copyright owners for "reverse notice and takedown" demands. It would also require courts to allow those providing needed decryption skills and technology to benefit from the same privileged use exception that a *demandeur* had ultimately vindicated either in court or by silent acquiescence of the copyright owner. Above all, such a regime would particularly benefit from the kind of expeditious, low-cost administrative tribunals proposed in other contexts.[275]

These long-term considerations should not, however, obscure the feasibility or desirability of immediately instituting ad hoc case-by-case judicially devised reverse notice and takedown procedures to promote the formation of a jurisprudence of permissible non-infringing uses of technically protected content to complement and supplement the jurisprudence of infringing uses discussed above.[276] *Netcom* has shown that courts in the U.S. can evolve balanced solutions in response to digital copyright problems. Reverse notice and takedown procedures could attenuate the tension between section 1201(a) of the DMCA, which on its face seems oblivious to fair use and other permissible uses of technically protected content, and section 1201(c), which seeks to preserve public interest uses. The exact contours for attaining this goal need to be worked out over time.

Section 1201(a) might seem to imply that it is not lawful to develop self-help decryption devices to crack the technological fence and remove unprotected or unprotectable matter. But bona fide non-infringing users should be able to petition for the right to have a tool to extract specified matter for specified non-infringing uses. If these proposals are documented by supporting evidence, they could trigger recourse to section 1201(c) in order to prevent section 1201 from perversely thwarting legislatively and judicially sanctioned permitted uses.

Resort to a reverse notice and takedown procedure of this kind would help make the DMCA into an instrument that promotes adequate protection of copyrighted works without creating barriers to entry that thwart

---

275. *See, e.g.*, Lipton, *supra* note 14, at 149-55.

276. After all, the "notice and take down" provisions of section 512 of the DMCA emerged from a negotiated compromise derived from the teachings of prior case law on contributory infringement in the digital environment. *See supra* notes 36-57 and accompanying text.

new technologies for sharing unprotected matter. It could facilitate licensing to nonprofit entities on reasonable terms and conditions, and it could help to frustrate growing tendencies to put public domain matter off limits by encasing it in impenetrable electronic fences. It could also attenuate the systematic use of digitized, electronic prior restraints on speech, which are likely to eventually provoke constitutional challenges.[277] Indeed, an extension of the reverse notice and takedown model could present would-be users of public domain material with a workable choice between sustaining the costs of securing and implementing judicially approved circumvention or purchasing the public domain matter from the vendor at reasonable prices for the sake of convenience.

2. *Illustrative Applications*

Below are four examples of situations in which courts might find the proposed reverse notice and takedown procedure useful:[278]

(1) Some years ago, the American Civil Liberties Union challenged the constitutionality of a law requiring public libraries to install filtering software if they take funds to promote Internet access to patrons. The filters were meant to protect minors from accessing indecent or otherwise harmful materials. However, such software under- and over-blocks content, and it impedes access to materials which, though harmful to minors, may qualify as constitutionally protected speech for adults.[279] When the Supreme Court ultimately ruled against the constitutional challenge, it recognized the under- and over-blocking problem, and held that over-blocking interfered with the legitimate interests of adults in accessing some blocked materials.[280]

---

277. *Cf.* Benkler, *supra* note 14, at 414-29 (challenging the constitutionality of the DMCA anti-circumvention rules); Ginsburg, *supra* note 14, at 21 (anticipating such challenges).

278. These examples largely reflect the scope for the proposed reverse notice and takedown procedure under U.S. law. As we explain in Part IV, we believe that the reverse notice and takedown procedure would also be an appropriate and desirable means for EU member states to implement their obligations under the Copyright Directive. But the precise scope of those obligations is a matter that different member states have read differently. *See infra* text accompanying notes 326-327. For other examples of public interest uses that have been or may be thwarted or chilled by the DMCA, *see, e.g.*, Benkler, *supra* note 14, at 388-89; Ginsburg, *supra* note 14, at 20; Lipton, *supra* note 14, at 113-15; Sadd, *supra* note 14, at 321-22; Samuelson, *supra* note 14, at 544-45, 548-49, 553. *See also* UNINTENDED CONSEQUENCES, *supra* note 112.

279. United States v. Am. Library Ass'n, 539 U.S. 194 (2003).

280. Justices Kennedy and Breyer thought that the interests of adults in access to a wider array of materials was adequately addressed by provisions of the Congressional legislation that allowed libraries to unblock sites for patrons wishing to view blocked but

The challenge for libraries since that decision has been to decide whether to install filters, and if installed, which filtering software to choose. Libraries may want to conduct a comparative assessment of the efficacy of software filtering programs, but filtering software will likely use TPMs to block access to the list of sites that the software blocks. Because makers of filtering software are likely to consider block-lists as proprietary trade secrets, they are unlikely to agree to bypassing the TPMs. Library staff may also lack sufficient expertise to bypass the TPMs to make such an assessment.[281]

It is in the public interest for libraries to have access to this information. Under a reverse notice and takedown procedure, a court could order the software filtering firms to take down the TPMs so that the comparative analysis could take place. The software filter developer could petition the court to condition the takedown on the libraries' willingness not to reveal the trade secret block-lists. We have confidence that courts could fashion appropriate relief that balanced the interests of the libraries in being able to communicate findings with other librarians and the interests of the software developers in keeping the list data secret.

(2) A linguistics professor might want to develop a compilation of clips from movies to show that the word "redskins" in Western movies has been systematically used in a derogatory fashion.[282] If this professor is not a technically sophisticated person, he or she may not be able to bypass CSS in order to make these clips from DVD movies. If the professor requests access to unprotected forms of these movies to engage in the stated fair uses and this request is ignored or denied by the motion picture studio copyright owners, the linguistics professor should be able to ask a court to

---

nonetheless lawful content. *Id.* at 214-15 (Kennedy, J., concurring); *id.* at 215-20 (Breyer, J., concurring). Unblocking may, however, involve circumvention of a TPM, which could run afoul of section 1201(a)(1)(A).

281. *See* Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 790-91 (2007) (discussing an effort to reverse engineer a TPM to get access to block-list information for filtering technologies, such as those widely used by libraries, that was thwarted by threats of DMCA anti-circumvention liability).

282. *See* Samuelson, *supra* note 14, at 540 (giving this example). Public interest users should not, in our judgment, have to undertake extra expense and effort to search for possible alternative formats for the works of which they want to make fair use when a technically protected format is near at hand. In this respect, we join the EFF's criticism of the Copyright Office for its unwillingness to consider the inconvenience and expense of such efforts as a factor favoring permitting fair use exemptions for such users. *See* EFF on Rulemaking, *supra* note 138, at 4-5.

order the studios to provide the appropriate access to the movies or to authorize the takedown by a circumvention service on their behalf.[283]

(3) The Computer History Museum is among the entities that might want to undertake a project to preserve computer programs written during the 1960's to early 1980's.[284] Some software developers have employed TPMs to control access to the programs; many programs are, moreover, stored in now-obsolete formats and/or on obsolete storage media that have effectively become TPMs. A Computer History Museum researcher would have to bypass the TPMs to preserve this historical material and store it in updated formats. Rather than waiting three years for the next LOC rulemaking,[285] Computer History Museum personnel should be able to ask a court to issue a reverse notice and takedown order insofar as copyright owners of the software did not agree or could not be found to give consent to bypassing the TPM.[286]

(4) Security researchers are often interested in reverse engineering TPMs, such as those used to protect commercially distributed sound recordings, for purposes such as determining if the TPMs might cause software to be installed on users' computers that would cause the computers to

283. *See, e.g.*, Ginsburg, *supra* note 14, at 17 (suggesting that judges could authorize circumvention services to facilitate fair uses of works protected by TPMs).

284. It is not entirely clear whether computer programs in machine-executable forms would have been protectable under the Copyright Act of 1909, although the U.S. Copyright Office began accepting registration of computer programs as copyrightable works in the mid-1960's. *See* Copyright Office Circular 31D (Jan. 1965), *reprinted in* Duncan M. Davidson, *Protecting Computer Software: A Comprehensive Analysis*, 1983 ARIZ. ST. L.J. 611, 652 n.72. Obviously, bypassing a TPM protecting access to programs written in this period would not give rise to section 1201 liability if the programs were not copyrightable, but the risk for a preservationist in circumventing these old TPMs would nevertheless be real, given the registrations accepted then.

285. 17 U.S.C. § 1201(a)(1)(C). There is currently a partial exemption for libraries and archives to bypass a TPM to preserve digital content stored in obsolete formats, but this may not apply to museums and it certainly does not authorize the making of tools in order to engage in such circumventions. *See* Perzanowski, *supra* note 142, at 16 (discussing the narrowness of the exception for obsolete formats).

286. Difficulties in locating copyright owners have prevented many creative and educational reuses of copyrighted works, especially many older ones. The U.S. Copyright Office has proposed allowing reuses of so-called "orphan works" to proceed if the reusers have made reasonably diligent efforts to seek permissions. *See* U.S. COPYRIGHT OFFICE, REPORT ON ORPHAN WORKS 8 (2006). A similar problem may arise with TPMs. With the possibility of up to $2500 of statutory damages per circumvention at stake for violation of section 1201, *see* 17 U.S.C. § 1203(c)(3), there is a risk that public interest users, such as archivists, would be deterred from preservation activities. With a reverse notice and takedown procedure, the archivist could be assured that he or she would incur no liability for this circumvention as long as he or she did not infringe copyrights in the works.

be vulnerable to security attacks or that might surreptitiously monitor and report back on users' behaviors.[287] Undertaking such research would almost certainly involve bypassing the TPM and making tools to do so. Given the narrowness of the encryption research or computer security testing exceptions to section 1201, this activity would probably not qualify for a statutory safe harbor.[288] Yet, the work would nevertheless be in the public interest, even if the right holder in the sound recording did not approve of this activity.

Security researchers ought to be able to engage in such reverse engineering and to disclose the results of their research at scientific conferences.[289] In keeping with the reverse notice and takedown regime, a court could determine that research-related activities of this sort are lawful under a proper interpretation of section 1201.

3. *Other Considerations*

Although it would be more cost-effective to have a streamlined administrative process for considering reverse notice and takedown requests,[290] a

---

287. *See, e.g.*, Deirdre Mulligan & Aaron Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. 1157 (2007). Another public interest issue posed not only by the Sony BMG rootkit incident but more generally is that right holders do not always give notice that they have deployed TPMs in mass-marketed digital content. Without notice of TPMs, it becomes possible to inadvertently violate sections 1201(a)(1)(A) and 1201(a)(2) if one reverse engineers a purchased copy of digital content. For a discussion of this issue and the policy issues it raises, see Pamela Samuelson & Jason Schultz, *Regulating Digital Rights Management Technologies: Should Copyright Owners Have to Give Notice About DRM Restrictions?*, J. TELECOMM. & HIGH TECH. L. (forthcoming 2007).

288. If, for example, the TPM does not use encryption, but some other technique, the encryption research exception would, strictly speaking, not apply. *See* 17 U.S.C. § 1201(g). The computer security testing exception only applies if one is testing a computer network for security flaws. *Id.* at § 1201(j). The unduly narrow nature of these exceptions is discussed in DIGITAL DILEMMA, *supra* note 113, at 171-76.

289. *See, e.g.*, Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L.J. 501, 528-37 (2003) (arguing for flexibility in the anti-circumvention regulations as applied to scientific research). It is worth pointing out that security researchers are unlikely to be interested in getting access to the digital content protected by the TPM; they are primarily interested in the TPM itself and how it might interact with the content. As long as such researchers do not engage in or knowingly facilitate copyright infringement, their activities should not violate the DMCA. A reverse notice and takedown regime could be adapted to facilitate such research.

290. *See, e.g.*, Lipton, *supra* note 14, at 155 ("Administrative approaches tend to be more flexible and less formal in their procedures than judicial processes and are generally less costly than judicial hearings."). We recognize that our proposal has at least two disadvantages. First, few prospective privileged users may have the resources to seek judicial support for reverse notice and takedown challenges to technically protected content,

judicially developed case-by-case evolution is, in our judgment, preferable to a statutorily mandated administrative process. The case-by-case approach is more dynamic, flexible, and responsive to the fine details of each situation. It is, moreover, likely to lead to a normative framework for dealing with such requests. We fear that a statutorily created administrative process at this point would remain vulnerable to political economy problems akin to those that brought about the unbalanced DMCA anti-circumvention rules in 1998.

Once the courts develop normative baselines for dealing with reverse notice and takedown requests, however, an administrative process could evolve over time to apply and refine this normative framework. This development could also induce copyright owners to engage in private initiatives consistent with this framework, such as designating circumvention services to which putative public interest users might apply to obtain circumvention for non-infringing purposes.[291]

We believe that courts will be able to discern when putative public interest users are not acting in good faith when making reverse notice and takedown requests. Courts can also put in place safeguards to ensure that the reverse notice and takedown regime does not bring about the increased

---

and second, the prospective privileged users will have to identify themselves to the copyright owner rather than making spontaneous fair or other non-infringing uses without informing the relevant copyright owners. *See* Burk & Cohen, *supra* note 14, at 59-61 ("[A] preauthorization requirement would be costly and would chill spontaneous uses. . . . [A]pplication to a third party is likely to compromise the sort of anonymity that users presently enjoy. . . . Spontaneous uses likely would disappear altogether. . . . [U]nder this system, fair use might become the sole provenance of well-capitalized firms with the resources to engage in the process.").

The first problem may be mitigated by the rise of public interest organizations (including nonprofit organizations such as the Electronic Frontier Foundation and high technology clinics such as those in operation at American University, Boalt Hall, Stanford, and USC Law Schools) with the capacity to represent prospective fair users. Moreover, in time, an administrative process might be set up to resolve these challenges, as Lipton proposes, *supra* note 14, at 149-55.

As to the second problem, a comparative approach is necessary. Realistically, the fair use infrastructure that Burk and Cohen propose is less likely to be achievable than the reverse notice and takedown procedure we propose. So while their proposal is more socially optimal than ours in that copyright owners would not have to know the identity of the prospective fair user, ours is more socially optimal in that courts can actually make it happen. Moreover, a reverse notice and takedown procedure might, in time, lead to something akin to the fair use infrastructure they envision, if copyright owners found it more efficient to designate a service to deal with public good circumvention claims instead of having to respond to them on a regular basis.

291. Indeed, this may be a way to accomplish the "fair use infrastructure" that Burk and Cohen envisioned some years ago. *See* Burk & Cohen, *supra* note 14.

infringements that the DMCA was enacted to avoid (for example, by ordering copyright owners to make use of trusted circumvention services rather than ordering takedowns of the TPMs that might lead to massive infringements).

Whether courts in the United States will, in practice, defend good faith public interest communities against technologically induced inhibitors of non-infringing uses with the same zeal they have thus far used in guarding against online inducers of infringement in *Napster*, *Aimster,* and *Grokster* remains to be seen. Certainly, the logic with which the courts have justified limitations on regulation of dual-use technologies resonates with similar concerns to vindicate non-infringing uses of technically protected content and to remove barriers now thwarting development of appropriate technologies to achieve this goal. A judicially engrafted reverse notice and takedown solution could provide a minimalist bridging device to achieve this balance. *Chamberlain* and *StorageTek* provide a conceptual framework for an interpretation of section 1201 out of which the reverse notice and takedown approach we propose could develop through common law adjudication.

IV. REVERSE NOTICE AND TAKEDOWN AS A MODE OF IMPLEMENTING ARTICLE 6(4) OF THE EU COPYRIGHT DIRECTIVE

As noted earlier, the reverse notice and takedown approach is eminently consistent with the WCT, which expressly reserved legally permitted uses from the scope of the obligatory anti-circumvention measures.[292] In countries that adopted the treaty verbatim, such as Japan, there can be no domestic or international objections to any effort to introduce the reverse takedown and notice approach. Because of the civil law traditions prevalent in the EU, it would not be feasible for member states to adopt the reverse notice and takedown regime through common law litigation. So it is fortunate that the EU Copyright Directive has provided a general (if incomplete) framework for member states to achieve a balanced solution by providing legal reinforcement of TPMs used by copyright owners

292. WCT, *supra* note 1, art. 11, which states:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or *permitted by law.*

Id. (emphasis added).

to protect their works while at the same time enabling public interest uses of technically protected content.

Indeed, Article 6(4) of the EU Copyright Directive *requires* member states to adopt mechanisms that preserve the ability of users to take advantage of certain exceptions and limitations guaranteed by copyright law notwithstanding the application of TPMs.[293] The proposed reverse notice and takedown procedure is one way in which member states could fulfill that obligation.[294] Moreover, such a procedure would effectuate the basic normative commitment to the continued availability of exceptions to exclusive rights expressed in Article 6(4).[295] In fact, it does so more fully than current member state implementation of the Article (which has arguably been confined by textual limits on the scope of Article 6(4)) itself.[296]

In this part, we explain the basic contours of Article 6(4) of the Directive, and how adoption of the reverse notice and takedown procedure would implement member states' obligations under that provision. This discussion also allows us to elaborate further on some aspects of the proposal already mentioned in Part III.

A. The Unfulfilled Normative Commitment Underlying Article 6(4)

The EU Copyright Directive starts from the general normative position that exceptions and limitations that would have been available absent the application of TPMs should remain available notwithstanding the application of such measures.[297] Unlike the DMCA, the Copyright Directive does not contain a list of exemptions from the circumvention prohibitions.[298]

---

293. *See* Copyright Directive, *supra* note 10, art. 6(4).

294. *See infra* Section IV.C.

295. *See infra* Section IV.A.

296. *See infra* text accompanying notes 311-314. For a summary and analysis of member state implementation, see Guido Westkamp, *The Implementation of Directive 2001/29/EC in the Member States* (Feb. 2007), *in* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11.

297. *See* Copyright Directive, *supra* note 10, art. 6(4). Of course, this is not the only normative commitment embodied in the Directive. The Commission also sought to create a climate in which copyright owners would pursue new business models for online distribution of content. Reconciliation of these competing policy objectives may explain, although not coherently, the different constrictions on Article 6(4). *See infra* text accompanying notes 311-314.

298. Recitals 48 and 51 of the Directive suggest the possibility of exemptions for cryptography research and public security. *See id.*, recitals 48, 51; *see also* Richard Li-Dar Wang, *DMCA Anti-Circumvention Provisions in a Different Light: Perspectives from Transnational Observation of Five Jurisdictions*, 34 AIPLA Q.J. 217, 237 (2006). Because the Directive lacks any specific exemptions, it is seen by some as rejecting any

However, the EU legislators were aware of the risk that TPMs might become an absolute prohibition restricting users from engaging in acts permitted under traditional copyright law.[299] Concern about that prospect found expression in Article 6(4).[300] The first paragraph of Article 6(4) provides that:

> Notwithstanding [the prohibitions against acts of circumvention and circumvention devices], in the absence of voluntary measures taken by right holders, including agreements between right holders and other parties concerned, member states shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation provided for in national law in accordance with [various articles in the Directive listing permissible exceptions to copyright, such as copyright in connection with teaching], the means of benefiting from that exception or limitation .... [where that beneficiary has legal access to the work].[301]

The Directive thus seems to take the position that a technological adaptation, namely, the application of TPMs, should not alter the balance that existed under default rules of copyright law with respect to the en-

---

right of "self-help." However, some member states have implemented rights of self-help to circumvent TPM under strict conditions. *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 106 (describing Norwegian and Danish implementation). Moreover, there is nothing in the Directive to suggest that the "appropriate measures" called for by Article 6(4) might not include immunity from liability after the right holder had failed to make available the means of benefiting from an exception or limitation. *See id.* at 108-109 (noting the Directive's preference for voluntary arrangements by right holders, but suggesting that the broad language of "appropriate measures" leaves much room for member states to adopt different approaches); *cf.* Christophe Geiger, *The New French Law on Copyright and Neighbouring Rights of 1 August 2006—An Adaptation to the Needs of the Information Society?*, 38 IIC 401, 421-23 (2007) (noting the dangers of deferring entirely to right holder arrangements and arguing that "the only measure that would truly have been 'appropriate' within the meaning of Article 6(4)" would have been a prohibition on right holders applying TPM to deprive the public of the benefit of exceptions with a "pronounced social function").

299. *See* LIONEL BENTLY & BRAD SHERMAN, INTELLECTUAL PROPERTY LAW 309-11 (2d ed. 2004) (noting fears expressed).

300. *See* Bernt Hugenholtz, *Why the Copyright Directive is Unimportant, and Possibly Invalid*, 22 EUR. INTELL. PROP. REV. 501 (2000) (describing article 6(4) as "a provision that is presumably intended to reconcile the interests of right owners employing technical protection measures with the interests of users wishing to benefit from copyright limitations"); BENTLY & SHERMAN, *supra* note 299, at 310 ("As regards the relationship between the technological measures and exceptions to copyright, article 6(4) of the [Copyright Directive] provides for a strange, barely comprehensible, compromise.").

301. *See* Copyright Directive, *supra* note 10, art. 6(4).

joyment of exceptions and limitations.[302] We call this principle "prescriptive parallelism," to convey the notion that the traditional copyright balance of rights and exceptions should be preserved in the digital environment.[303]

Article 6(4) is only one dimension of parallelism in the EU Directive. It also contains a provision that anticipates a reduction in private copying levies under national copyright laws, potentially to zero, where copyright owners have applied TPMs to works and thus secured by technology what they formerly obtained through legally sanctioned levy schemes.[304] Copyright owners should not be able to double dip, and should receive the same level of effective protection, whether through law or technology.

We do not want to overstate the principle of prescriptive parallelism underlying the EU Directive. Article 6(4) is a means by which the EU sought to ensure that the balance of copyright law was maintained after the application of technological protection measures.[305] But that goal is pursued against the broader backdrop of a Directive that contemplates adjustments to the legal rights of both copyright owners and users to reflect the availability and application of such measures. For example, one of the principal objectives of the EU Directive was to provide legal protection against circumvention of technological protection measures, which might be conceived as enhanced legal protection for copyright owners in light of enhanced copying capacity.[306]

Moreover, the prescriptive parallelism of Article 6(4) must also be viewed against the treatment of exceptions by the EU Directive generally.

---

302. Article 5(3)(o) also permits member states to create exceptions or limitations to rights provided for in articles 2 and 3 "in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses . . . ." Copyright Directive, *supra* note 10, art. 5(3)(o).

303. Compare the similar concept expressed in Agreed Statements, *supra* note 2, statement concerning art. 10.

304. Article 5(2)(b) of the Copyright Directive permits member states to create exceptions or limitations to the reproduction right "in respect of reproductions on any medium made by a natural person for private use . . . on condition that the right holders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work for subject matter concerned." Copyright Directive, *supra* note 10, art. 5(2)(b).

305. *See* Hugenholtz, *supra* note 300, at 501.

306. *See* Copyright Directive, *supra* note 10, art. 6(1)-(2). During the legislative debates, the Commission apparently suggested that *all* exceptions listed in Article 5 should explicitly prevail over contrary TPMs, and Article 6(4) was the compromise provision that reconciled the Commission's position with that adopted by the Council of Ministers (which was more supportive of right holders' freedom to use TPMs). *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 104.

Although the stated objective of the Directive was in part to harmonize the disparate sets of exceptions and limitations available under national copyright laws in the EU, the Directive effected only a very modest amount of harmonization, at least in the short run.[307] Its broad list of exceptions is largely permissive,[308] although there is a mandatory exception for ephemeral copies,[309] and there is a restriction on adoption of further exceptions.[310]

More importantly for purposes of this Article, the failure to *mandate* the adoption of a wide range of exceptions undermines the effectiveness of Article 6(4) in achieving its general goal of prescriptive parallelism. Article 6(4) only guarantees that technological protection measures should not impede the ability of third parties to take advantage of exceptions or limitations if they are provided in national law.[311] Furthermore, there are a number of other significant textual constraints on the potential effectiveness of Article 6(4), including its limitation to seven defined exceptions rather than all exceptions or limitations existing in national law,[312] its in-

307. *See generally* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11; *see also* INST. FOR INFO. LAW, UNIV. OF AMSTERDAM, THE RECASTING OF COPYRIGHT AND RELATED RIGHTS FOR THE KNOWLEDGE ECONOMY (2006). These studies were commissioned by the European Commission's Internal Market Directorate-General.

308. *See* Copyright Directive, *supra* note 10, art. 5(2)-(3) (providing that member states *may* provide for certain exceptions or limitations); *see also* Hugenholtz, *supra* note 300.

309. *See* Copyright Directive, *supra* note 10, at art. 5(1). The Directive states:

> [T]emporary acts of reproduction . . . which are transient or incidental and an integral and essential part of the technological process and whose sole purpose is to enable a transmission in the network between third parties by an intermediary, or a lawful use, of a work or other subject matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right.

Id.

310. *See id.* at recital 32. *But see id.*, art. 5(3)(o) (quoted *supra* note 302). It might be that over time the mere listing of permissible exceptions will cause a convergence as different national legislators begin to work from the same turnkey list, secure in the knowledge that adopting such exceptions will not meet with the objections of the European Commission.

311. *See id.* at art. 6(4).

312. These include exceptions for copying by libraries and educational institutions, copying for the benefit of persons with a disability, and copying for the purpose of scientific research. There is no coherent explanation, other than raw political compromise, for the inclusion of these exceptions but not others in Article 6(4). *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 110 ("Because this provision was negotiated in the last hours before adoption of the final text of the Directive, there is no public record available to shed light on the legislator's intent. As a result, the list of limitations included in Article 6(4) appears highly arbitrary."). Indeed, the arbitrariness of the list

applicability to works made available on-demand,[313] and its unclear relationship with the anti-circumvention and interoperability provisions in the Software Directive.[314]

These limitations in the text of the Directive have caused many scholars to doubt the capacity of the provision to achieve its declared objectives.[315] In deference to ordinary canons of interpretation, we are reluctant

---

may simply reflect the broader failure of the Directive to rationalize treatment of exceptions generally. *See id.*

Moreover, Article 6(4) does not, for example, include uses that users are entitled to make because a work is in the public domain or because all that is taken is otherwise unprotected by copyright law. It can be argued that the protections of Article 6 do not apply to public domain material in the first place because right holders are not in a position to authorize uses of such works. As a result, some national legislatures have taken the position that TPMs on public domain works can be circumvented without liability. *See* Urheberrechtsgesetz [Copyright Act], Sept. 12, 2003, BGBl. I at 1774, art. 1, §95(a)(2) (F.R.G.). Of course, in practical terms, if right holders package public domain works with some protected works, it is unclear whether this interpretation will be sufficient to save access to such works without more affirmative legislative statement. *See* BENTLY & SHERMAN, *supra* note 299, at 309.

313. The mechanisms of article 6(4) do not apply where the work is made available on an on-demand basis because the provision is inapplicable where "the work or other subject matter is made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at the time individually chosen by them." The language of this sentence in the directive itself makes the scope of the limitation uncertain and could be tested in a number of ways. *See* BENTLY & SHERMAN, *supra* note 299, at 311 n.132 (noting room for dispute regarding the phrase "agreed contractual terms"); *see also* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 112 (suggesting that confining this limit on Article 6(4) to negotiated contracts would be consistent with the legislative purpose).

More importantly, the on-demand language surely cannot be read in ways that render the general provision meaningless. *See* Maciej Barczewski, *International Framework for Legal Protection of Digital Rights Management Systems*, 27 EUR. INTELL. PROP. REV. 165, 167 (2005) (noting that reading the "available contractually on-demand" limits in Article 6(4) in ways that allowed digital lock-up of all works available online would conflict with the directive's aims); *see also infra* text accompanying note 323. The same interpretive rationale surely should be applied to yet another limit on Article 6(4), namely, that because the provision only applies where the beneficiary has legal access to a work, it is arguably ineffective against access control measures. *See* Severine Dusollier, *Fair Use by Design in the European Copyright Directive of 2001*, COMM. OF THE ACM, Apr. 2003, at 51, 53-54 (2003) [hereinafter *Fair Use by Design*]; Dusollier, *supra* note 11.

314. Council Directive 91/250/EEC, 1991 O.J. (L 122) 42 (EC) [hereinafter Software Directive]. The anti-circumvention provisions and interoperability exceptions in the Software Directive appear to survive the adoption of Article 6. *See* Copyright Directive, *supra* note 10, recital 50; *see also* Software Directive, *supra*, art. 7(1)(c); BENTLY & SHERMAN, *supra* note 299, at 311-312 (discussing UK implementation and noting different treatment of software).

315. *See* Hugenholtz, *supra* note 300; Dusollier, *Fair Use by Design*, *supra* note 313.

to read the limits in Article 6(4) in ways that render the general provision meaningless.[316] However, rather than focus on the details of the limitations of Article 6(4) as enacted, and perhaps looking forward to the possible revision of the Directive to take into account a recent report commissioned from the University of Amsterdam Institute for Information Law,[317] we will view the conceptual mechanism of Article 6(4) as a means of ensuring continued viability of privileged uses notwithstanding the application of technological protection measures. More particularly, we will consider the reverse notice and takedown proposal as a vehicle for implementing Article 6(4) and exploring its possible reform.

B. Reverse Notice and Takedown as a Mode of Implementing Article 6(4)

The reverse notice and takedown proposal articulated in Part III essentially consists of two parts. First, implicitly, all uses privileged under traditional copyright principles should continue to be privileged in an era of digital rights management. The application of TPMs should not alter the balance of rights between copyright owners and users.[318] This is a substantive principle, which might be followed with different modifications in different countries.[319]

Second, in order to effectuate this substantive principle, users need a mechanism by which to vindicate their rights and to secure the certainty required to engage in creative activity privileged under traditional copyright principles. Different institutional or procedural means through which

316. *See* Thomas Rieber-Mohn, *Harmonising Anti-Circumvention Protection with Copyright Law: The Evolution from WCT to the Norwegian Anti-Circumvention Provisions*, 37 IIC 182, 188 (2006) (offering an interpretation of which contractual arrangements by right holders would preempt member state intervention by reference to the need to give Article 6(4) some meaning); Barczewski, *supra* note 313, at 167.

317. *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11. That report concluded that "the principle underlying article 6(4) . . . is worth maintaining" but recommended that the provision be simplified and clarified in a number of ways that ensure its effectuation. *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 133.

318. *See, e.g.*, Paolo Spada, *Copia privata ed opera sotto chiave* ["Private Copies and Locked Down Works"], 2002(1) RIVISTA DI DIRITTO INDUSTRIALE 591, 597-598 (stating that the system of technological protection measures provided authors by the EC Directive must acknowledge the exceptions to authors' rights, including privileged uses, because "these are an integral part of the authors' rights system and not merely contingencies of contract or the owners' brute force") (trans. JHR).

319. Even within the traditional copyright system, exceptions are quite different from one country to the next. How each country might want to approach the digital environment is unlikely to be more uniform.

to pursue this objective are possible,[320] but we believe the reverse notice and takedown procedure affords a number of distinct advantages, many of which were canvassed in Part III.

As an initial matter, we believe the proposed reverse notice and takedown procedure should be considered as a means of implementing member state obligations under Article 6(4). This proposal should be studied by countries committed to compliance with the EU regime, which includes not only the member states of the EU, but also countries that commit to such a regime (whether in general terms or in detail) in bilateral trade negotiations.[321] Even if certain limits apparently embodied in Article 6(4) turn out to circumscribe its actual scope in EU member states,[322] member state implementation of a narrower provision (e.g., with respect only to certain exceptions) might still afford insights as to how the basic structure of the proposed reverse notice and takedown procedure could be enhanced to better ensure that anti-circumvention provisions are consistent with privileged uses.

Moreover, such an exercise might also highlight the ways in which Article 6(4) could itself be broadened as EU legislators consider a revision of the Directive in light of the recent report by the Institute for Information Law at the University of Amsterdam.[323]

---

320. For example, Professor Spada believes that the Directive entitles privileged users disadvantaged by TPMs to assert their rights under the Directive in national courts. *See* Spada, *supra* note 318, at 598.

321. Compliance with EU law is an obligation not only of all European Union member states, but also of member states of the European Free Trade Area (EFTA), as well as a number of countries pursuing future European Union membership or entering into bilateral trade agreements with the European Union. *See* MAXIMILIANO SANTA CRUZ, INT'L CENTRE FOR TRADE AND SUSTAINABLE DEVELOPMENT, INTELLECTUAL PROPERTY PROVISIONS IN EUROPEAN UNION TRADE AGREEMENTS: IMPLICATIONS FOR DEVELOPING COUNTRIES 2-3 (2007). In the past, the bilateral trade agreements negotiated by the EU have contained obligations with respect to intellectual property stated at a very general level, such as compliance with the WIPO Copyright Treaty. *See id.* at 10. In contrast, the United States has in its bilateral trade agreements sought to secure compliance with more detailed standards that resemble the language of the DMCA than the terms of the WCT. *See* Chander, *supra* note 18, at 206. However, some observers have detected a shift in the EU approach toward the more aggressive US approach in more recent negotiations. *See* SANTA CRUZ, *supra*, at ix-x, 18.

322. *See supra* text accompanying notes 311-314.

323. *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 132-33 (criticizing limits of Article 6(4)).

C. Application of Reverse Notice and Takedown Under Article 6(4)

Under Article 6(4), right holders are required to ensure that beneficiaries of exceptions have the ability to exercise those exceptions notwithstanding the application of technological protection measures to copyrighted works.[324] If right holders do not voluntarily ensure that result, member states are obliged to devise a mechanism to compel it.[325]

Member states have implemented this obligation in a number of different ways.[326] Each of the different forms of implementation offers a model for preserving privileged uses; yet, most are deficient and would benefit from a reverse notice and takedown procedure.[327]

1. Triggering an Entitlement to Relief

The reverse notice and takedown procedure would be available to any particular user who wished to engage in a privileged use with respect to even a single work. Thus, the threshold would be substantially lower than the "adverse effect on classes of work" standard found in the rulemaking authorization contained in the DMCA, even as refined under the 2006 rulemaking.[328] But this more generous approach is fully consistent with Article 6(4), which would appear to allow analysis of particular uses of particular works by particular users.[329]

One could argue that the unavailability of a single work to be put to a single use might be deemed insufficiently substantial a cost to justify the mechanisms contemplated by Article 6(4). But this calculus depends in part upon the nature of the mechanism and upon what is contemplated by the member state as an "appropriate measure" in response to any given

---

324. *See* Copyright Directive, *supra* note 10, art. 6(4).

325. *See id.*

326. *See generally* Westkamp, *supra* note 296; *see also* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 132 ("In some member states, only individual beneficiaries may claim the application of the limitation, while in other countries, interest groups and third parties also have the right to do so. In yet other member states, administrative bodies may be entitled to force right holders to make the necessary means available to beneficiaries of limitations.").

327. Of course, much of the blame can be laid at the door of the Directive itself. *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 132-33.

328. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68472 (Nov. 27, 2006) (to be codified at 37 C.F.R. §201) [hereinafter 2006 Rulemaking], at 6-7.

329. *See* Copyright Directive, *supra* note 10, art. 6(4) (incorporating by reference exceptions in Article 5 that involve particular uses for particular purposes including, for example, copying for the purpose of scientific research).

inability to exercise an exception granted by copyright law. If the procedure were speedy, and if "appropriate measure" meant one that permits a single circumvention, then there would be virtually no real cost to a state acting on the basis of a lower trigger threshold.[330]

Because the reverse notice and takedown procedure contemplates the possibility of relief in the form of a limited exemption for a particular user, it would seem perfectly appropriate that the obligation of member states should arise more easily than if broader relief were sought. As the recent refinement by the Librarian of Congress of the notion of "classes of works" reflects,[331] the sub-categories of privileged uses that emerge from a matrix of affected works, from groups of users, and from a range of uses, are substantial and disparate. Not only must different forms of relief be available, but also different levels of need to actuate permitted uses should trigger such relief.

The fact that relief under the reverse notice and takedown procedure might be appropriate even with respect to a single use of a single work should not preclude the possibility of using the procedure where technological protection measures are having a more pervasive effect. Arguably, the relief available under any state-imposed mechanism should reflect the degree and type of harm caused by the application of technological protection measures. Thus, member states may need to create more intrusive or structural relief for third-party users or competitors if lawful uses of entire classes of works are being impeded.[332]

While this type of analysis parallels that conducted by the Register of Copyrights in the triennial rulemaking to some extent, the reverse notice and takedown procedure might remedy some of the deficiencies of that procedure. In particular, despite refinement in the 2006 rulemaking of the notion of adverse classes, the Register remains limited in the relief that she can offer, namely, the grant of a temporary exemption to a specified category of works from the application of Section 1201.[333] And that relief does not immunize third parties who, through the distribution of devices, assist in ensuring that privileged uses are made. Moreover, the process occurs only every three years.[334]

---

330. *See* Symposium, *The Law & Technology of Digital Rights Management*, 18 BERKELEY TECH. L.J. 697, 760, 765 (2003) (remarks of Graeme B. Dinwoodie on Anti-circumvention Regulations in the United States and Elsewhere).

331. *See* 2006 Rulemaking, *supra* note 328.

332. *See* Symposium, *supra* note 330, at 765-66 (remarks of Dinwoodie).

333. *See supra* text accompanying note 137.

334. *See supra* text accompanying note 136.

Implementation of Article 6(4) in the United Kingdom includes the possibility that the complaint of obstruction to the exercise of privileged uses can be made on behalf of a class of users.[335] This type of claim should be a component of the reverse notice and takedown procedure. It would provide a useful, more flexible, and more dynamic complement to the rulemaking procedure.[336]

2. *Encouraging the Proper Role for Voluntary Arrangements*

We believe that the reverse notice and takedown proposal should be available to users and competitors even if copyright owners voluntarily make works available by overriding TPMs to some extent. In this respect, the proposal might appear to depart from the strict text of the EU Directive. Under the Directive, the obligation upon member states arises "in the absence of voluntary measures taken by right holders, including agreements between right holders and other parties concerned."[337] However, even though the provision contemplates some room for right holders to forestall legal intervention through voluntary arrangements such as contract, this freedom cannot be unlimited without rendering Article 6(4) meaningless.[338] In any event, we do not believe that right holders have, in fact, undertaken such voluntary measures thus far, which is why a reverse notice and takedown regime is sorely needed.

The very availability of the reverse notice and takedown procedure may, in fact, facilitate licensing on reasonable terms and conditions and

---

335. *See* Copyright and Related Rights Regulations, 2003, S.I. 2003/2498, art. 24, § 296ZE(2) (U.K.), *available at* http://www.opsi.gov.uk/si/si2003/20032498.htm ("person being a representative of a class of persons prevented from carrying out a permitted act"); *see also* Unterlassungsklagengesetz [UklaG, Injunctions Act], Aug. 27, 2002, BGBl. I at 3422, as amended by Urheberrechtsgesetz [Copyright Act], Sept. 10, 2003, BGBl. I at 1774, art. 3, § 3a (F.R.G.)

336. If the request could not be made on behalf of a class of users, there might arise the problem whether similarly situated third parties could rely on responses of copyright owners to a request from a user under the reverse notice and takedown procedure. To the extent that the request invokes a "purpose exception," it is unlikely that copyright owners would make distinctions between users and thus as a practical matter similarly situated third parties could rely on relief granted by copyright owners. To the extent that copyright owners did make distinctions for improper reasons, occasion may arise to invoke Dan Burk's proposed anti-circumvention misuse doctrine. *See* Burk, *supra* note 152. With respect to "identity" exceptions, persons falling within the group of beneficiaries entitled to exercise the exception should be able to take advantage (i.e., treat as "precedential") relief granted to others possessing the same identity.

337. Copyright Directive, *supra* note 10, art. 6(4).

338. *See* Rieber-Mohn, *supra* note 316, at 188 (arguing that voluntary measures by right holders must be "appropriate" in order to avoid member state intervention and must occur within a reasonable period of time).

induce other voluntary measures to ensure that exceptions can be exercised; voluntary measures that adequately preserved the ability to exercise those exceptions would obviate the need for member states to take further action against right holders. Whether acting in advance of the threat of later sanctions (under the general language of Article 6(4)), or under contemporaneous threat (in the case of the reverse notice and takedown procedure implementing that provision), the shadow of legal compulsion might foster private ordering that is more balanced in nature.[339]

The only type of "voluntary measure" expressly referenced in Article 6(4) is "agreements between right holders and other parties concerned."[340] However, reaching consensus among the vast range of interests now implicated by copyright law may be quite difficult. The process of legislating copyright law, which often approximates a contractual negotiation, has become tortuous and slow. It is unlikely that agreements between copyright owners and users over taking down TPMs will be easy to achieve.

Because many exceptions depend on the type of use, rather than the category of user (i.e., purpose exceptions, not identity exceptions), it may not suffice merely to identify the relevant beneficiaries with whom to negotiate. If the obvious categories of users are singled out as beneficiaries, focusing on identity exceptions, it will privilege traditional "fair use communities,"[341] which may constrain important sources of creativity. Consensus among collectives often ignores the needs of single users or users within very loosely organized communities, and the reverse notice and takedown proposal will accommodate these potentially important creators.

Agreements are not the only form of voluntary measure through which right holders might forestall the intervention of member states. For example, right holders might apply TPMs in ways that permit privileged uses. Although this outcome might seem ideal in theory, such an approach carries with it technological limitations. Implementing such fact-specific exceptions as the fair use doctrine or other privileged uses in computer code will prove immensely difficult.[342] Thus, this cannot be the sole mechanism through which to ensure privileged uses.

Moreover, such arrangements raise broader normative concerns. Relying on copyright owners accurately to map technology to legal rules dele-

339. Some private ordering has clearly occurred in the shadow of Article 6(4). *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 107.

340. *See id.*

341. *See also* Ginsburg, *supra* note 14.

342. *See* Nic Garnett, *Automated Rights Management Systems and Copyright Limitations and Exceptions*, WIPO Doc. No. SCCR/14/5 (Apr. 27, 2006), *available at* http://www.wipo.int/edocs/mdocs/sccr/en/sccr_14/sccr_14_5.doc.

gates immense power to those owners both in the interpretation of the default rules and in assessing the adequacy of the technology used to guarantee permitted uses.[343] Even if the copyright owners accurately interpreted and implemented existing permitted uses, technological features would remain inherently backward-looking.[344] One of the advantages claimed for the fair use doctrine is its capacity to adapt efficiently to reflect new technological conditions.[345]

The European Commission viewed legislative intervention as a background threat to provide incentives for voluntary arrangements with copyright owners. Even so, the reverse notice and takedown approach—immediately guaranteeing the right to demand the exercise of privileged uses, regardless of voluntary arrangements—may be preferable. The desired end is the same: encouraging private parties to make arrangements that allow valuable and privileged uses.

3. *Ensuring an Effective Ability to Engage in Privileged Uses*

One of the principal points of contention in implementing the WCT has been whether national legislation should prohibit both acts of circumvention and devices designed to facilitate circumvention. Creating excep-

---

343. *See* Eduardo M. Penalver & Sonia Katyal, *Property Outlaws* (Fordham Law Legal Studies Research Paper No. 90, Apr. 2007), *available at* http://ssrn.com/abstract=745324 (discussing "anti-delegation" architecture of copyright law). To the extent that we wish to rely on the incorporation of privileged uses in the architecture of the technological protection measures, it might be important to enlist the support of unfair competition or consumer protection law in requiring the disclosure by copyright owners of the precise nature and extent of technological protection measures. This objective has been secured in a number of European countries, in part through DRM-specific legislation (e.g., Germany), Urheberrechtsgesetz [Copyright Act], Sept. 12, 2003, BGBl. I at 1774, art. 1, § 95(d) (F.R.G.), and in part through litigation under general principles of consumer protection (e.g., in France). *See* Association CLCV / EMI Music France, Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Nanterre, 6e ch., June 24, 2003 (Fr.), *available at* http://www.legalis.net/jurisprudence-decision.php3?id_article=34 (fining Sony for failing to disclose TPM). As a result, market forces may play a greater role in ensuring that copyright owners do not abuse the application of technological protection measures in the first place. *See also* Nika Aldrich, *A System of Logo-Based Disclosure of DRM on Download Products* (Apr. 29, 2007), *available at* http://www.ssrn.com/abstract=983551.

344. Of course, the same may be true of agreements reached between copyright owners and users. Thus, any voluntary agreement that is concluded ideally should go beyond the articulation of present substantive rules and contemplate procedural or institutional components that facilitate attention to the spontaneity and dynamism of the ways in which users might wish to engage with copyrighted works.

345. *See* H.R. REP. NO. 94-1476, at 66 (1976); *see also* Pamela Samuelson, *Fair Use For Computer Programs and Other Copyrightable Works in Digital Form: The Implications of* Sony, Galoob *and* Sega, 1 J. INTELL. PROP. L. 49 (1993).

tions to a prohibition on circumventing technological protection measures may be effectively meaningless if third parties with the technological capacity to engage in circumvention are not able to provide privileged users with circumvention tools.

Article 6(4) requires member states to ensure that right holders make available to the beneficiary of an exception or limitation the means of benefiting from that exception or limitation. This may impose a more affirmative obligation on member states to ensure that circumvention tools are available to some degree. Certainly, the forms of relief contemplated by Commission officials under the provision include quite affirmative steps, such as the distribution of the "unlocking keys" necessary to circumvent the technological protection measures.[346]

If the reverse notice and takedown procedure is to ensure the possibility of privileged uses notwithstanding the application of TPMs, the procedure might offer standing to providers of circumvention tools. Alternatively, third-party service providers might be afforded the right to take advantage of the relief secured by individual users under the procedure. In Part III, we thus suggested that courts "allow those providing needed decryption skills and technologies to benefit from the same privileged use exception that a *demandeur* had ultimately vindicated either in court or by silent acquiescence of the copyright owner."[347]

Copyright law does not typically permit a third party to defend the legality of their activities on the basis that it is facilitating the exercise of privileged uses by another party (outside the context of secondary liability).[348] Yet, absent the involvement of such third parties, the rights secured

---

346. *See* Dusollier, *Fair Use by Design*, *supra* note 313; Nora Braun, *The Interface Between the Protection of Technological Protection Measures and the Exercise of Exceptions to Copyright and Related Rights: Comparing the Situation in the United States and the European Community*, 25 EUR. INTELL. PROP. REV. 496, 502 (2003).

347. *See supra* text accompanying note 275.

348. *See* Princeton Univ. Press v. Mich. Document Serv., 99 F.3d 1381, 1391 (6th Cir. 1996), *cert. denied*, 520 U.S. 1156 (1997) (quoting WILLIAM PATRY, FAIR USE IN COPYRIGHT LAW 420 n.34 (1996)) (arguing that "the courts have . . . properly rejected attempts by for-profit users to stand in the shoes of their customers making nonprofit or noncommercial uses"). The historical weakness of prohibiting commercially oriented third parties from claiming third-party beneficiary status with respect to the assertion of privileged uses forced the British House of Lords, in a leading case involving control of the spare parts market, to adapt a doctrine based in property law that imposed restrictions on the initial seller of the property, rather than find a right personal to the user of the property. Thus, in *British Leyland Motor Co. v. Armstrong Patents*, [1986] 1 All E.R. 850 (H.L.) (U.K.), the Court held that the owner of copyright in the drawings of an exhaust pipe of a car could not enforce that copyright so as to prevent the sale of unauthorized

by the reverse notice and takedown procedure may effectively become worthless.[349] In this context, the proposal thus derogates from parallelism with traditional copyright law, but it does so because the technological realities are different. A commercial copyshop might have improved the efficiency of professors producing coursepacks or students making personal copies, but the copying could have occurred without their help.[350] The same is not true of technological circumvention (otherwise there really would be some doubt about whether the measures were "effective").

4. Developing Appropriate Forms of Relief

Of course, one can avoid this debate entirely, at least within the structure of Article 6(4), by noting that this question is closely tied to the question of relief. To the extent that the relief provided is more structural in nature, such as requiring the modification of the TPMs or the distribution of the work in unprotected format, procedural devices such as expanded standing or third-party beneficiary rules would be unnecessary. Such "structural" relief does appear consistent with the type of approach contemplated by Commission officials under Article 6(4), when they suggested that the relief might include the "distribution of unlocking keys."[351]

Focusing on the nature of relief available under the reverse notice and takedown procedure might be a cleaner approach than innovating with procedural devices. In Part III, we suggested that copyright owners receiving the reverse notice and takedown request would either have the responsibility to take down the TPMs that impeded privileged uses or the obligation to contest the use on legally actionable grounds.[352] Compliance with such a request would, of course, effectively grant structural relief, albeit

---

spare parts because to do so would derogate from the grant of the property right in the car.

This doctrine, though short-lived in UK copyright law because statutory revisions quickly addressed the specific problem of spare parts and rights in the designs of useful articles, highlights the importance of limiting the rights of the right holder rather than conferring personal rights only on individual users. *Cf.* Canon Kabushiki Kaisha v. Green Cartridge Co., [1997] A.C. 728 (P.C.) (appeal taken from H.K.) (*per curiam* opinion by Lord Hoffman); Mars U.K. v. Tecknowledge Ltd., [2000] F.S.R. 138 (Ch.) (U.K.) (opinion of Jacob, L.J.) (noting effect of demise of the *British Leyland* principle under UK law).

349. *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 133.

350. *See* Princeton Univ. Press v. Mich. Document Serv., 99 F.3d 1381 (6th Cir. 1996), *cert. denied*, 520 U.S. 1156 (1997).

351. *See* Jorge Reinbothe, *The Legal Framework for Digital Rights Management*, Digital Rights Management Workshop, Brussels, Feb. 28, 2002, at 2, *available at* http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/doc/workshop2002/drm_workshop_brx_rev.doc.

352. *See supra* Section III.D.1.

without judicial or administrative intervention. A failure to comply with the reverse notice and takedown request could then provide a user group with standing to seek the right to circumvent for the purposes of specified non-infringing uses.

If the user group was successful, the ability of similarly situated third parties to take advantage of the court's decision would depend upon the nature of the relief granted. In countries that recognize the doctrine of collateral estoppel, third parties could clearly rely on the court's determination whether the use in question was privileged. However, spreading the full benefits of the court's ruling might depend upon whether the court simply permitted the requesting party to circumvent, permitted the user group to employ a provider of circumvention services to unlock the TPM, or ordered the copyright owner to modify the TPM.[353]

The significance of the nature of the relief granted in this regard becomes clearer when one examines the deficiencies in one member State's implementation of Article 6(4). Under the provisions implementing Article 6(4) in the United Kingdom, users who are unable to engage in a privileged use due to the application of TPMs may petition the Secretary of State.[354] The Secretary of State can require the copyright owner to demonstrate a "voluntary measure or agreement" or face "directions" that enable the relevant beneficiary to take advantage of the copyright exemption.[355] If the copyright owner fails to follow those directions, it will be found in breach of a duty actionable by the user that complained.[356]

This procedure suffers from several deficiencies. In particular, it requires an application to the Secretary of State every time a user believes its right to engage in a privileged use is being impeded.[357] The reverse no-

353. It might also depend upon any conditions that the court placed on the exercise of the rights granted to the user. *See supra* text accompanying notes 283-284.

354. Copyright and Related Rights Regulations, 2003, S.I. 2003/2498, art. 24, §§ 296ZD(2), 296(2) (U.K.).

355. *See id.* at § 296ZE(3).

356. *See id.* at § 296ZE(6).

357. Other national laws employ different institutions to determine the claims of the users. For example, under Greek law, the matter is referred to mediators and, absent consent to the mediators' conclusion, to the Court of Appeal. But these institutions are still assessing whether a technological protection measure is impeding any particular privileged use, not whether an act of circumvention (or a device) will *ex post* be excused from liability because of that fact. *See* Law 3057/2002 (Official Gazette A/239/10 October 2002), art. 81, Implementation of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society and Other Provisions, *available at* http://portal.unesco.org/culture/en/file_download.php/3368a2bd0fffab9a5310a8e00abfb9

tice and takedown procedure may also suffer from a similar problem if applications must be made on a case-by-case approach and the relief contemplated simply authorizes a particular user to circumvent a particular technological protection measure and no more. However, this direct approach should prove much simpler than a formal referral to an administrative body, and practice under the proposal—as supplemented by judicial decisions, when necessary—should facilitate reliance on the mechanism over time, especially in common law jurisdictions.

If the "directions" from the Secretary of State required the copyright owner to modify the TPM, as a Recital of the Directive hints, one form of "appropriate measure" might be one that would have an across-the-board effect.[358] If the relief that a user could request under the reverse notice and takedown procedure could likewise take this form, a similar *erga omnes* effect could be achieved.[359]

The possibility of structural relief is important in ameliorating another weakness of the UK procedure (which might also, to some extent, be leveled at the reverse notice and takedown proposal). Requiring application by the beneficiary of the exemption fails to give adequate weight to those instances where creative acts covered by a privileged use are spontaneous in nature.[360] Copyright exemptions traditionally operated on the premise that the user would engage in the contested act and the legitimacy of that act would later be determined by application of the allegedly relevant exemption, a practice whose risks might also inhibit actual resort to spontaneous uses. The departure from this traditional assumption is in part simply a product of the application of TPMs, which of themselves establish an

---

26Greek_law+.pdf (Greece). *See generally* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 67-68 (summarizing institutional choices made).

358. *See* Copyright Directive, *supra* note 10, recital 51 (providing example of "modifying an implemented technological measure").

359. The recital expressly mentions "other means" of ensuring the ability to engage in privileged uses. One of the responsible Commission officials suggested at the time the Directive was adopted that these means might include "handing out locking keys." *See* Reinbothe, *supra* note 351, at 2. Certainly, the language of "right holders making available to the beneficiary" seems to suggest affirmative conduct, beyond merely enacting an exemption to allow the beneficiary to engage in an act of circumvention (though that would also be a possible measure).

360. Requiring an application to a government official in order to engage in creative activity also devalues the importance of privacy or anonymity as an aspect of the creative environment. *See supra* note 290 (admitting this defect). In the notice and takedown procedure established by section 512, the copyrighted works at issue are created prior to the joining of dispute. Thus, the procedure does not interfere with the spontaneity of creative acts, or the potential importance of anonymity in the creative process.

inverted default of "ask first, act later." Nevertheless, requiring individualized applications in order to engage in privileged uses does not help.

Here again, if structural relief could be requested by a user seeking to engage in privileged uses, the costs of such a procedure and the repressive effect of having to seek permission would more often become a one-time occurrence. This supports the suggestion above that the reverse notice and takedown procedure should permit the *demandeur* to seek broader relief than merely obtaining immunity to circumvent.

While such structural relief as requiring the modification or elimination of technological protection measures may, at first blush, seem quite radical, it is fully consistent with Article 6(4), which contemplates that copyright owners have an affirmative role to play in ensuring the preservation of the balance of rights between owners and users of works.[361] To be sure, the relief that would be secured through the mechanisms implementing Article 6(4) is not detailed in the Directive, and some commentators have argued that it cannot require the copyright owner to reveal the digital lock.[362] But a per se rule foreclosing such relief is inconsistent with the open-ended nature of the Directive, and indeed with statements by Commission officials after its adoption.[363]

Whether such relief could undermine the efforts of copyright owners to protect against even infringing uses[364] would depend upon the terms under which such disclosure was made. For example, if a handover of the digital lock were conditioned on the manner in which the information was used or disclosed, it might enable the privileged uses without undermining the copyright owner's legitimate rights to protect against infringement. This possibility should make the reverse notice and takedown procedure attractive to industry. To the extent that the information is disclosed to third parties who will facilitate the privileged use by a particular *demandeur*, the provision of circumvention services as opposed to the manufac-

---

361. *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 68-69 (noting affirmative nature of obligations).

362. *See* Braun, *supra* note 346, at 502 (arguing that "handing over the 'key' to circumvent the technological measure to users is inappropriate and would endanger the whole system of technological measures").

363. *See* Reinbothe, *supra* note 351, at 2; BENTLY & SHERMAN, *supra* note 299, at 311.

364. Some might argue that our entire proposal will cause more infringement. But every time you legitimate any dual-use technology, there is a risk of infringement. On the other hand, if you lock up all works in technological fences, there is a risk of fewer public interest uses. For the reasons explained in Part II, we think that the balance between these two risks needs to be better calibrated, and can be done so without jeopardizing the ability to enforce copyrights effectively against bad actors.

ture of devices is less likely to implicate the copyright owners' nightmare scenario.

Likewise, under the original Australian implementation of the WCT, the statute allowed circumvention devices to be supplied to a beneficiary of an exception for a permitted use if the person making the privileged use provided the supplier with a signed declaration to that effect.[365] In any event, allowing a circumvention service provider to assist a particular user should be less problematic.[366]

No predetermined single form of relief should be established. One size will likely not fit all, given the wide range of uses that should be privileged. Yet, there may be circumstances when, under defined conditions, even the disclosure of the digital lock might be appropriate. One of the benefits of the fair use doctrine has been its flexibility and its ability to adapt to changing circumstances. The capacity of technology to effectuate a balance of rights, and what that balance should be, may well be very different in five years time. Bodies established under Article 6(4) in the European Union, and courts in the United States under a reverse notice and takedown procedure, should remain free to develop appropriate means to ensure the continued ability to engage in privileged uses.

D. Broader Perspectives and the Role of the Commission

The reverse notice and takedown procedure is precisely the type of conceptual approach that is mandated, albeit in a narrow form, by Article 6(4). A member state could implement the reverse notice and takedown procedure as a means of fulfilling the obligations imposed by Article 6(4). As a result of the Directive's inadequate harmonization of exceptions and the opaque language of Article 6(4) itself, it is unclear how many privileged uses are protected by Article 6(4).[367] Some countries have implemented Article 6(4) without clear reference to specific limitations; others have explicitly singled out specific limitations as preserved by Article 6(4) despite the application of TPMs.

---

365. *See* Jeffrey Cunard et al., WIPO Standing Comm. on Copyright and Related Rights, *Current Developments in the Field of Digital Rights Management*, WIPO Doc. No. SCCR/10/2 (Aug. 1, 2003), *available at* http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf.

366. *See* Ginsburg, *supra* note 14, at 17.

367. *See* COPYRIGHT DIRECTIVE IMPLEMENTATION STUDY, *supra* note 11, at 169 (suggesting revision of Article 6(4) to "give protected status to those limitations that . . . reflect the fundamental rights and freedoms enshrined in the European Convention on Human Rights, [and] those that have a noticeable impact on the Internal Market or concern the rights of European consumers").

The most that can be said with any confidence is that implementation in member states has been inconsistent.[368] But, even absent any further harmonization of different national choices, each member state could adopt the reverse notice and takedown procedure as a mechanism to preserve the precise range of privileged uses that the member state reads as permitted by the Directive.[369]

Even if the Commission might not look favorably on any effort to expand the general norm of Article 6(4) beyond the narrow context in which the Directive currently requires it, this would not preclude other countries from introducing a reverse notice and takedown procedure. To the extent that the US or the EU might seek to repress such efforts through bilateral trade negotiations, Article 6(4) shows that acting within the regime of DRM to protect uses privileged by traditional copyright law is fully consistent with the WCT. If the EU can limit copyright owners' control as to some undefined exceptions, why could another country not do so with respect to all exceptions traditionally protected by copyright law and consistent with international copyright obligations?

Moreover, even within the EU, the Commission's recently solicited review of the copyright *acquis* might provide an opening for some reform of existing law, including the expansion of the general principle contained in Article 6(4). The reverse notice and takedown procedure discussed in this Article should be given serious attention during the Commission's review. At least, a Policy Statement from the Commission acknowledging the ability of member states to build upon the underlying norm of Article 6(4), even beyond a strict reading of the text, might provide room for important procedural innovations in ways that truly effectuate the values not only of the Directive but of the WCT that it claims to implement.

V. CONCLUSION

By the end of the multilateral negotiations held at Geneva in 1996, the intense struggle among stakeholders representing content providers, the telecommunications industry, online service providers, and the educational and scientific communities produced a workable compromise in the WCT.

---

368. *See* Marcella Favale, *Technological Protection Measures and Copyright Exceptions in EU27: Towards The Harmonization,* at 22, August 10, 2007, http://www.law.depaul.edu/institutes_centers/ciplit/ipsc/paper/Marcella_FavalePaper.pdf, at 22 (draft paper presented at Intellectual Property Scholars Conference) ("Every country that decided to single out only some exceptions, picked from the list a different selection from that [in Article 6(4)] of the directive, and from that of the other countries.").

369. *See supra* note 319 and accompanying text (making this point).

The importance of preserving access to the copyrighted culture protected in cyberspace under the new Treaty was expressly recognized in at least three important places:

1) The broad preambular recognition of "the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information;"[370]

2) The further express recognition, in Article 11, that the international standard for reinforcing TPMs was not meant to entitle authors to "restrict acts, in respect of their works, which are . . . permitted by law;"[371]

3) And the express understanding in the Agreed Statement concerning Article 10, which permitted contracting parties "to carry forward and appropriately extend into the digital environment" existing limitations and exceptions in their national laws and "to devise new exceptions and limitations that are appropriate to the digital network environment."[372]

This historic compromise made it possible to establish a balanced legal infrastructure for worldwide networked communications of copyrighted works in the digital environment.

Unfortunately, at the national implementation phase, the balance struck at Geneva gave way, in the United States, to the one-sided provisions of the DMCA and, in the European Union, to the only slightly less unbalanced approach of the EU Directive. While the DMCA formally acknowledged the need to preserve privileged uses in section 1201(c), sections 1201(a) and (b) have arguably separated access from privileged use and made it difficult, and under some interpretations impossible, to raise questions of privileged use once TPMs control access to copyrighted works. The EU Copyright Directive took an equally tough approach to restricting access through TPMs. Although the Directive generally invoked a need to respect exceptions and limitations in local law, it simultaneously limited the scope of the provision enabling such privileged uses.

The end result on both sides of the Atlantic has been the emergence of a distorted, unbalanced copyright regime in cyberspace with a growing chorus of complaints from educational, scientific, and other public interest users, among others, and a growing revolt against the legal restraints on

370. WCT, *supra* note 1, Preamble.
371. *Id.*, art. 11.
372. Agreed Statements, *supra* note 2, statement concerning art. 10.

legitimate uses of the copyrighted culture in some quarters. The abusive possibilities inherent in the DMCA's access control provisions became dramatically visible in the recent lock-out cases, where TPMs were used to perpetuate the kind of "fraud on the patent law" that the Supreme Court had struck down in its 1880 decision in *Baker v. Selden*.[373]

Moreover, these extreme distortions of basic copyright principles mask the much greater daily pressures that the DMCA puts upon the public interest user community, which depends upon easy and continuous access to ideas, facts and other inputs to knowledge that copyright laws have never been allowed to protect. Unless these distortions are remedied, a copyright system that was designed to promote progress by expanding the outputs of literary and artistic works could end by choking off access to essential inputs to the production of knowledge as a global public good in the digital environment.

Our proposal for a reverse notice and takedown procedure—designed to reduce the tensions between access protection measures and privileged uses—attempts to rebalance the copyright equation in cyberspace before the damaging effects of overprotection give rise to systematic failure or breakdown. Among its many advantages in the U.S. is the fact that it can be judicially developed and applied on a case-by-case basis, with low transaction costs and relatively few risks to either side. It allows bona fide public interest users to continue their work without undue interference from TPMs and with the support of the content-providing industries themselves, who may verify the legitimate uses being enabled and contest uses that seem to stretch the boundaries of legally defined privilege. It builds on workable procedures that have already proved their usefulness in the context of ISP liability, while enabling pinpoint litigation on borderline issues that all sides will want clarified. There is good reason to believe that industry itself might prefer a gradualist mechanism of this kind to more intrusive legislative measures with unknown future consequences.

If judicial experimentation with a reverse notice and takedown procedure proved unsuccessful for reasons we cannot foresee, it could be judicially abandoned as easily as it had been adopted. If, instead, it proved effective, the end results could eventually be codified both in the United States and abroad on the basis of the experience gained in the meantime. In that event, our proposal would have helped copyright law to regain its traditional balance in the digital environment while implementing the true spirit of the historic compromise originally embodied in the WIPO Copyright Treaty of 1996.

---

373. 101 U.S. 99 (1880).

NO PLACE LIKE HOME FOR MAKING A COPY: PRIVATE COPYING IN EUROPEAN COPYRIGHT LAW AND CONSUMER LAW

By Natali Helberger[†] & P. Bernt Hugenholtz[‡]

TABLE OF CONTENTS

I. **INTRODUCTION** 1061

II. **EUROPEAN COPYRIGHT LAW** 1064

A. THE PLACE OF THE CONSUMER IN EUROPEAN COPYRIGHT LAW 1065
B. RATIONALES OF PRIVATE COPYING LIMITATIONS 1067
1. *Privacy* 1068
2. *Justice* 1069
3. *Promotion of Creativity and Speech* 1070
4. *Economic Arguments* 1071
C. LEGAL NATURE OF PRIVATE COPYING EXCEPTIONS 1073
D. ASSESSMENT 1077

III. **EUROPEAN CONSUMER LAW** 1078

A. RATIONALES 1080
1. *Empowering the Consumer as Sovereign Market Actor* 1080
2. *Protecting the Weaker Party* 1081
B. PRIVATE COPYING AND CONSUMER LAW 1084
1. *Conformity with Consumers' Reasonable Expectations* 1084
2. *Fairness of Contractual Terms* 1089
3. *Rules on Consumer Information* 1090
C. ASSESSMENT 1093

IV. **CONCLUSION** 1096

I. INTRODUCTION

As an ancient Dutch proverb goes, "There is no place like home for making a private copy." Well, not really. But certainly the sense of entitlement to make private copies of copyrighted works is deeply ingrained in

---

[†] Senior Researcher at the Institute for Information Law.

[‡] Professor of Intellectual Property Law and Director of the Institute for Information Law of the University of Amsterdam (IViR).

Dutch society, as it is in most other Member States of the European Union. Recent surveys of European consumers show that the ability to make private copies is among the main concerns of consumers of information goods and services.[1] Surprisingly, this general expectation does not rest on legally solid ground. On the one hand, while permitting the Member States of the European Union to adopt their own copyright limitations allowing private copying,[2] European copyright law[3] does not clearly define the legal status of private copying—its scope and enforceability, both in contractual relationships and where private copying is impeded by digital rights management (DRM). On the other hand, consumer protection law in Europe may on occasion give "teeth" to private copying limitations,[4] al-

---

This paper is based on two presentations given at the conference "Copyright, Digital Rights Management Technology and Consumer Protection". We would like to thank the participants of the conference for their valuable comments on the presentations. Any comments are welcome to helberger@ivir.nl.

1. NICOLE DUFFT ET AL., INDICARE, DIGITAL VIDEO USAGE AND DRM, RESULTS FROM A EUROPEAN CONSUMER SURVEY 26-28 (2006), http://www.indicare.org/tiki-download_ file.php?fileId=170 [hereinafter DUFFT ET AL., DIGITAL VIDEO USAGE]; NICOLE DUFFT ET. AL., INDICARE, DIGITAL MUSIC USAGE AND DRM, RESULTS FROM A EUROPEAN CONSUMER SURVEY 26-28 (2005), http://www.indicare.org/tiki-download_file. php? fileId=110 [hereinafter DUFFT ET AL., DIGITAL MUSIC USAGE].

2. Council Directive 2001/29 on the Harmonization of Certain Aspects of Copyrights and Related Rights in the Information Society, art. 5(2)(b), 2001 O.J. (L 167) 10, 16 (EU) [hereinafter Information Society Directive]
("Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases: . . . (b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned.").

3. Note that, strictly speaking, "European copyright law" does not exist. The twenty-seven Member States of the European Union each have their own copyright laws. At the European Community level, the existing body of copyright law consists of seven directives that have harmonized distinct aspects of copyright law in the Member States. See note 17 for a complete listing of Directives. The primary aim of harmonization is to remove disparities between national laws, and thus help create an Internal (Single) Market for goods and services. A harmonization Directive is binding upon a Member State, but does not directly bind its citizens. Directives require Member States to adapt their national laws to the norms of the Directive by transposing (implementing) these into national law. National courts are bound to interpret harmonized norms in the light of the corresponding provisions of a directive, subject to ultimate review by the European Court of Justice. Consequently, the laws of copyright in the Member States are similar insofar as the states have implemented the Directives. Absent complete harmonization of copyright, national laws of the Member States will continue to show enormous variety.

4. Note that the term "limitation" is used throughout this article to indicate a statutory limit (i.e., exemption) to the copyright holder's exclusive right of reproduction. The

lowing consumers to make private copies where copying constitutes an essential functional characteristic of digital media (e.g., time and format shifting, porting, and archiving). However, as recent decisions from courts in France and Belgium demonstrate, consumer law as applied to private copying also suffers from a lack of legal certainty and other deficiencies, stemming in part from the ambiguity in European copyright law regarding private copying.[5]

This Article examines the intersection of copyright law and consumer law relating to private copying in Europe and queries their effectiveness as legal instruments to protect consumers in dealings with information suppliers. The focus will be on traditional consumers, defined as private users of information goods and services for non-commercial purposes. Commercial or institutional users of copyright-protected works, such as publishers, broadcasters, libraries, and universities, therefore remain beyond the scope of this Article. The Article will also not address "prosumers," consumers doubling as producers. Although national statutes and case law are discussed throughout the Article, the primary reference will be the existing body of European directives that have partly harmonized the laws of copyright and consumer protection of the Member States.

Part II briefly looks at the history and rationales of private copying limitations in Europe, then examines the legal nature and enforceability of private copying exemptions in their diverse manifestations and concludes with a general assessment. Thereafter, Part III analyzes European consumer law following roughly the same structure, first describing the various, sometimes conflicting goals and approaches of consumer protection law in Europe, then examining relevant legal tools, and finally querying how and to what extent these tools might serve to protect consumers' freedom to make private copies. Ultimately, we demonstrate that while copyright law in Europe does offer a measure of comfort to consumers, the legal instruments of European consumer law are potentially more effective in achieving the freedom to make private copies that European consumers generally expect.

---

synonymous term "exception," which is often used in European legislation and scholarship, is avoided here because of its pejorative connotation. In the opinion of the authors of this article, limitations in copyright law are not exceptional. *See* P. Bernt Hugenholtz, Institute for Information Law, University of Amsterdam, Fierce Creatures, Copyright Exemptions: Towards Extinction?, Keynote Speech at IFLA/IMPRIMATUR Conference, Amsterdam: Rights, Limitations and Exceptions: Striking a Proper Balance (Oct. 30, 1997), *available at* http:// www.ivir.nl/publications/hugenholtz/PBH-FierceCreatures.doc.

5. *See infra* notes 146, 150, 152, 185, 186.

II. EUROPEAN COPYRIGHT LAW

For over twelve years, private copying has been the proverbial *hot potato* on the menu of European copyright lawmakers. In 1995, the European Commission (EC) initiated an early attempt to harmonize this thorny issue across Member States in the form of a widely circulated but never published draft proposal for a directive.[6] However, this attempt was aborted because existing differences in private copying legislation in the Member States were considered too great to overcome.[7] Six years later, the EC legislature was more successful by codifying a rule on private copying in article 5(2)(b) of the Information Society Directive,[8] the first piece of EC legislation to address private copying in general terms.

Serious problems remained. First, Member States are not required to adopt the Directive's rule on private copying, leaving them complete discretion *not* to adopt any rules allowing private copying.[9] Consequently, the rules on private copying have remained largely unharmonized in the European Union. Second, the issue of copyright levies,[10] directly associated with private copying, always was and still remains a matter of considerable controversy. The European Commission recently attempted to give guidance on the future phasing out of private copying levies in response to DRM's emerging ability to limit private copying. This attempt met enormous opposition from levy collecting societies and the French Govern-

---

6. Proposition de Directive du Parlement Européen et du Conseil relative à l'harmonisation de certaines règles du droit d'auteur en des droits voisin applicables à la copie privé [Proposed Directive of the European Parliament and Council Relating to the Harmonisation of Certain Rules for Royalties and Copyrights], Brussels, December 1995 (unpublished proposal, copy on file with the authors).

7. Note that general private copying limitations did not, and do not, exist in all Member States. *See infra* note 9.

8. Information Society Directive, *supra* note 2, art. 5(2)(b).

9. General private copying exemptions do not exist in the United Kingdom and Ireland; however, these jurisdictions do allow the making of private copies of broadcast for the purpose of time-shifting. Copyright, Designs and Patents Act, 1988, c. 48, § 101 (U.K.).; Irish Copyrights and Related Rights Act, 2000 § 101 (Act No. 28/2000) (Ir.) *available at* http://acts.oireachtas.ie/en.act.2000.0028.8.html#partii-chapvi-sec101 (last visited Aug. 28, 2007).

10. Copyright levies are private taxes imposed upon the manufacture and importation of reproduction equipment (e.g., video recorders and MP3 players) and/or blank recording media (e.g., recordable CDs and DVDs). Levies usually have their legal bases in national copyright norms on private copying requiring equitable or fair compensation of copyright holders. Levy systems exist in most Member States of the European Union but vary considerably with regard to tariff and scope. *See infra* Section II.B.2.

ment and was subsequently abandoned.[11] Third, the Information Society Directive does not address the question of whether private copying exemptions in national law trump, or may be overridden by, contracts between information producers and consumers. Finally, the Directive's complex rules on DRM and their interplay with the freedom to make private copies are the cause of considerable confusion, and have led to varied implementations by national legislatures.[12]

This Part will describe the current state of private copying in European copyright law, its history and rationales, its various manifestations in European copyright law, and finally assess its strengths and weaknesses, primarily from the perspective of information consumers.

A. The Place of the Consumer in European Copyright Law

For most of the 20th century, private copying occupied a very modest place in the law of copyright in Europe. Buyers and readers of books and other printed matter were rarely perceived as potential competitors or threats to the copyright holders' interests. Early laws on copyright were not concerned with the kind of small-scale hand-made reproduction that occurred in homes or at the workplace. Private copying exemptions have existed in various forms in European jurisdictions since the early days of copyright.[13] For instance, the German Act of 1876 allowed for the making of a single copy of a work of art, provided it was not intended for commercial use.[14] In legal doctrine, a freedom to make private copies was recognized as well. According to the famous German legal scholar Joseph Kohler, the exclusive right of reproduction was implicated only when a copy of a work "is intended to serve as a means of communicating [the work] to others."[15] In other words, copyright protected authors against acts of unauthorized communication, not consumptive usage.

---

11. Press Release, Copyright Levies Reform Alliance, Industry Condemns Commission Backdown on Reform: Reform of Copyright Levies Abandoned Following Opposition from France (Dec. 13, 2006), *available at* http://www.eicta.org/fileadmin/user_upload/document/document1166542590.pdf.

12. *See infra* Section II.C.

13. For example, art. 16 of the Dutch Copyright Act enacted in 1912 allowed copying for personal uses. LUCIE M.C.R. GUIBAULT, COPYRIGHT LIMITATIONS AND CONTRACTS 49-50 (2002).

14. JACOB HENDRIK SPOOR, SCRIPTA MANENT: DE REPRODUKTIE IN HET AUTEURSRECHT 9 (1976).

15. JOSEPH KOHLER, DAS AUTORRECHT 230 (1880); SPOOR, *supra* note 14, at 11.

Even in 2007, the consumer as such remains almost completely invisible in the law of European copyright.[16] The main actors are the content producers, such as authors and other right holders, and the mainstream intermediaries, such as publishers, broadcasters, libraries, and educational institutions. Somewhat confusingly, particularly for those versed in the jargon of consumer law, these intermediaries are traditionally referred to as "users." The terms "consumer" and "end user" rarely if ever appear in legislative texts on copyright and are absent from the body of harmonized European copyright law. Indeed, none of the provisions of the seven copyright-related directives adopted by the European legislature since 1991 even mention the word "consumer."[17]

Until the digital revolution, the consumer remained mostly an *entité negligeable* in European copyright law. This changed, however, as European copyright law began to address computer programs.[18] Based on the rather technocratic argument that all digital operations involve some form of copying, however temporary or transient, the right of reproduction was stretched into an exclusive right to use works in digital form.[19] This very broad interpretation of the reproduction right was first codified in the EC's Computer Program Directive of 1991[20] and Database Directive of 1996[21] and later elevated to a general norm in the Information Society Directive

16. The same can be said of current U.S. copyright law. *See* Joseph P. Liu, *Copyright Law's Theory of the Consumer*, 44 B.C. L. REV. 397, 399 (2003); Julie E. Cohen, *The Place of the User in Copyright Law*, 74 FORDHAM L. REV. 347, 347 (2005).

17. Council Directive 91/250 on the Legal Protection of Computer Programmes, 1991 O.J. (L 122) 42 (EC) [hereinafter Computer Programs Directive]; Council Directive 92/100 on Rental and Lending Rights and Certain Rights Related to Copyright in the Field of Intellectual Property, 1992 O.J. (L 346) 61 (EC) [hereinafter Rental Rights Directive]; Council Directive 93/83 on the Co-Ordination of Certain Rules Concerning Copyright and Rights Related to Copyright Applicable to Satellite Broadcasting and Cable Retransmission, 1993 O.J. (L 248) 15 (EC) [hereinafter Satellite and Cable Directive]; Council Directive 93/98 harmonizing the Term of Protection of Copyright and Certain Related Rights, 1993 O.J. (L 290) 9 (EC) [hereinafter Term Directive]; Council Directive 96/9 on the Legal Protection of Databases, 1996 O.J. (L 77) 20 (EC) [hereinafter Database Directive]; Information Society Directive, *supra* note 2; Council Directive 2001/84 on the Resale Right for the Benefit of the Author of an Original Work of Art, 2001 O.J. (L 272), 32 (EU) [hereinafter Resale Rights Directive].

18. *See* Computer Programs Directive, *supra* note 17, art. 1(1) (requiring Member States to "protect computer programs, by copyright, as literary works . . .").

19. P. Bernt Hugenholtz, *Convergence and Divergence in Intellectual Property Law: The Case of the Software Directive*, *in* INFORMATION LAW TOWARDS THE 21ST CENTURY 319, 323 (Willem F. Korthals Altes, Egbert J. Dommering, P. Bernt Hugenholtz & Jan J.C. Kabel eds. 1992).

20. Computer Programs Directive, *supra* note 17.

21. Database Directive, *supra* note 17.

of 2001.[22] Thus, a powerful new right was added to the copyright owners' palette of rights: an exclusive right to *consume* works electronically.[23]

B. Rationales of Private Copying Limitations

A variety of arguments, informed by those that traditionally underpin European copyright law, are made to justify private copying exemptions in Europe. Dutch legal scholar Willem Grosheide describes the main rationales of copyright:[24]

a) The "Personality" rationale: The work of authorship bears the personal imprint of its maker. Copyright ("author's right") is a species of a general right of personality,[25] which is informed by the fundamental right to privacy.[26]

b) The "Justice" rationale: Copyright reflects notions of natural justice. "[A]uthor's rights are not created by law but always existed in the legal consciousness of man."[27]

c) Cultural rationales: Copyright acts as an incentive to create and disseminate works that advance knowledge and contribute to our cultural heritage.[28] Copyright is the proverbial "engine of free expression."[29]

d) Economic rationales: Copyright turns information, which is essentially a public good, into a tradable commodity by allocating property rights in informational goods.[30] Correcting this "market failure" promotes economic efficiency and competition in information markets.[31]

---

22. Computer Programs Directive, *supra* note 17, art. 4(a); Database Directive, *supra* note 17, art. 5(a); Information Society Directive, *supra* note 17, art. 2.

23. This stretching of the reproduction right was met with serious criticism from European scholars. *See* LEGAL ADVISORY BOARD (LAB), REPLY TO THE GREEN PAPER ON COPYRIGHT IN THE INFORMATION SOCIETY (1995), http://europa.eu.int/ISPO/legal/en/ipr/reply/ reply.html.

24. F. WILLEM GROSHEIDE, AUTEURSRECHT OP MAAT 128-45 (1986).

25. *Id.* at 129-32.

26. *See infra* text accompanying notes 42-43.

27. EDWARD W. PLOMAN & L. CLARK HAMILTON, COPYRIGHT: INTELLECTUAL PROPERTY IN THE INFORMATION AGE 13 (1980); GROSHEIDE, *supra* note 24, at 130.

28. GROSHEIDE, *supra* note 24, at 128.

29. Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985).

30. William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 326 (1989).

31. GROSHEIDE, *supra* note 24, at 128.

The "justice" and "personality" rationales typically support the "author's rights" systems that prevail in continental Europe,[32] while the more utilitarian arguments, the cultural and economic rationales, underpin the copyright systems that are dominant in common law jurisdictions, such as the United States.[33] As the EC continues to harmonize copyright law in the European Union based on market norms and largely driven by economic considerations, however, the main differences between Europe-style author's right and US-style copyright are gradually disappearing.[34] Nevertheless, the justice and personality rationales, as reflected in the moral rights that are omnipresent throughout Europe's copyright laws, undoubtedly remain important drivers of copyright law and policy in Europe. Similar arguments also underlie the copyright limitations allowing private copying that currently exist in most Member States.[35]

1. Privacy

Historically, private copying in Europe remained outside the scope of copyright because private copies were not considered means of communicating works to the public.[36] The rationale of a private copying exception is informed, at least in part, by the idea of protecting the end user's private sphere. For similar reasons, modern European copyright laws have limited the prohibition of public performance or communication to the public by exempting acts done in the private sphere.[37] Such limits reflect the right to privacy, considered a fundamental right or freedom in Europe since the European Convention on Human Rights was signed in 1950.[38]

---

32. PAUL GOLDSTEIN, INTERNATIONAL COPYRIGHT 3 (2001).

33. *Id.*

34. *Id.* at 4.

35. *See, e.g.*, Auteurswet [Copyright Act], Sept. 23, 1912, Stb. 2006, 60, art. 16(b) (Neth.).

36. *See supra* Section II.A.

37. For example, article 12(4) of the Dutch Copyright Act exempts performances in a restricted circle composed of "relatives or friends or equivalent persons and [if] no form of payment whatsoever is made for admission to the recitation, performance or presentation." Copyright Act, *supra* note 35.

38. 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.

Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov 4, 1950, 213 U.N.T.S. 222.

Privacy considerations also played a crucial role in the German Federal Supreme Court's landmark *Personalausweise* decision of 1964,[39] which reaffirmed an earlier holding that manufacturers of private recording equipment were liable for contributory copyright infringement.[40] In *Personalausweise*, the German levy collecting society GEMA[41] sought a court order requiring equipment manufacturers to record the names of purchasers of recording equipment. The Court denied GEMA's request, finding that to grant such a court order would encroach upon the end users' constitutionally protected private sphere.[42] This decision eventually led to the introduction of a levy on the importation and sale of home recording equipment as a way of remunerating copyright holders while respecting the fundamental right to privacy of end users.[43]

2. Justice

Since their introduction by the German Federal Supreme Court in 1964, copyright levies have gradually spread across the European Union.[44] With the notable exception of the UK and Ireland, where private copying has never been fully legalized,[45] most Member States now have a system

39. *Personalausweise*, Bundesgerichtshof [BGH] [German Federal Supreme Court] May 25, 1964, [1965] Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 104 (106) (F.R.G).

40. *Grundig Reporter*, Bundesgerichtshof [BGH] [German Federal Supreme Court] May 18, 1955, [1955] Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 492 (492) (F.R.G).

41. GEMA (Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte) collectively administers performance and mechanical reproduction rights of composers in Germany, and is presently one of the largest collecting societies in Europe. *See* GEMA Home Page—English, http://www.gema.de/engl/home.shtml (last visited Aug. 8, 2007).

42. Dirk J.G. Visser, *Copyright Exemptions Old and New: Learning from Old Media Experiences*, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 49, 50 (P. Bernt Hugenholtz ed. 1996); GUIBAULT, *supra* note 13, at 47-56; Andrew F. Christie, *Private Copying and Levy Schemes: Resolving the Paradox of Civilian and Common Law Approaches* (Univ. of Melbourne Legal Studies Research Paper No. 116, 2004), *available at* http://ssrn.com/abstract=690521.

43. Note that Recital 57 preceding the Information Society Directive underscores the importance of implementing privacy safeguards in DRM systems, so as to avoid a conflict with well-developed EC data protection law. Information Society Directive, *supra* note 2, rec. 57.

44. P. BERNT HUGENHOLTZ, LUCIE GUIBAULT & SJOERD VAN GEFFEN, THE FUTURE OF LEVIES IN A DIGITAL ENVIRONMENT 13-29 (2003) [hereinafter FUTURE OF LEVIES], *available at* http://www.ivir.nl/publications/other/DRM&levies-report.pdf.

45. British law does provide for a more limited defense of "fair dealing" for the purpose of research or private study. This defense, however, does not apply to a broadcast, cable program, sound recording, or film. Copyright, Designs and Patents Act, 1988, c. 48,

of private copying levies.[46] Levies are imposed on the importation and manufacture of copying equipment, blank media, or both and collected by collecting societies representing authors, performing artists, film producers, and publishers.[47] Consumers ultimately pay the price of levies.

Levies reflect the "remuneration principle" prevailing in Member States of the authors' rights tradition. Under this conception of copyright, authors are entitled to "equitable" remuneration for each and every use of their work as a matter of fairness. Although more sympathetic to a future world controlled by DRM than the currently prevailing system of private-copying-cum-levies, the Information Society Directive instructs Member States that permit private copying to grant "fair compensation" to copyright holders.[48] The Directive does not explicitly mandate levies as a form of "fair compensation," but levies have remained by far the most common remuneration scheme for private copying in Europe.[49]

3. *Promotion of Creativity and Speech*

An entirely different objective of private copying exemptions is closely linked to yet another main rationale of copyright. If copyright is supposed to promote culture and serve as the "engine of free expression,"[50] the law of copyright must also allow prospective authors to "stand on the shoulders of giants" and freely engage in transformative uses of works of authorship.[51] Private copying is an essential first step in this process of follow-on creation.[52]

---

§ 29 (Eng.). *See* LIONEL BENTLY & BRAD SHERMAN, INTELLECTUAL PROPERTY LAW 199 (2001).

46. FUTURE OF LEVIES, *supra* note 44, at 13-29.

47. *Id.*

48. Information Society Directive, *supra* note 2, art. 5(2)(b). Note however that "fair compensation" is connected to the notion of harm, *id.* at rec. 35, and therefore may amount to less than "equitable remuneration," a notion based on fairness. *See* FUTURE OF LEVIES, *supra* note 44, at 36; Stefan Bechtold, *Directive 2001/29/EC, in* CONCISE EUROPEAN COPYRIGHT LAW 343, 373 (Thomas Dreier & P. Bernt Hugenholtz eds., 2006); Information Society Directive, *supra* note 2, art. 5(3)(b).

49. Alternatively, a system of state subsidies, as it exists in Norway, would also qualify as "fair compensation."

50. *See* Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985).

51. LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 249 (2001).

52. MARTIN R.F. SENFTLEBEN, COPYRIGHT, LIMITATIONS AND THE THREE-STEP TEST: AN ANALYSIS OF THE THREE-STEP TEST IN INTERNATIONAL AND EC COPYRIGHT LAW 39 (2004) (justifying the need to permit transformative uses on the ground of "intergenerational equity").

However, the rules on private copying in the Information Society Directive do not refer to private copying for transformative uses. Although some provisions in the Directive do allow Member States to permit such non-private transformative uses as quotation and parody,[53] the Directive treats private copying mainly as a consumptive act.[54] By contrast, several Member States expressly deal with "transformative" private copying in their national laws. For example, German copyright law is more generous regarding private copying for purposes of study and research than, for instance, purely consumptive "home taping" of radio and television programs.[55]

4. Economic Arguments

Economic arguments have been used both to justify and to limit private copying and associated levy schemes in Europe. The "market failure" inherent in the absence of practicable licensing and enforcement mechanisms vis-à-vis consumers of copyright works has been a powerful argument in favor of statutory licenses permitting private copying. Concomitantly, the recent emergence of DRM systems that do allow copyright holders to engage in individual end-user licensing has cast into doubt the survival of private copying exemptions.[56]

Indeed, it is surprising that the Information Society Directive does not totally prohibit private digital copying[57] given certain provisions in the earlier Computer Programs[58] and Database Directives.[59] The Database Directive tolerates copying for private purposes only with regard to non-electronic databases.[60] The Computer Programs Directive prohibits private copying of computer software altogether, except for the occasional back-up copy.[61]

---

53. Information Society Directive, *supra* note 2, art. 5(3)(d), (k).

54. *Id.*, art. 5(2)(b).

55. Urheberrechtsgesetz [Copyright Act], Sept. 9, 1965 BGBl. I at 1273, §§ 53, 54 (F.R.G.).

56. ANDRE LUCAS & HENRI-JACQUES LUCAS, TRAITE DE LA PROPRIETE LITTERAIRE ET ARTISTIQUE 268 (2d ed. 2001).

57. Early drafts of the Information Society Directive did not permit digital private copying. An echo of this early policy can be heard in Recital 38, which considers that digital private copying is "likely to be more widespread and have a greater economic impact" than analog private copying. Information Society Directive, supra note 2, rec. 38.

58. Computer Programs Directive, *supra* note 17.

59. Database Directive, *supra* note 17.

60. *Id.*, arts. 6(2) and 9(a).

61. Computer Programs Directive, *supra* note 17, art. 5(2).

Although the Information Society Directive does not prohibit private copying, the idea that DRM can effectively overcome market failure has informed the provisions of the Directive. Article 5(2)(b) of the Directive instructs the Member States that in calculating the amount of "fair compensation" for acts of digital private copying the "application or non-application of technological measures" be taken into account.[62] In other words, as DRM gradually displaces private copying, levies are to be phased out.

Considerations of economic industrial policy, or perhaps consumerism, may have also played a role in permitting private copying, especially in countries such as the Netherlands where electronics manufacturers have more political clout than copyright holders. As the Dutch Government explained to its Parliament in 1972, home recording equipment "would lose all attraction" to consumers if private copying were not permitted.[63]

Economic considerations have also limited the consumer's freedom to make private copies. Private copying is no longer permitted wherever private uses compete with commercial uses reserved to right holders. Article 5(2)(b) of the Information Society Directive requires copies be "made by a natural person for private use and for ends that are neither directly nor indirectly commercial."[64] This excludes any form of commercial copying, be it for legitimate business-related purposes or ordinary "piracy."[65] Moreover, Article 5(2)(b) does not permit exemptions allowing "private" copying by or within business enterprises or other legal persons, even if such copying is without commercial purpose.[66]

Article 5(5) of the Directive imposes yet another economically motivated ceiling on private copying, requiring all private copying exemptions to comply with the so-called "three-step test."[67] The three-step test, which can be found in various instruments of international copyright law,[68]

---

62. Information Society Directive, *supra* note 2, art. 5(2)(b).

63. Visser, *supra* note 42, at 49 (quoting Second Chamber of Parliament 1972, L. de Vries, *Parlementaire geschiedenis van de Auteurswet 1912 zoals sedertdien gewijzigd* (Parliamentary history of the Copyright Act of 1912, as revised), The Hague 1989, 17).

64. Information Society Directive, *supra* note 2, art. 5(2)(b).

65. Bechtold, *supra* note 48; Information Society Directive, *supra* note 2, art. 5(3)(e).

66. Information Society Directive, *supra* note 2, art. 5(3)(e).

67. *Id.*, art. 5(5) ("The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.").

68. Berne Convention for the Protection of Literary and Artistic Works art 9(2), Sept. 9, 1986, S. Treaty Doc. No. 99-27 (1986), 1161 U.N.T.S. 3; Agreement on Trade-

serves as a general restriction to *all* exemptions presently found, or to be introduced, in the Member States' copyright laws pursuant to the Directive. Even if an exemption falls within one of the 21 categories of permitted exceptions enumerated in Article 5, it is for the legislatures (and, eventually, the courts) of the Member States to determine on a case-by-case basis whether the general criteria of the three-step test are met.[69] Exemptions permitting digital private copying, therefore, are permitted only (1) "in certain special cases"; (2) "which do not conflict with a normal exploitation of the work"; and (3) "do not unreasonably prejudice the legitimate interests of the right holder."[70]

It is a matter of some speculation, and eventually for the European Court of Justice to decide, whether a generally worded private copying exemption will pass the three-step test. On the one hand, in the digital environment, where end users are capable of producing perfect copies with the proverbial "push-of-a-button," private copying might not be a "certain special case" and may conflict with a "normal exploitation of the work" almost by definition.[71] On the other hand, broadly worded private copying exemptions already existed in many European countries at the time Article 9(2) of the Berne Convention, the predecessor of Article 5(5) of the Information Society Directive, was introduced in 1967.[72] These exemptions presumably were "grandfathered in" under the Berne Convention and are therefore not subject to the test.[73]

C. Legal Nature of Private Copying Exceptions

The legal nature of private copying limitations under European copyright law is uncertain and a matter of persistent controversy.[74] The various user freedoms codified in the Information Society Directive come in several flavors, varying from traditional limitations that users may invoke in

---

Related Aspects of Intellectual Property Rights art. 13, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299; 33 I.L.M. 1197 (1994); WIPO Copyright Treaty art. 10, Dec. 20, 1996, WIPO Doc. CRNR/DC/94 (published Dec. 23, 1996), *available at* http://www.wipo.int/documents/en/diplconf/ distrib/pdf/94dc.pdf.

69. Bechtold, *supra* note 48; Information Society Directive, *supra* note 2, art. 5(6).

70. *See generally* SENFTLEBEN, *supra* note 52.

71. SENFTLEBEN, *supra* note 52, at 206.

72. WIPO, 2 RECORDS OF THE INTELLECTUAL PROPERTY CONFERENCE OF STOCKHOLM 291-292 (1967), *available at* http://www.oup.com/uk/booksites/content/9780198259466/15550029; SENFTLEBEN, *supra* note 52, at 158.

73. SAM RICKETSON, THE BERNE CONVENTION FOR THE PROTECTION OF LITERARY AND ARTISTIC WORKS: 1886-1986 (1987), 479-81.

74. *See generally* GUIBAULT, *supra* note 13, at 90-110 (qualifying limitations in terms of either a subjective right or an objective right or privilege).

their defense against copyright holders to remedies against technical protection measures that more resemble "user rights." This section considers the various legal manifestations of private copying limitations as they presently exist at the European level and in the Member States.

Article 5(2)(b) of the Information Society Directive, which allows Member States to permit private copying under specific conditions, is part of a very lengthy Article 5 that exhaustively lists permitted limitations. Although Article 5(1) of the Directive obliges Member States to exempt certain acts of transient copying from the exclusive right of reproduction, including such consumptive acts as browsing and caching content from the web, the other listed limitations are optional. Member States may or may not choose to adopt them, but are not allowed to legislate limitations beyond the list.[75]

As the structure and official caption of Article 5, "Exceptions and limitations," suggest, the norms of Article 5, inasmuch as they are transposed by the national legislatures, set limits to the copyright holders' exclusive rights and thus form a first line of defense against copyright holders invoking their exclusive rights. But the Directive has left the Member States in the dark as to the legal nature and enforceability of these user freedoms. Are they simply "exceptions" that may be, and surely will be, pre-empted by contract, by way of the now omnipresent (click-wrap) end user licenses? Or are they inalienable rights that provide relief to qualified users even inside contractual relationships?

The Directive's silence on this crucial issue contrasts starkly with the two earlier European directives dealing with "digital" issues.[76] Both the Computer Programs Directive and the Database Directive guarantee lawful users certain end user freedoms, such as a right to make back-up copies[77] of and to study or test[78] legally acquired computer software, as well as a right to consult databases.[79] These freedoms are not framed as mere "exceptions" to copyright, but as full-fledged end user rights that cannot

75. Bechtold, *supra* note 48, at 369; Information Society Directive, *supra* note 2, art. 5(1)(b).

76. *See* LUCIE GUIBAULT ET AL., STUDY ON THE IMPLEMENTATION AND EFFECT IN MEMBER STATES' LAWS OF DIRECTIVE 2001/29/EC ON THE HARMONISATION OF CERTAIN ASPECTS OF COPYRIGHT AND RELATED RIGHTS IN THE INFORMATION SOCIETY, REPORT TO THE EUROPEAN COMMISSION 160 (2007) [hereinafter STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC], *available at* http://www.ivir.nl/publications/guibault/Infosoc_report_2007.pdf.

77. Computer Programs Directive, *supra* note 17, art 5(2).

78. *Id.*, art. 5(3).

79. Database Directive, *supra* note 17, art. 6(1).

be overridden by contract.[80] However, the Information Society Directive does not expressly give similar imperative status to these exemptions for private copying.[81]

Given the Information Society Directive's silence, the legal nature of the limitations listed in Article 5 remains unclear, and is left for the time being to the discretion of the Member States. Two Member States, Belgium and Portugal, have dealt with the issue in their national copyright laws. According to Belgian law, as amended in 1998, nearly all exceptions mentioned in the Belgian Copyright Act, including a private copying exemption, have imperative character and thus cannot be overridden by contract.[82] Similarly, the Portuguese Copyright Act, as recently amended during the process of transposing the Information Society Directive, declares null and void any contractual provision eliminating or impeding the normal exercise of the free uses mentioned in the Act.[83]

While the enforceability within contractual relationships of the limitations listed in Article 5 remains unclear, the Information Society Directive is more interventionist when it comes to protecting users against DRM. Although the Directive does not allow users to circumvent technological "locks" designed to prevent unauthorized copying,[84] Article 6(4) seeks to ensure that users of copyrighted works are able to benefit from designated copyright limitations despite DRM measures meant to prevent copying.[85]

---

80. *Id.*, art. 15; Computer Programs Directive, *supra* note 17, art. 9(1).

81. "Imperative" status means that the exemption is mandatory in contractual relationships—in other words, that the user's freedom (e.g., to make a private copy) cannot be overridden by contract. Note that according to Article 9 of the Information Society Directive, the provisions of the Directive are without prejudice to "the law of contract." An amendment of the European Parliament stating that "no contractual measures may conflict with the exceptions or limitations incorporated into national law pursuant to Article 5" was rejected by the Council. STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC, *supra* note 76, at 160.

82. Loi relative au droit d'auteur et aux droits voisins [Law on Copyright and Neighboring Rights of 1994], June 30, 1994, Moniteur belge/Belgisch Staatsblad 27/07/1994 at 19297, § 22 (Belg.), *translation available at* http://www.wipo.int/clea/docs_new/pdf/en/be/be003en.pdf. *See* STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC, *supra* note 76, at 160-61.

83. Law No. 62/98 of Sept. 1, 1998, Diário da República [D.Re.] [Official Gazette of Portugal] I Série-A [Series I], Sept. 1, 1998, p. 4524. (Portuguese Act on Copyright and Neighboring Rights) *See* STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC, *supra* note 76, at 160-61.

84. Information Society Directive, *supra* note 2, art. 6(1); *see also id.*, rec. 52.

85. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make

Member States may, but are not obliged to, extend this "facilitation" rule to the private copying exemption,[86] as several countries indeed have done.[87] In those countries, disenfranchised consumers unable to make "private copies" from DRM-protected works have recourse to the courts, special government agencies, a copyright tribunal, or direct government intervention to ensure that such copies can actually be made.[88]

For example, the recently revised French Copyright Act[89] establishes a special "Authority" charged with regulating DRM measures.[90] Private individuals, consumer associations, and other organizations are entitled to bring a case before the Authority requesting the application of the private copying limitation codified in the French Act.[91] Accordingly, the Authority has the power to arbitrate disputes and to determine the minimum number of authorized private copies allowed, depending on the type of work or subject matter protected.[92]

> available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.
>
> A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

Id., art. (6)(4).

86. *Id.*

87. These countries include France, Italy, the Netherlands, and Spain. STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC, *supra* note 76, at 160-62. *See* GUIDO WESTKAMP, PART II: THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC IN THE MEMBER STATES, REPORT TO THE EUROPEAN COMMISSION (2007), *available at* http://www.ivir.nl/ publications/guibault/InfoSoc_Study_2007.pdf.

88. STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC, *supra* note 76, at 126-29.

89. Law No. 2006-961 of Aug. 1, 2006 art. 14, art. L. 331-6, Journal Officiel de la République Française [J.O.] [Official Gazette of France], Aug. 3, 2006, p. 11529.

90. STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC, *supra* note 76, at 127.

91. CODE CIVIL [C. CIV.] art. L. 122-5 (2) (French Intellectual Property Code).

92. STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC, *supra* note 76, at 127.

The remedies articulated in Article 6(4) of the Directive cannot be enforced against DRM-protected works offered on-demand under agreed-upon contractual terms.[93] Because DRM-protected content is typically offered online under click-wrap licenses, this exception effectively swallows the rule. Moreover, if a copyright holder designs a DRM measure that allows some private copying, then Member States are prohibited from recognizing the consumer remedies articulated in Article 6(4).[94] In any case, copyright holders may use DRM measures to control the number of reproductions in accordance with Articles 5(2)(b) and 5(5).[95]

D. Assessment

To what extent does the emerging body of European copyright law warrant a consumer right to make private copies, and thus cater to the needs and interests of information consumers? Clearly, the traditional copyright system has little to offer to consumers directly. Even in 2007, consumers are not expressly mentioned in the law of copyright.[96] In the old days of analog reproduction, that did not really matter. Information consumers remained largely off copyright law's radar screen. Copyright and consumer law operated on different planes.

With the advent of the digital age, reproduction in copyright has taken on an entirely new meaning. The information consumer has involuntarily stepped into the copyright arena, and immediately occupied center stage. The expansive interpretation of the reproduction right that has drawn the consumer into the sphere of copyright has seriously compromised end user freedoms and thus does not bode well for consumer autonomy. Despite

---

93. Information Society Directive, *supra* note 2, art. 6(4).

94. STUDY ON THE IMPLEMENTATION OF DIRECTIVE 2001/29/EC, *supra* note 76, at 108.

95. *Id.* at 111, 155. See Information Society Directive, *supra* note 2, rec. 52, which states:

> Voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, as well as measures taken by Member States, do not prevent rightholders from using technological measures which are consistent with the exceptions or limitations on private copying in national law in accordance with Article 5(2)(b), taking account of the condition of fair compensation under that provision and the possible differentiation between various conditions of use in accordance with Article 5(5), such as controlling the number of reproductions. In order to prevent abuse of such measures, any technological measures applied in their implementation should enjoy legal protection.

Id.

96. *See supra* Section II.A.

legislative attempts to protect end user freedom, every act of information consumption by digital means nowadays effectively requires a "license." In Europe, this has led to a variety of consumer-protective measures in copyright law, ranging from simple "exceptions" allowing private copying without permission of copyright holders, to "use rights" that cannot be overridden by contract. In addition, European law provides certain, albeit rather toothless, remedies to certain users disenfranchised by DRM technology.

Despite the promise of the Information Society Directive to harmonize and add legal certainty to the European copyright framework,[97] the laws on private copying in the Member States still vary enormously, both in scope and legal character. While most countries of the European continent permit some measure of private copying, copying for personal uses is generally considered copyright infringement in the United Kingdom and Ireland. Most Member States treat private copying as a simple "exception" to the copyright holder's exclusive right of reproduction, but some countries, such as Belgium and Portugal, have given elevated status to the limitation by immunizing private copying against contractual overrides.[98] Other countries, including France, Italy, and Spain, have made the limitation enforceable against technological protection measures.[99]

As Part III shall demonstrate, the varied legal landscape of private copying in Europe has a ripple effect on consumer law and explains much of the confusion surrounding the legal status of private copying in European consumer law.

III. EUROPEAN CONSUMER LAW

European consumer law sets basic rules for the bargaining game between "persons acting as consumer in the marketplace and their counterparts, the businesses."[100] The approach of consumer law differs fundamentally from the copyright-holder-centric approach of copyright law. Consumer law is consumers' law, where "the consumer" is the central protagonist.

97. Information Society Directive, *supra* note 2, rec. 4.

98. *See supra* Section II.C.

99. *See supra* text accompanying note 87.

100. Thomas Wilhelmson, *Consumer Law and the Environment: From Consumer to Citizen*, 21 J. CONSUMER POL. 45, 46 (1998).

Consumers are neither professional sellers nor producers. In all the various definitions of the "consumer"[101] in European consumer law, a "consumer" is a natural person acting outside his professional capacity. In other words, consumer law is the body of law that protects consumers' reasonable expectations to enjoy goods and services in their private environment. To this end, consumer law is designed to protect and promote the interests of consumers of goods and services in their commercial relationship with suppliers.

European consumer law has influenced to a substantial degree the consumer laws of the Member States of the European Union.[102] Furthermore, the Directorate General for Consumer Affairs has begun to show a pronounced interest in digital information consumers and the potential of consumer law to protect their interests,[103] and an extensive review of the current state of EC law is on its way.[104] A chief objective of the EC review is to strengthen the rights of consumers of digital information services.[105] Without repeating this exercise, this Part demonstrates on a more abstract level how consumer law can give "teeth" to the private copying exemption. To this end, this Part analyzes the main rationales and legal tools of

---

101. *Cf.* Council Directive 2005/29, Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market, art. 2(a), 2005 O.J. (L 149) 22 (EU) [hereinafter Unfair Commercial Practices Directive] ("any natural person who, in commercial practices covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession"); Council Directive 2000/31 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, art. 2(e), 2000 O.J. (L 178) 1, 7 (EC) [hereinafter Electronic Commerce Directive] ("any natural person who is acting for purposes which are outside his or her trade, business or profession"); Council Directive 99/44 on Certain Aspects of the Sale of Consumer Goods and Associated Guarantees, art. 1(2)(a), 1999 O.J. (L 171) 12, 14 (EC) [hereinafter Sale of Consumer Goods Directive] ("any natural person who, in the contracts covered by this Directive, is acting for purposes which are not related to his trade, business or profession"); Council Directive 97/7 on the Protection of Consumers in Respect of Distance Contracts, art. 2(2), 1997 O.J. (L 144) 19 (EC) [hereinafter Distance Selling Directive] ("any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession"); Council Directive 93/13 on Unfair Terms in Consumer Contracts, art. 2(b), 1993 O.J. (L 95) 29 (EC) [hereinafter Unfair Terms Directive] ("any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession").

102. NORBERT REICH & HANS-W. MICKLITZ, EUROPÄISCHES VERBRAUCHERRECHT [EUROPEAN CONSUMER LAW] 45 (4th ed. 2003).

103. *Commission Green Paper on the Review of the Consumer Acquis*, at 6, COM (2006) 744 final (Feb. 8, 2007) [hereinafter *2006 Green Paper*].

104. *Id.* at 6.

105. *Id.* at 3.

generic European consumer law,[106] leaving aside procedural questions and the effectiveness of remedies.

A. Rationales

Two distinct and major rationales underlie consumer law—to empower the consumer as a sovereign market actor and to protect the consumer as the weaker party in commercial dealings with suppliers.

1. Empowering the Consumer as Sovereign Market Actor

The image of the consumer as a sovereign market actor has shaped large parts of European consumer law.[107] The prevailing image of the European consumer in EC law is that of the "average" consumer who is "reasonably well informed and reasonably observant and circumspect"—a concept developed by the European Court of Justice.[108] This average consumer, provided he is adequately informed, is well equipped to address his own needs and preferences and is able to search among the services and products that are publicly available for those that best meet his needs. Of course, what best addresses a consumer's needs differs from consumer to consumer. Such needs can be economic (e.g., getting the best deal for the money), non-economic (e.g., the making of private copies to engage in transformative uses), self-centered, or altruistic.[109] Note that in the European perception the sovereign consumer plays a far more active role than just "consuming." He is an active driver behind the development of the Internal Market[110] and behind a competitive offering of services that re-

106. Note that for the time being there is little sector-specific information consumer law. Some provisions in the Electronic Commerce Directive are aimed specifically at digital consumers, including, but not limited to, consumers of information services and products.

107. J.G.J. Rinkes, *Europees consumentenrecht* [European Consumer Law], *in* HANDBOEK CONSUMENTENRECHT. EEN OVERZICHT VAN DE RECHTSPOSITIE VAN DE CONSUMENT [CONSUMER LAW. AN OVERVIEW OF THE LEGAL POSITION OF THE CONSUMER] 31, 36 (E.H. Hondius & G.J. Rijken eds., 2006).

108. Unfair Commercial Practices Directive, *supra* note 101, rec. 18. *See also* Case C-210/96, Gut Springenheide GmbH and Rudolf Tusky v. Oberkreisdirektor des Kreises Steinfurt—Amt für Lebensmittelüberwachung, 1998 E.C.R. I-04657, para. 55; Case C-470/93, Verein gegen Unwesen in Handel und Gewerbe Köln e.V. v. Mars GmbH, 1995 E.C.R. I-01923, para. 24.

109. *Cf.* Thomas Wilhelmsson, *The Consumer's Right to Knowledge and the Press*, *in* CONSUMER LAW IN THE INFORMATION SOCIETY 367, 379 (Thomas Wilhelmsson, Salla Tuonminen & Heli Tuomola eds., 2001) (discussing what constitutes reasonable expectations of newspaper consumers); Thierry Bourgoignie, *Characteristics of Consumer Law*, 14 J. CONSUMER POL. 293, 303 (1992).

110. One of the goals of current EU policy is to realize an Internal or Single European Market, a situation where people, goods, services, and capital can move freely be-

sponds to the interests of consumers of the European Union.[111] In other words, if the European consumer attaches any value to private copying, it is up to him to make markets deliver information products and services that can be copied for private use.

To be an active market player, the sovereign consumer must have choice. Accordingly, protecting the sovereign consumer's "right to choice" is a central objective of European consumer law.[112] Principle One of the EC's Ten Basic Principles of Consumer Protection in the European Union is: "Buy what you want, where you want."[113] Consequently, consumer law's role is to create the market conditions that allow consumers to "vote with their purse" by rectifying market failures, most notably information asymmetries.[114] Consumer information is an important prerequisite for the sovereign consumer to manage his own affairs.[115] Thus, EU consumer policies focus on consumer empowerment, or "consumer assistance," with minimal intervention,[116] rather than on consumer protection. The better the market serves the interests of consumers, the smaller the role of the legislature can remain.[117]

2. Protecting the Weaker Party

In contrast, proponents of a more interventionist role of the state in consumer matters warn against overestimating the self-regulatory powers of the market and emphasize that empowering the consumer is not always sufficient to guarantee an adequate standard of consumer protection.[118] Common justifications for a more activist role of the regulator are welfare

---

tween the different national markets of the member states of the European Union without encountering legal or economic barriers. For further information visit European Commission, The EU Single Market, http://ec.europa.eu/internal_market/index_en.htm (last visited Aug. 8, 2007).

111. *Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee, EU Consumer Policy strategy 2007-2013 Empowering Consumers, Enhancing Their Welfare, Effectively Protecting Them*, at 2-6, COM (2007) 99 final (Mar. 13, 2007) [hereinafter *Empowering Consumers*].

112. René Barents, *The Image of the Consumer in the Case Law of the European Court*, 1 EUR. FOOD L. REV. 6, 8 (1990).

113. EUROPEAN COMMISSION, CONSUMER PROTECTION IN THE EUROPEAN UNION: TEN BASIC PRINCIPLES 3 (2005), *available at* http://ec.europa.eu/consumers/cons_info/10principles/en.pdf . *See also* Barents, *supra* note 112, at 8.

114. Barents, *supra* note 112, at 15-18.

115. *Empowering Consumers*, *supra* note 111, at 3.

116. Bourgoignie, *supra* note 109, at 305.

117. *See Empowering Consumers*, *supra* note 111.

118. *See, e.g.*, Barents, *supra* note 112, at 22; Norbert Reich, *Diverse Approaches to Consumer Protection Philosophy*, 14 J. CONSUMER POL. 257, 260-61 (1992).

economics and imbalances in the transactional relationship between consumers and service providers.[119] Through this lens, the consumer is less the sovereign decision maker and more the structurally weaker party in commercial negotiations. Unlike the sovereign consumer, the weak consumer is less capable of minding his own affairs because he lacks information, education, awareness, or negotiation power.[120] Thus, removing market failures that obstruct the consumer's "right to choice" is not enough to protect the weak consumer.[121] From this perspective, the primary role of consumer law is to intervene where consumers suffer harm or are treated unfairly by suppliers in business relationships.

Playing a central role in European consumer law, corrective justice is also an important justification underlying consumer sales law, the rules on unfair commercial business practices, and the rules on contracts.[122] The basic assumption is that commercial dealings between consumers and suppliers must weigh the legitimate interests of both parties to be considered just and fair. An important benchmark in assessing the fairness of a transaction is the standard of parties' "reasonable expectations."[123] This standard has evolved into one of the leading benchmarks of European consumer law.[124] Consideration of parties' reasonable expectations sets limits to the principle of freedom of contract that defines the commercial relationship between consumers and suppliers.[125] The moment that a product or service does not meet the reasonable expectations of the consumer, the contract can no longer be assumed to reflect the consumer's free will to commit to the transaction.

Distributive or social justice is a related rationale underlying consumer law and includes a more abstract social policy motive: to increase equality

---

119. Reich, *supra* note 118, at 260-61.

120. Ewoud Hondius, *The Protection of the Weak Party in a Harmonised European Contract Law: A Synthesis*, 27 J. CONSUMER POL. 245 (2004); Santiago Cavanillas Múgica, *Protection of the Weak Consumer Under Product Liability Rules*, 13 J. CONSUMER POL. 299, 300-02 (1990).

121. Barents, *supra* note 112, at 16 (referencing law of the European Court of Justice).

122. Thomas Wilhelmsson, *Consumer Law and Social Justice*, *in* TWELVE ESSAYS ON CONSUMER LAW AND POLICY 191, 192-93 (Tuuli Junkkari ed. 1996).

123. Wilhelmsson, *supra* note 109, at 378; CLARISSE GIROT, USER PROTECTION IN IT CONTRACTS: A COMPARATIVE STUDY ON THE PROTECTION OF THE USER AGAINST DEFECTIVE PERFORMANCE IN INFORMATION TECHNOLOGY 32 (Kluwer Law International 2001); Martien Schaub, *A Breakdown of Consumer Protection Law in the Light of Digital Products*, INDICARE MONITOR, July 29, 2005, at 13, *available at* http://www.indicare.org/tiki-read_article.php?articleId=123.

124. Wilhelmsson, *supra* note 109, at 380.

125. *See* GIROT, *supra* note 123, at 33-51.

and fairness in society.[126] Governments and policy makers weigh considerations of distributive justice and then translate these abstract goals into concrete policy measures. For example, during the German EU presidency, considerations of distributive justice served as an impetus to the adoption of the Charter on Consumer Sovereignty in the Digital World, part of the initiative of the German Federal Ministry for Food, Agriculture and Consumer Protection.[127] The Charter highlighted the importance for future consumer policy of ensuring equal access for consumers to a diversity of cultural products and services, including respect for the existing exemptions under copyright law.[128] The ministry acknowledged that the protection of fundamental freedoms—such as freedom of speech, freedom from discrimination, and the protection of privacy—is a new challenge for consumer policy.[129] To this end, the Charter emphasized the need to formulate clear rights for consumers of digital services.[130]

European telecommunications law provides an example of the realization of distributive goals and fundamental freedoms as a matter of consumer policy. Certain rules in European telecommunications law, specifically aimed at consumers of communication services, take as their policy objective the realization of fair and equal access to services and of fundamental rights of the information consumer.[131] For example, the Universal Service Directive[132] provides a mix of measures that both serve the interests of individual end users *and* pursue social objectives, such as the broad accessibility and affordability of communications services for all users, including disadvantaged users.[133] The underlying image of the consumer

126. Wilhelmsson, *supra* note 122, at 193 (defining distributive justice as "the goal of increasing equality between members of society").

127. BMELV Consumer Protection, Charter increases consumer confidence in digital technologies, http://www.bmelv.de/cln_045/nn_749980/EN/03-ConsumerProtection/CharterDig.html__nnn=true (last visited Aug. 8, 2007).

128. *Id.* at 1, 3.

129. *Id.*

130. *Id.* at 1.

131. European communications law provides for a sector-specific definition of the consumer of communication services. "Consumer" means "any natural person who uses or requests a publicly available electronic communications service for purposes which are outside his or her trade, business or profession." Council Directive 2002/21 on a Common Regulatory Framework for Electronic Communications Networks and Services, art. 2(i), 2002 O.J. (L 108) 33, 39 (EU) [hereinafter Framework Directive].

132. Council Directive 2002/22 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, 2002 O.J. (L 108) 51 (EU) [hereinafter Universal Service Directive].

133. *Id.* art. 1(1).

in the Universal Service Directive is *also* that of a citizen.[134] Thus, apart from a set of "classical" consumer rights,[135] the Directive entitles national regulatory authorities to safeguard fairness in commercial dealings between consumers and providers of telecommunications services, for example, by defining reasonable pricing and prohibiting discriminatory practices or practices that impede the ability of consumers to choose between different operators.[136] Giving national regulatory authorities this power achieves "the twin objectives of promoting effective competition," which the Directive translates into greater choice for consumers, and "pursuing public interest needs, such as maintaining the affordability of publicly available telephone services for some consumers."[137] Where the market will not likely give consumers access to services at affordable conditions, the Directive authorizes Member States to mandate access to a pre-defined minimum set of services to all consumers at affordable prices, the so-called universal service obligations.[138] Universal service obligations are another example of rules tailored in part for consumers in pursuit of distributive justice—in this case, to provide access to communications services for disadvantaged consumers, such as consumers in geographically isolated areas, financially weaker consumers, and elderly or disabled consumers.[139]

B. Private Copying and Consumer Law

European consumer law provides for a number of legal instruments that may legitimize the interests of consumers in making private copies. This section introduces three of these instruments: the rules of conformity of products with reasonable consumer expectations, the test of fairness of contractual terms, and rules on consumer information.

1. Conformity with Consumers' Reasonable Expectations

Consumers have a right to expect that goods "show the quality and performance which are normal in goods of the same type and which the

134. Peter Rott, *Consumers and Services of General Interest: Is EC Consumer Law the Future?*, 30 J. CONSUMER POL. 49, 53 (2007).

135. *E.g.*, Universal Service Directive, *supra* note 132, art. 20 (articulating minimum requirements for consumer contracts about the supply of communication services); *id.* arts. 20-21 (requiring information about prices, service quality, and standard terms and conditions); *id.*, art. 24 (discussing interoperability of consumer digital television equipment).

136. This and the specific conditions are laid down in Article 17(1)-(2) of the Universal Service Directive, *supra* note 132.

137. *Id.*, rec. 26.

138. *Id.*, arts. 1(2), 3(1).

139. *Id.*, rec. 7.

consumer can reasonably expect, given the nature of the goods."[140] According to the EC Directive on Sale of Consumer Goods, the right to expect quality in goods that is in conformity with consumers' reasonable expectations cannot be restricted or abrogated by contract.[141] For the time being, however, the European rules on product conformity do not extend to services; the matter is currently under review.[142]

The reasonable expectation test is subject to judicial interpretation. There is still very little conclusive case law on whether consumers have a right to expect to be able to make private copies of information products or services. For this reason, the following discussion remains somewhat speculative. Note that the reasonable consumer expectation standard counterweighs the copyright-holder-centered norms on private copying that prevail in a copyright law analysis.[143] The test leaves room for considering the individual circumstances of a particular case, such as a product's intended use,[144] and thereby introduces an individual, subjective element into an environment usually governed by mass standard contracts. On the other hand, the test also leaves room to consider more objective factors, such as price, shared social values, voluntary industry guidelines as instruments of self-regulation, industry practice, and the "normal use" of a product.[145] Normal use can refer to consumptive use in a narrow sense, such as, for example, the ability to listen to, read, or watch digital products.[146] Normal use can also extend to consumptive uses in a broader sense, including the making of private copies.[147] What constitutes normal use of a product depends not merely on consumer perception but also on external factors, such as the state of the market, the state of technology,

140. Sale of Consumer Goods Directive, *supra* note 101, arts. 3(1), 2(2)(d).

141. *Id.*, art. 7(1).

142. *2006 Green Paper*, *supra* note 103, at 24.

143. *Cf. supra* Section II.C.

144. *See* Sale of Consumer Goods Directive, *supra* note 101, art. 2(2)(b).

145. *Cf.* GIROT, *supra* note 123, at 47-50.

146. *See, e.g.*, Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Nanterre, 6e ch., Sept. 2, 2003, Françoise M. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=33; Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, 5e ch., 1e sec., Jan. 10, 2006, Christophe R. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article =1567 (both cases holding that a DRM-protected CD that cannot play on a car radio is "defective" under the French rules on nonconformity (Article 1646 of the Civil Code), in part because consumers had not been informed about this prior to purchase).

147. Peter Rott, *Die Privatkopie aus der Perspective des Verbraucherrechts*, *in* INTERESSENAUSGLEICH IM URHEBERRECHT [BALANCE OF INTERESTS IN COPYRIGHT LAW] 267, 268 (R. Hilty & A. Peukert eds. 2004)

and the nature of comparable goods.[148] A limiting element is the reasonableness of consumers' expectations—not all expectations of consumers merit protection; consumers must have reasonable grounds to expect a certain quality from a product.

If a court were faced with the question of whether consumers should legitimately expect to make private copies, it might consider the following arguments. European consumer surveys have demonstrated that the making of copies for private use—be it for social purposes (sharing with close family or friends), making back-up copies, or time-shifting—is an important element of how consumers have grown accustomed to using digital content.[149] Consequently, a court might conclude that the making of private copies constitutes "normal use." However, the mere fact that consumers have grown accustomed to certain forms of use is no guarantee that such uses will remain "normal" in the future. For example, if music or software on a CD is sold at a considerably lower price than other comparable products, one could argue that consumers must also expect the CD to be of a lower quality or to have more limited functionality. Here, the ability to make private copies might arguably not be a reasonable consumer expectation. In the (unlikely) scenario that all digital content were subject to technological copy control protection, consumers would no longer have good reason to believe that the making of private copies is still "normal." Even then, however, consumers might still be entitled to expect being able to make private copies in situations where levies are imposed on blank carriers, which is still the case in most Member States of the EU.[150] In countries that have a private copying limitation that allows copying of

148. E.H. Hondius, *Consumentenkoop van Roerende Zaken [Consumer Purchase of Goods]*, *in* HANDBOEK CONSUMENTENRECHT. EEN OVERZICHT VAN DE RECHSTPOSITIE VAN DE CONSUMENT [CONSUMER LAW. AN OVERVIEW OF THE LEGAL POSITION OF THE CONSUMER] 93, 104-05 (E.H. Hondius & G.J. Rijken eds. 2006).

149. DUFFT ET AL., DIGITAL VIDEO USAGE, *supra* note 1, at 26-28; DUFFT ET AL., DIGITAL VIDEO USAGE, *supra* note 1, at 26-28.

150. *Compare* Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, 5e ch., 1e sec., Jan. 10, 2006, Christophe R. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=1567 (holding as an argument against a potential conflict between private copying and legitimate interests of rightholders that because French law imposes levies on blank carriers, holders of the exclusive reproduction right receive a remuneration each time that a blank carrier is being bought), *with* Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, 3e ch., 2e sec., Apr. 30, 2004, Stéphane P. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=722, *and* Tribunal de première instance [T.P.I.] [ordinary court of original jurisdiction] Brussels, May 25, 2004, Rôle de Référes 2004, 46 (Belg.) (both cases holding that the fact that levies are paid to copyright holders does not indicate legislative intent to grant the "right to private copying").

digital content, the existence of such a provision in law can be another valid reason for consumers to expect that private copying remains possible, even in a world ruled by Digital Rights Management (DRM).

It is ambiguous whether and to what extent the private copying limitation in the Information Society Directive supports consumers' reasonable expectations to make private copies.[151] On the one hand, a reasonably observant and circumspect consumer will understand that the making of a large number of copies to later distribute or sell would go beyond copying for private use. In other cases, however, the relationship between the private copying limitation, the three-step test, the limitation's interface with contract, and the rather cryptic provision of Article 6(4) of the Information Society Directive are confusing, to say the least.

Courts may interpret the normative role of copyright law's private copying exemption in consumer law in two different ways. One possibility is that courts will resolve the unclear legal situation against the consumer and conclude that, because there is no clear "right to private copying" in copyright law, consumers cannot expect to be able to make private copies of, for example, DVDs or CDs.[152] The difficulty with this approach is that to expect judgment no more sophisticated than that of a layman from the consumer leaves the reasonable expectation test devoid of any meaning. The other possibility is that a court might conclude that the interpretation of the private copying limitation is not a matter for private parties to decide, but rather for the lawmaker. If the lawmaker wishes to prioritize the commercial interests of right holders in preventing private copying, the lawmaker must clarify this in copyright law itself. Until then, consumers

---

151. *See supra* Section II.C.

152. *See, e.g.*, Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, 3e ch., 2e sec., Apr. 30, 2004, Stéphane P. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=722, *aff'd*, Cour de Cassation [CC] [highest court of ordinary jurisdiction] Paris, 1e ch., Feb. 28, 2006, Stéphane P. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=1583 (holding that the private copying exception is no right and that consumers cannot reasonably expect making private copies of a DVD because this would conflict with the normal exploitation of such a DVD and hence with the legitimate interests of rightholders); Tribunal de première instance [T.P.I.] [ordinary court of original jurisdiction] Brussels, May 25, 2004, Rôle de Référes 2004, 46 (Belg.) (denying a claim of consumers to being able to make private copies, because consumers had no right to private copying and finding the primary purpose of the private copying exception is to signify that the consumer is not required to ask for permission for the making of private copies). *See also* Cour d'appel [CA] [regional court of appeal] Paris, 4e ch., sec. A, Apr. 4, 2007, Stéphane P. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=1909 (holding that the private copying exception may be used solely as defense but not as a legal basis for affirmative actions against suppliers).

might reasonably expect to be able to make private copies, even if DRM technologies are employed by distributors of digital media.[153]

Finally, both consumers and sellers themselves can influence the quality standard that consumers can reasonably expect. For example, under the Directive on Sale of Consumer Goods,[154] if a consumer indicates to the seller before purchase the intent to make back-up copies of a CD or to rip the CD to play on an MP3 player, and the seller agrees, then the consumer has a legally enforceable contractual expectation that no DRM technology will prevent him from making copies. More likely, however, the seller or manufacturer will inform consumers of what they may expect from the product or service. For example, sellers or manufacturers may do this through advertising or labeling of the product, assuming the information is specific enough. If a consumer is notified in advance that a product or service does not permit private copying, or sets limits thereto, the consumer cannot later claim that his expectations have not been met.[155] In other words, suppliers of CDs and DVDs can easily avoid liability under the rules on nonconformity by preemptively informing consumers prior to purchase that a CD or DVD cannot be copied. If suppliers do not label their products as such on their own initiative, a number of European directives expressly require suppliers to inform consumers about the main characteristics of a product or service, an obligation which arguably includes information about the ability to make copies.[156]

If a product lacks a quality that consumers are entitled to expect, consumers have a choice of remedies under either national or European consumer law. One remedy is to have the good restored to conformity with

153. *See, e.g.*, Cour d'appel [CA] [regional court of appeal] Paris, 4e ch., sec. B, Apr. 22, 2005, Stéphane P. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=1432. Here, the court held that although the private copying exception is not a full-fledged right of consumers, it is also not entirely at the disposal of suppliers. According to the court, it is the legislator's prerogative to formulate limitations to the private copying exception or the modalities of limiting the private copying exception ("cette exception légale ne peut être limitée qu'aux conditions précisées par les textes"). Moreover, the complete blocking of any possibilities of making private copies was an impermissible behavior under French copyright law. *See also* Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, 5e ch., 1e sec., Jan. 20, 2006, Christophe R. (Fr.). Based on its reading of Article 6(4) of the European Information Society Directive, the court concluded that technological protection measures must respect the French private copying exception. The court found that DRM measures that prevent private copying are not in compliance with French copyright law.

154. Sale of Consumer Goods Directive, *supra* note 101, arts. 2(1), 2(2)(b), 3(1).

155. *Id.*, art. 2(3); Rott, *supra* note 147, at 267, 283; Schaub, *supra* note 123, at 14.

156. *See infra* Section III.B.3.

the contract free of charge or to have the good replaced.[157] For example, if a DRM mechanism that impedes the making of private copies is deemed to be the cause of the defective quality, a consumer may demand removal of the DRM measure or a new copy of the product without copy control. If this is impossible or burdens the seller with disproportionately high costs, the consumer may demand a price reduction or may return the product against the purchase price.[158] Under the laws of some Member States, consumers are also entitled to the compensation of damages.[159]

2. Fairness of Contractual Terms

Maintaining "fairness" in commercial dealings between consumers and suppliers is the main objective of the EC Directive on Unfair Terms in Consumer Contracts (the "Unfair Terms Directive").[160] Under the Unfair Terms Directive, "fairness" is understood as the balance of the parties' rights and obligations that arise under a contract.[161] The Directive protects consumers against the contracting away of important consumer rights or against otherwise uncompensated one-sided obligations in standard form contracts.[162] The Directive's underlying assumption is that standard form contracts do not allow for individual negotiation on the part of the consumer.[163] This makes the consumer more vulnerable to one-sided, disadvantageous obligations. The key question here is whether a contractual clause that prohibits or restricts the making of private copies is "unfair" under the Directive. If so, the clause will not be binding upon the consumer.[164]

Part of the Directive is an annex comprising a "blacklist" of contractual terms that are presumed unfair.[165] Most relevant to the discussion of "fairness" of restrictions on private copying is the blacklisted term that reserves the right to unilaterally change the terms and conditions of the contract, for example, the number of copies that a consumer can make.[166]

---

157. Rinkes, *supra* note 107, at 111-112.

158. *Id.* at 112.

159. *Id.* at 116. *See, e.g.*, Burgerlijk Wetboek [BW] [Civil Code] bk. 5, tit. 6, art. 74 (Neth.); Bürgerliches Gesetzbuch [BGB] [Civil Code] Aug. 18, 1896, Reichsgesetzblatt, [RGBI] § 437(3) (F.R.G.).

160. Unfair Terms Directive, *supra* note 101, rec. 9.

161. *Id.*, art. 3(1).

162. *Id.*, rec. 9.

163. *Id.*

164. *Id.*, art. 6(1).

165. *Id.*, art. 3(3), Annex.

166. *Compare id.*, Annex (1)(k) *with* iTunes Store, Terms of Service, term 20, http://www.apple.com/legal/itunes/us/service.html (last visited June 21, 2007). *See also*

Apart from this clause, the annex has little to say about the fairness of a contractual waiver of the private copying exemption.[167]

The compatibility of restrictive terms with the principle of objective good faith under Article 3(1) of the Unfair Terms Directive requires courts to weigh the legitimate interests or reasonable expectations of consumers against those of copyright holders. Article 3(1) of the Unfair Terms Directive reads: "A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer." Like the rules on nonconformity, the standard of reasonable consumer expectations again serves as a benchmark to assess fairness.[168] The reasonableness of a consumer's expectation to make private copies depends not only on the scope of the private copying limitation, but also on other factors. Again, courts may consider the price of the product or service, the number of copies allowed, what is "normal" in comparable products or services, the purpose for which a product or service is bought, the reasons for copying—for example, to make back-up copies, to share,[169] or for creative uses—among other factors.[170] The legal scholar Lucie Guibault, who studied the interplay of the rules on unfair contracts and copyright law in depth, concludes convincingly that the answer is likely to vary between Member States.[171] The outcome would largely depend on the legal climate in each Member State, the attitude of its courts to consumer issues, and the willingness of its courts to also consider more fundamental rights of consumers, such as freedom of speech or the right to privacy.[172]

3. *Rules on Consumer Information*

In addition to rules on product conformity and unfair terms, European consumer law includes a variety of rules on consumer information. The primary goal of these rules is to improve consumer autonomy and freedom

---

Lars Grøndal, *DRM and contract terms*, INDICARE MONITOR, Feb. 24, 2006, at 13-14, *available at* http://www.indicare.org/tiki-download_file.php?fileId=174.

167. *See also* GUIBAULT, *supra* note 13, at 254.

168. Schaub, *supra* note 123; GIROT, *supra* note 123, at 62-66.

169. Rott even goes so far to argue that the principle of good faith could protect the interest of consumers in sharing contents with their direct social environment. Rott, *supra* note 147, at 282.

170. GUIBAULT, *supra* note 13, at 255. Compare GIROT, *supra* note 123, at 46-49.

171. GUIBAULT, *supra* note 13, at 256.

172. It would exceed the scope of this paper to deal with this question in more depth. Instead, see the excellent comparative analysis of Guibault. GUIBAULT, *supra* note 13, at 256, 263. *See also* Rott, *supra* note 147, at 280.

of choice,[173] predicated on the assumption that suppliers are at an advantage because they know more about the product or service than consumers know. Information asymmetries can prevent consumers from choosing the products or services that correspond best to their individual preferences. Providing adequate information is also a form of empowering consumers as catalysts of functioning competition, which may explain why the rules on consumer information are integral to EC consumer law.[174] As the European Court of Justice has observed, "[U]nder [European] Community law concerning consumer protection the provision of information to the consumers is considered to be one of the principal requirements."[175]

Both the Distance Selling Directive[176] and the Electronic Commerce Directive[177] include important rules imposing obligations upon suppliers to provide consumers with the necessary information. Both Directives apply to the selling of products *and* services. The Electronic Commerce Directive can be applied to various electronic services, including electronic newspapers, video-on-demand services, and music download stores such as Apple's iTunes, but also to the online sale of books, software, CDs, and DVDs. The Distance Selling Directive also addresses contracts for the purchase of products and services, in particular contracts that are concluded by means of electronic communication (e.g., e-mail, online order, telephone).[178] Failure to comply with duties to inform triggers sanctions under the aforementioned rules on nonconformity as well as the rules on unfair or misleading business practices in Articles 5(3)(a) and 5(1) of the Directive on Unfair Commercial Business Practices.[179] The Distance Selling Directive itself does not provide for any sanctions against sellers other than an extension of the period during which consumers can exercise a right of withdrawal, a right of consumers to cancel the contract within a

173. Reich, *supra* note 118, at 258-59.

174. Barents, *supra* note 112, at 16; Rinkes, *supra* note 107, at 51; Wilhelmsson, *supra* note 122, at 200-01.

175. Case 362/88, GB-INNO v. Confederation du Commerce Luxembourgoise, 1990 E.C.R. I-00667, para. 18.

176. Distance Selling Directive, *supra* note 101, art. 4.

177. Electronic Commerce Directive, *supra* note 101, art. 5.

178. Distance Selling Directive, *supra* note 101, arts. 1, 2(1), 2(4), Annex I.

179. Neither the Distance Selling Directive nor the Electronic Commerce Directive provide for remedies or sanctions where a supplier fails to comply with information duties. Instead, the Directives oblige Member States to ensure the availability of adequate and effective means to demand compliance. *See, e.g., id.*, art. 11(1).

minimum of seven working days without giving any reason and without penalty, except the cost of returning the goods.[180]

Consumers have the unwaivable right to be informed about prices and the main characteristics of the goods or services.[181] "Main characteristics" are those features of a product or service the absence of which would cause the consumer to make a different transactional decision.[182] These "main characteristics" include measurable characteristics that concern functionality or possibilities of usage.[183] At present, little European or national case law in Europe sheds light on whether contractual or DRM restrictions on copying are "main characteristics" of a product or service. As mentioned earlier, a number of surveys have demonstrated that the ability to make private copies appears to be an important factor in the purchasing decisions of consumers.[184] This suggests that suppliers must inform consumers if a product or service does not permit copying or restricts the number of copies allowed.[185] Note that the ability to make copies as a main characteristic of a product or service and the legitimacy thereof are two different things. Arguably, a duty to inform exists irrespective of whether a court might find in an individual case, through application of the three-step test, that the interests of a copyright holder outweigh the in-

180. *Id.*, art. 6(1). Note, however, that the right of withdrawal does not apply to the supply of most information products or services, including audio or video recordings or computer software which have been unsealed by the consumer and the supply of newspapers, periodicals, and magazines. *Id.*, art. 6(3).

181. *Id.*, arts. 4(1)(b), 12(1).

182. Jan Kabel, *Misleiding [Misleading Advertisement]*, *in* PRAKTIJK RECLAMERECHT [ADVERTISEMENT LAW IN PRACTICE], Supp. 45, 226 (Jan Kabel ed. 1989).

183. *Id.* at 258-60.

184. *See supra* Section III.B.1.

185. *See, e.g.*, Cour d'appel [CA] [regional court of appeal] Paris, 4e ch., sec. B, Apr. 22, 2005, Stéphane P. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=1432. Here, the court held that the "copy-ability" of a DVD is an essential characteristic of a DVD. The court also found that labeling the DVD with "CP" ("copie prohibée"—copying prohibited) does not constitute compliance with a supplier's obligation to inform consumers about copy restrictions. Because French consumers know that private copying is permitted under French copyright law, the court found that "CP" could be interpreted to mean something other than "copying prohibited." *See also In re Sony BMG Music Entm't*, No. C-0623019, 2007 FTC LEXIS 10 (FTC Jan. 20, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130cmp0623019.pdf; Rott, *supra* note 147, at 285; Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, 3e ch., 2e sec., Apr. 30, 2004, Stéphane P. (Fr.), *available at* http://www.legalis.net/breves-article.php3?id_article=722 (holding that whether a DVD can be copied is not an essential characteristic of the DVD because the consumer cannot invoke the private copy exception).

terests of a consumer.[186] Otherwise, the consumer would bear the risk of the present legal uncertainty surrounding private copying. Suppliers should be relieved of their duty to inform only where certain acts of copying are obviously beyond the scope of the private copying limitation, even to the untrained layman.

C. Assessment

Consumer law is a logical choice when looking for ways to give legal effect to information consumers' interests in private copying. Private copying in today's information markets has become a matter of contracts and electronic rules between commercial suppliers and information consumers. Unlike copyright law, consumer law targets the commercial relationship between these two parties with the goal to ensure standards of fairness, equality, and transparency.

Unlike in copyright law, consumer law's yardstick for evaluating information markets is not the legitimate commercial expectations of copyright holders but the legitimate usage expectations of consumers. If consumers can reasonably expect to be able to make private copies, consumer law provides the means to challenge contractual terms that seek to override the limitation allowing private copying or the means to redress unexpected copy restrictions in information products. Consumers may also demand to be informed about possible technical impediments to copying, and whether private copies can be made at all. Furthermore, European consumer law provides for specialized procedures and remedies that consumers can use to defend their interests.

In the end, whether a consumer can reasonably expect to make private copies will largely depend on the facts of a given case. Factors that shape reasonable consumer expectations include the characteristics of comparable goods or services and the price of the product or good concerned.[187] Advertisements and consumer information can also influence consumers' expectations.[188] As these factors are subject to change, the standard of consumer expectations is in constant flux. A more stable factor that will surely also influence consumer expectations is the set of copyright provi-

---

186. *But see* Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, 3e ch., 2e sec., Apr. 30, 2004, Stéphane P. (Fr.). Here, the court denied that private copying is an essential characteristic because the making of private copies conflicts with the "normal exploitation" of a DVD. Thus, consumers should not benefit from the private copying exception, and no obligation to inform consumers about copy restrictions applies.

187. *See supra* Sections III.B.1, III.B.2.

188. *See id.*

sions relating to private copying limitations in force in a particular jurisdiction. For now, however, existing copyright law continues to give mixed and confusing signals. Consumers may have difficulty making sense of a law that, on the one hand, provides a limitation allowing private copying but that, on the other hand, accepts that this limitation exists at the will of copyright holders, by way of standard form contracts or DRM. For the private copying limitation to play a meaningful role in consumer law cases, the limitation should be sufficiently clear and conclusive as to inform consumers of what they may expect from information goods or services.

Even if courts find that consumers can reasonably expect to make private copies, deviations from this standard are still possible and legitimate. Respect for the contractual freedom and freedom of choice of both consumers and suppliers remains a core principle of consumer law. A consumer can still decide to download from iTunes copy-restricted songs for 99 Eurocents instead of more expensive, "higher quality" iTunes Plus files for €1.29, which allow the making of an unlimited number of copies. What matters under consumer law is that the consumers' transactional decisions are based on their free will, and that these decisions are not influenced by unfair commercial practices, lack of adequate information, or structural imbalances in negotiation power.[189]

European consumer law relies to a considerable degree on the rules on consumer information to guarantee that consumers engage only in commercial transactions that are advantageous to themselves. The European information paradigm corresponds with the prevalent image of the European consumer, reasonably observant and circumspect as sovereign decision maker and a countervailing power in the market mechanism. Critical here is whether simply informing consumers that they are not entitled to make private copies sufficiently safeguards the balance that consumer law seeks to maintain.

Regarding mandatory information duties as a primary means to safeguard the interests of the information consumer is a matter of concern for a number of reasons. First, to be truly informed, information consumers must have a sound understanding of complex norms, such as the extent and scope of the private copying limitation. Where consumers lack such an understanding, the risk of a creeping sell-out of traditional user freedoms is real. Less scrupulous representatives of the information industry may gradually degrade the general standard of what consumers ought to be able to expect from information services and products. The opposite

189. GIROT, *supra* note 123, at 30-32.

may also be true. Collective consumer power that does not respect basic concepts of copyright law could be the end of many perfectly lawful business models. Second, how much more information can the information consumer take? Information overload can hamper the consumer's abilities as a sovereign decision maker as much as too little information. What information consumers need is not necessarily more information, but more intelligent information—comprehensive information that informs them not only of the product or service itself, but also of its impact on consumers' rights and legitimate interests. Finally, mandatory disclosure laws might act as disincentives for suppliers to produce products that cannot be copied. Through informing consumers in advance, suppliers can avoid liability for nonconformity with consumers' reasonable expectations.

Consumer law may offer meaningful protection of consumers' legitimate interests in the making of private copies by halting the downward spiral of reasonable consumer expectations. One suggestion that merits serious consideration is to add as a category those clauses that depart from the private copying limitation to the Unfair Terms Directive "blacklist" of contractual terms that are presumed unfair.[190] A difficulty with this solution is that it could yield tensions with the short-term interests of consumers.[191] Although invalidating contractual clauses that prohibit private copying would certainly do much to rescue the consumer's freedom to make private copies, it could also undermine new, potentially attractive business models, such as iTunes, or deter the industry from making content available online at all. In the end, an absolute ban on contractual clauses that prohibit private copying would result in less choice for consumers. Other possible alternatives include more sophisticated, intelligent solutions to inform consumers, for example in the form of a "fair use" label. A fair use label could incorporate standards that are elaborated in cooperation between representatives from both consumers and the industry. Arguably, the market parties themselves are best situated to determine how many copies might still be considered a fair amount of private use. One source of inspiration could be the "Webtrader" labeling initiative, which is an initiative led by a number of European consumer organizations to develop a trust scheme for electronic commerce services.[192] Busi-

190. *Cf.* GUIBAULT, *supra* note 13, at 304.

191. Interestingly, on this topic, Wilhelmsson discusses eventual contradictions of public environmental policy and short term goals of consumer law. Thomas Wilhelmsson, *Consumer Law and the Environment: From Consumer to Citizen*, 21 J. CONSUMER POL. 45, 61 (1998).

192. *See, e.g.*, WebTraderUK, About the WebTraderUK Scheme, http://www.webtraderuk.org.uk/content/Default.asp (last visited Aug. 8, 2007).

nesses can apply for online certification and the grant of a "Webtrader" label, provided they comply with the Webtrader code of conduct. This code of conduct addresses specific problems of consumers in an electronic commerce setting and is updated whenever new legal or market developments require.[193]

IV. CONCLUSION

Both European copyright law and consumer law offer some comfort to information consumers keen on making private copies, even against overreaching "end user" license terms or oppressive technical protection measures. Private copying exemptions are permitted, but not required, by the Information Society Directive, and currently exist in most Member States. Despite the Directive's silence on the issue of "overridability," a few Member States have given limitations allowing private copying imperative status. Other Member States have benefited from the option left to them by the Directive to make these limitations enforceable against DRMs. In all, the law of private copying in Europe remains as diverse as its cultural traditions. If this is harmonization, then it might be time to call the process over.[194]

Nevertheless, effectively protecting the freedom to make private copies remains problematic in the context of European copyright law. The copyright model of a set of rights against the world sits uncomfortably with the norms of contract law that form the essence of consumer protection law. User's *rights*, such as those found in early European Directives, fit uneasily in the copyright system. For this reason, user's rights have remained exceptional and are not addressed in the more recent Information Society Directive. Except for the limited recourse Article 6(4) may give against the "Übercopyright" norms of DRM, the Information Society Directive leaves consumers at the mercy of copyright holders and distributors unilaterally imposing standard license terms.

But even a copyright system that does consider certain consumer interests will always fall short of fulfilling the real needs of information consumers. In Europe, copyright is chiefly designed as a property right, as are its structure and its discourse. Exclusive rights are the rule, while free-

193. *See* European Commission, WEBTRADER trust scheme for B2C e-commerce, supported by the Enterprise DG—main results of the pilot operation, http://ec.europa.eu/enterprise/ict/policy/webtrader.htm (last visited Aug. 8, 2007).

194. P.B. HUGENHOLTZ ET AL., THE RECASTING OF COPYRIGHT & RELATED RIGHTS FOR THE KNOWLEDGE ECONOMY, REPORT TO THE EUROPEAN COMMISSION (2006), *available at* http:// www.ivir.nl/publications/other/IViR_Recast_Final_Report_2006.pdf.

doms are framed as "exceptions" that must be narrowly construed, especially in the author's rights tradition. Due to copyright law's systemic pro-right-holder bias, as reflected in the property model, achieving a proper balance between protecting the interests of copyright holders and the interests of users will always be an uphill struggle for consumer groups. To borrow a phrase from European football, the lingua franca of European culture, consumers will always be playing an "away game" in the copyright arena.

The norms of European consumer law are more conducive to the interests of information consumers in making private copies, at least in principle. However, existing consumer law also has its weaknesses. Although consumer law norms generally apply to the supply of goods and services, they have not been designed with consumers of digital content in mind. Even if consumers may successfully claim a right to make private copies under a variety of consumer protection doctrines, the lack of legal certainty that the existing copyright framework has to offer is mirrored in the framework of consumer law. Particularly troublesome is the test of "reasonable consumer expectations." This notion is informed by a variety of dynamic exogenous factors, including the state of the law of copyright and evolving business practices, which makes the test a moving target. What may be a consumer's reasonable expectation to make a private copy one day in Member State A may be wishful thinking in Member State B another day.

Harmonization of Member States' law and creating a uniform, predictable legal interface between the norms of European copyright law and consumer law would create greater legal certainty in the realm of private copying. A recent study by the Institute for Information Law suggested that one way to achieve this would be to make private copying a mandatory exemption that all Member States must implement and to immunize the exemption against unilaterally set standard terms, for example, by including it in the blacklist of the Unfair Terms Directive.[195] In the meantime, more research is needed that addresses possible means and procedures for consumers and suppliers to reach consensus on a common standard establishing the extent of private copying that consumers can reasonably expect from products and services that incorporate copyrighted works.

Finally, although this Article has examined the issue of private copying from the perspective of a traditional, self-centered, essentially passive consumer, the consumption of information services and products takes

195. GUIBAULT, *supra* note 13, at 169.

place in a broader cultural and social context. In information markets, consumers often act in the combined roles of consumer *and* citizen. To examine this relationship, a query of the potential of consumer law to realize wider public policy aims in relation to information markets would be enlightening. Such a query should examine consumer law's ability to address the goals of distributive justice as a way to ensure consumers' equal access to a diversity of cultural products and services, as suggested in the Charter for Consumer Sovereignty in the Digital World.[196] Such a political—or perhaps even constitutional—conception of consumer law already exists, for instance, in European telecommunications law, which combines traditional consumer protection with the realization of information policy objectives, notably the broad availability of communications services.

196. BMELV Consumer Protection, *supra* note 127.

ENABLING COPYRIGHT CONSUMERS

By Joseph P. Liu[†]

TABLE OF CONTENTS

I. **INTRODUCTION** 1099

II. **WHOSE SHOES?** 1101

A. PHOTOCOPYING OF COURSEPACKS 1102
B. SPACE-SHIFTING AND TIME-SHIFTING 1105
C. BOWDLERIZATION OF DVDS 1107

III. **TRYING THEM ON FOR SIZE** 1109

A. CRITIQUE AND MODIFICATIONS 1110
B. SOME EXAMPLES 1112

IV. **HOW DO I LOOK?** 1114

A. IMPLICATIONS FOR CASE LAW 1114
B. IMPLICATIONS FOR THE DMCA AND DRM 1116

V. **CONCLUSION** 1118

I. INTRODUCTION

When is it acceptable for a company to help consumers engage in fair use of copyrighted works? One might think that the answer would be: "always." After all, a fair use is a privileged use, which copyright grants to consumers of copyrighted works.[1] Consumers have the right, for example, to make personal copies of their CDs. If that is the case, then shouldn't a company be entitled to help consumers make copies of CDs? Similarly, consumers have the right to make copies of television broadcasts for later viewing.[2] Shouldn't a company be entitled to help consumers do this in the most efficient way possible? Shouldn't such a company, in fact, be lauded for making this process more efficient?

In fact, courts quite frequently hold companies liable for helping consumers engage in activities that would be fair or non-infringing uses if un-

---

† Associate Professor, Boston College Law School.

1. *See* 17 U.S.C. § 107 (2000).
2. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

dertaken by consumers themselves. For example, courts have suggested that students should be entitled to make and assemble, on their own, copies of excerpts from various books and articles.[3] But when a copy shop performs this task, the courts have held this to be infringing.[4] Similarly, consumers are generally understood to have the right to skip over the portions of a DVD they find objectionable or do not wish to see.[5] This would likely extend to the right to make edits to the DVD for such a clearly personal and non-commercial purpose. But when a company facilitates this activity by selling already edited versions of the DVD, the courts have found this to be infringing.[6] Most recently, a court held liable a cable company that stored broadcasts for later viewing on behalf of consumers,[7] despite the fact that such an activity would be fair use if a consumer did it in the privacy of his or her own home.

What explains the courts' dim view of companies that help consumers engage in fair or privileged uses? The structure of copyright doctrine provides an immediate explanation. In deciding such cases, courts generally apply the fair use defense to the activities of the companies, not the ultimate consumers. So in the copy shop cases, for example, the courts find that the nature of the use is commercial, since the copy shop profits from the copying.[8] The courts also frequently find that there is harm to the relevant market, since in many cases these companies could have secured a license from the copyright owner.[9] The fact that the use might have been fair if performed by a consumer is irrelevant.

In many ways, the doctrinal explanation makes good policy sense. Many consumer uses are considered fair because they pose little harm to the market for the copyrighted work.[10] The uses are, at least individually, small in scale. Moreover, the value of the uses is trivial in comparison to

---

3. *See* Princeton Univ. Press v. Mich. Document Servs. (MDS), 99 F.3d 1381, 1395 (6th Cir. 1996) (en banc) (Merritt, J., dissenting).

4. *See id.*

5. *Family Movie Act of 2004: Hearing on H.R. 4586 Before the H. Comm. on the Judiciary*, 108th Cong. 22 (2004) [hereinafter *Hearing*] (statement of Marybeth Peters, Register of Copyrights, Copyright Office of the U.S.).

6. Clean Flicks of Colo., LLC v. Soderbergh, 433 F. Supp. 2d 1236 (D. Colo. 2006).

7. Twentieth Century Fox Film Corp. v. Cablevision Systems Corp., 478 F. Supp. 2d 607 (S.D.N.Y. 2007).

8. *See* Princeton Univ. Press v. Mich. Document Servs. (MDS), 99 F.3d 1381 (6th Cir. 1996); Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522 (S.D.N.Y. 1991).

9. *See, e.g.*, *MDS*, 99 F.3d at 1387.

10. *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 451-52 (1984).

the costs that would be entailed if consumers were forced to seek authorization for these uses.[11] Under the familiar market-failure theory of fair use, copyright law should permit these uses.[12] When third parties enter the picture, however, they make it far easier for consumers to engage in such uses. This potentially increases the amount of harm to the market for the work. It also reduces the potential licensing costs. Thus, copyright theory might well support such a result.[13]

Although this perspective is in many ways quite valid, I argue in this Article that it is only partially correct. Specifically, the current judicial approach to such cases fails to take sufficient account of the interest that consumers have in engaging in fair or privileged uses. By conceiving of such uses as based largely on market failure, the existing approach finds it easy to allocate the benefits of efficiency to producers. However, if we view consumer uses as affirmative privileges that are based on more than simply market failure, then it becomes less clear why the benefits of efficiency should not be enjoyed, at least in part, by consumers and by the companies that serve them.

In this Article, I suggest a number of ways in which a more consumer-oriented perspective might affect the way courts approach this question. Part II of this Article examines three specific areas in which courts have found companies liable for engaging in activities that would be fair uses if performed by consumers themselves. Part III analyzes the approach adopted by these courts and identifies situations where consumer fair use has a claim to be viewed as an affirmative entitlement. Finally, Part IV argues in favor of a more nuanced application of the fair use factors in such situations and explores some of the implications of the analysis for judicial decision making, as well as statutory initiatives such as the Digital Millennium Copyright Act.

II. WHOSE SHOES?

Courts in copyright cases have generally been reluctant to allow companies to "stand in the shoes" of their customers when it comes to fair

11. *See* Wendy J. Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the* Betamax *Case and its Predecessors*, 82 COLUM. L. REV. 1600 (1982).

12. *See id.*

13. *See, e.g.*, Robert P. Merges, *The End of Friction? Property Rights and Contract in the Newtonian World of On-line Commerce*, 12 BERKELEY TECH. L.J. 115 (1997).

use.[14] This Part describes a number of areas where courts have either rejected or failed to consider such arguments.

A. Photocopying of Coursepacks

Perhaps the most express consideration of the issue raised by this Article can be found in the copy-shop cases: *Princeton University Press v. Michigan Document Services (MDS)*[15] and *Basic Books, Inc. v. Kinko's Graphics Corp.*[16] In *MDS*, the plaintiff, Princeton University Press, sued a photocopy store that produced coursepacks for university professors. The coursepacks consisted of photocopied collections of excerpts from copyrighted books and articles chosen by the professor as readings for a particular course. The professors assembled the coursepacks, the copy shop reproduced the coursepacks, and students in the class purchased the coursepacks from the copy shops. The copy shop in *MDS* did not pay any licensing fees for the right to reproduce the copyrighted books and articles, and the plaintiff sued for copyright infringement.[17]

The court of appeals in *MDS*, sitting en banc, rejected the defendant's assertion of fair use. Applying the four fair use factors, the court held that (1) the nature and purpose of the use was both commercial and nontransformative; (2) the amount of the copyrighted work used was substantial; (3) the nature of the copyrighted works was creative and entitled to protection; and (4) the impact on the market was significant, insofar as the activity deprived the publisher of licensing fees that it was successful in obtaining from other copy shops.[18] In reaching this result, the court analyzed the fair use defense from the perspective of the copy shop.

MDS had argued that the court should adopt, or at least take into account, the perspective of the students. From such a perspective, the fair use status of the practice looks quite different. The practice, noncommercial in nature and educational in purpose, is of precisely the type that fair use was originally designed to enable. Moreover, the impact on the market is not significant, insofar as students would not otherwise purchase all of the original copyrighted works. MDS argued that it was

14. *See* Llewellyn Joseph Gibbons, *Entrepreneurial Copyright Fair Use: Let the Independent Contractor Stand in the Shoes of the User*, 57 ARK. L. REV. 539 (2004).

15. 99 F.3d 1381 (6th Cir. 1996).

16. 758 F. Supp. 1522 (S.D.N.Y. 1991). The facts of *Basic Books* are very similar to the facts of *MDS*. Accordingly, this Article will focus its discussion on the latter, without repeating the analysis for the former.

17. *MDS*, 99 F.3d at 1384.

18. *Id.* at 1386-90.

merely facilitating the fair use of the students, and that the court should take this into account in its fair use calculus.[19]

One of the dissenting opinions noted the incongruity that the actions might well have been fair use if undertaken by the students themselves:

> That the majority lends significance to the identity of the person operating the photocopier is a profound indication that its approach is misguided. Given the focus of the Copyright Act, the only practical difference between this case and that of a student making his or her own copies is that commercial photocopying is faster and more cost-effective. Censuring incidental private sector profit reflects little of the essence of copyright law.[20]

Another dissenting opinion was even more express:

> There is nothing in the statute that distinguishes between copies made for students by a third person who charges a fee for their labor and copies made by students themselves who pay a fee only for use of the copy machine. Our political economy generally encourages the division and specialization of labor. There is no reason why in this instance the law should discourage high schools, colleges, students and professors from hiring the labor of others to make their copies any more than there is a reason to discourage lawyers from hiring paralegals to make copies for clients and courts. The Court's distinction in this case based on the division of labor—who does the copying—is short sighted and unsound economically.
>
> Our Court cites no authority for the proposition that the intervention of the copyshop changes the outcome of the case. The Court errs by focusing on the "use" of the materials made by the copyshop in making the copies rather than upon the real user of the materials—the students. Neither the District Court nor our Court provides a rationale as to why the copyshops cannot "stand in the shoes" of their customers in making copies for noncommercial, educational purposes where the copying would be fair use if undertaken by the professor or the student personally.[21]

Thus, to the dissenting judges, MDS was merely making more efficient the fair use that the students were otherwise entitled to engage in.

The majority, however, rejected this argument:

---

19. *Id.* at 1389.
20. *Id.* at 1393 (Martin, C.J., dissenting).
21. *Id.* at 1395 (Merritt, J., dissenting).

> Two of the dissents suggest that a copyshop merely stands in the shoes of its customers and makes no "use" of copyrighted materials that differs materially from the use to which the copies are put by the ultimate consumer. But subject to the fair use exception, 17 U.S.C. § 106 gives the copyright owner the "exclusive" right "to reproduce the copyrighted work in copies . . . ." And if the fairness of making copies depends on what the ultimate consumer does with the copies, it is hard to see how the manufacture of pirated editions of any copyrighted work of scholarship could ever be an unfair use.[22]

Thus, the court refused to consider or take into account the possibility that the students' activities might constitute fair use.[23]

While there may well be valid arguments against the position advanced by the dissenting opinions, the majority's response seems somewhat weak. The majority seems to be concerned that allowing the copy shop to stand in the shoes of the students would provide no limiting principle, i.e., that it would mean that copy shops could make wholesale copies of entire books. But this is not the case—the limiting principle would be the fair use rights of the students. Making a wholesale copy of an entire book would likely be infringing even if done by a student.[24] Thus there is no real concern that allowing the copy shop to stand in the shoes of students would lead to unlimited copying. Rather, the extent of the copy shop's right would be measured by, and be coextensive with, the rights of the students.

In a later portion of the opinion, the majority raised a more interesting objection. As noted above, the dissenting opinions argued that the copy shops were merely doing what the students were doing, but in a more efficient manner, and that it would be incongruous to penalize them for making the process more efficient. The majority responded by noting that other copy shops were able to serve this function while at the same time paying royalties to the publishers.[25]

Unlike the earlier response, this response hits closer to the mark. Here, the court seemed to implicitly acknowledge that there was value in ena-

---

22. *Id.* at 1386 n.2.

23. Note that the court expressed no opinion about whether copying by the students would have been fair: "As to the proposition that it would be fair use for the students or professors to make their own copies, the issue is by no means free from doubt." *Id.* at 1389.

24. In such a case, the fair use factors would point largely against the student, particularly if the book were available for purchase.

25. *Id.* at 1389.

bling students to access coursepacks in a more efficient manner. However, it took issue with the argument that achieving this result required a fair use defense for the copy shops. Thus, for the majority, the question was not whether students could access coursepacks in an efficient manner, but whether the publishers would be compensated.

Thus, in the end, the court expressly rejected the argument that the copy shop could stand in the shoes of the students.[26]

B. Space-Shifting and Time-Shifting

The same issue arises in cases involving space-shifting and time-shifting. Consumers have a relatively well-established right to record television broadcasts for later viewing, so-called time-shifting. They have also enjoyed, at least historically, the right to make personal copies of recorded music, so-called space-shifting. Both of these activities are generally considered fair use.[27]

Yet in a number of cases, courts have imposed liability on companies that have sought to facilitate and make more efficient the consumer exercise of these rights. In *UMG Recordings v. MP3.com*,[28] for example, the defendant MP3.com provided a service whereby consumers could store, on MP3.com's servers, music they had purchased on CDs. Consumers would place their CDs in the CD drive of their computer and then upload the music onto MP3.com's servers. Consumers could then access the music from any computer with an internet connection by signing onto the MP3.com site.[29]

In fact, however, MP3.com did not copy the music from the consumer's CD. Instead, MP3.com had already made copies of many music album CDs, such as those produced by UMG, and stored these copies on

---

26. *Accord* Zomba Enters., Inc. v. Panorama Records, Inc., 491 F.3d 574, 582 (6th Cir. 2007) (citing *MDS*, 99 F.3d 1381) (establishing the proposition that "the end-user's utilization of the product is largely irrelevant; instead, the focus is on whether alleged infringer's use is transformative and/or commercial"); Video Pipeline, Inc., v. Buena Vista Home Entm't, Inc., 192 F. Supp. 2d 321, 333-34 (D.N.J. 2002) (citing *MDS*, 99 F.3d at 1389) (noting that company cannot stand in the shoes of customer for purposes of the first sale doctrine). *See generally* Ann Bartow, *The Hegemony of the Copyright Treatise*, 73 U. CIN. L. REV. 581, 635-36 (2004) (tracing the source of the proposition that companies cannot stand in the shoes of their customers).

27. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984); Transcript of Oral Argument at 12, Metro Goldwyn Mayer Studios, Inc. v. Grokster, Inc., 545 U.S. 913 (2005) (No. 04-480); Audio Home Recording Act of 1992, 17 U.S.C. §§ 1001-10 (2000).

28. 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

29. *Id.* at 350.

its servers. Whenever a consumer placed such a CD in his or her CD drive, MP3.com would verify that the CD contained the stored music. Then, rather than uploading the music onto its servers from the consumer's CD, MP3.com would instead provide the consumer with access to the copies of the songs from the CD that already resided on MP3.com's servers. Alternatively, if the consumer did not have a particular CD, he or she could purchase the CD from a cooperating online retailer. MP3.com would then provide access to its online copy.[30]

UMG sued for copyright infringement, and the district court found MP3.com liable. In so doing, the court rejected MP3.com's fair use argument. In evaluating the fair use factors, the court found that the use was commercial and non-transformative, that MP3.com copied the entire work, and that the nature of the work was creative.[31] MP3.com had argued that its service did not harm the direct market for CDs and even had the effect of enhancing the market, insofar as it required the purchase of the CD. The court rejected this argument, noting: "Any allegedly positive impact of defendant's activities on plaintiffs' prior market in no way frees defendant to usurp a further market that directly derives from reproduction of the plaintiffs' copyrighted works."[32] In a separate opinion, the court awarded massive statutory damages to the plaintiffs.[33]

The court in *MP3.com* never directly addressed the argument that MP3.com was merely facilitating the exercise of a consumer's right. Either MP3.com never made that argument or the court rejected it and applied the fair use factors without acknowledging any consumer interest. The court did note in passing, however, that: "Copyright . . . is not designed to afford consumer protection or convenience but, rather, to protect the copyrightholders' property interests."[34]

Although in a slightly different doctrinal setting, a recent case presents a similar issue in the context of time-shifting television broadcasts. In *Twentieth Century Fox Corp. v. Cablevision Services*,[35] the cable company Cablevision introduced a service that allowed customers to record cable television broadcasts for later viewing. The service functioned like a personal video recorder such as TiVo. However, instead of recording the shows on a set-top box in the customer's home, the service stored the recordings centrally at Cablevision's facilities. Cablevision's computers al-

30. *Id.*
31. *Id.* at 351-53.
32. *Id.* at 352.
33. UMG Recordings, Inc., v. MP3.com, Inc., 2000 WL 1262568 (S.D.N.Y. 2000).
34. *UMG Recordings*, 92 F. Supp. 2d at 352.
35. 478 F. Supp. 2d 607 (S.D.N.Y. 2007).

located space to each consumer and stored shows on that space in response to the customer's choices about which shows to record.[36]

The case thus presented many of the same issues raised in the *MP3.com* case, insofar as the activity would likely have been fair use if performed by the customer in his or her own home. However, in *Cablevision*, the court never addressed the fair use issue because Cablevision had waived its fair use defense in exchange for plaintiff's waiver of a potential contributory liability claim. Instead, Cablevision argued that it was only passively enabling copying by consumers, and thus the consumers were the ones actually engaging in the act of copying.[37]

The court rejected Cablevision's argument, finding that Cablevision did more than passively facilitate copying by consumers. It pointed to the fact that Cablevision had extensive control over the means of copying and made decisions regarding when and how the copying would take place.[38] The court also distinguished Cablevision's service from a consumer's use of a personal video recorder, focusing largely on the technical differences between the two. It found that Cablevision's system more closely resembled a video-on-demand system, for which Cablevision paid royalties to the copyright owners.[39]

Thus, in the end, the court refused to permit Cablevision to step into the shoes of its customers.[40] The court's analysis focused almost exclusively on the actions of Cablevision itself and, in particular, on the technical details of Cablevision's service. It did not consider the possibility that Cablevision's service might represent a more efficient way for consumers to time-shift than through the use of set-top boxes.

C. Bowdlerization of DVDs

Another example of the same phenomenon appears in the debate over bowdlerized versions of movies on DVD. In recent years, a number of companies have begun offering to the public versions of movies on DVD that have been edited to remove or mask scenes that might be objection-

36. *Id.* at 612-16.

37. *Id.* at 617.

38. *Id.* at 618.

39. *Id.* at 618-19.

40. *Accord* Atl. Recording Corp. v. XM Satellite Radio, Inc., 2007 WL 136186, at *7 (S.D.N.Y. 2007) (refusing, under the Audio Home Recording Act, to allow a distributor of an XM receiver plus recording MP3 player to step into the shoes of consumers who would otherwise be authorized to make recordings of broadcasts); Pac. & S. Co. v. Duncan, 572 F. Supp. 1186, 1194-95 (N.D. Ga. 1983), *rev'd on other grounds*, 744 F.2d 1490 (11th Cir. 1984) (refusing to let operator of a TV news clipping service to stand in the shoes of its customers for fair use purposes).

able to certain segments of the public. A consumer mails a DVD to one of these companies. The company edits the movie to remove or mask objectionable content (nudity, language, violence, etc.), and then sends back a disk containing the modified movie. The companies are generally careful to maintain a one-to-one ratio between purchased DVDs and edited copies.[41]

A number of movie studios sued several such companies for copyright infringement. The district court rejected the companies' fair use defense.[42] The court found the use to be commercial and rejected the argument that the edited versions of the copyrighted works were transformative.[43] The court also held that the works were creative and that the companies had copied the entire works.[44] Finally, the court rejected the argument that the use had no negative impact on the market. The defendants had argued that their use actually increased the market for such works, insofar as they required consumers to first purchase the unedited DVDs. Thus, many consumers would not have purchased the DVDs but for the editing service. The court responded by noting that, even if this were the case, copyright owners should in any event have the right to decide whether or not they wished to enter this market.[45]

Here too, the court never directly addressed the interests of the consumers.[46] Consumers presumably have the right to skip over or mute portions of DVDs that they do not wish to see or hear.[47] Consumers would

---

41. *See* Clean Flicks of Colo., LLC, v. Soderbergh, 433 F. Supp. 2d 1236, 1238-39 (D. Colo. 2006).

42. *Id.* at 1242.

43. *Id.* at 1241.

44. *Id.* at 1241-42.

45. *See id.* at 1242. The court stated:

> The argument has superficial appeal but it ignores the intrinsic value of the right to control the content of the copyrighted work which is the essence of the law of copyright. Whether these films should be edited in a manner that would make them acceptable to more of the public playing them on DVD in a home environment is more than merely a matter of marketing; it is a question of what audience the copyright owner wants to reach.

Id.

46. The closest the court came was in rejecting statements from customers submitted by the companies, touting the value of the services rendered. The court held that this interest was "inconsequential to copyright law and is addressed in the wrong forum." *Id.* at 1240.

47. *Hearing, supra* note 5, at 22. Marybeth Peters, the Register of Copyrights, testified:

> Let me start with a proposition that I believe everybody can agree on. I do not believe anybody would seriously argue that an individual who is

also likely have a fair use right to modify DVDs they purchased in order to edit out objectionable portions.[48] Thus, in a sense, the providers of bowdlerization services merely enable consumers to access works in a way that they would be entitled to under fair use. Indeed, the services would appear to be essential to the widespread exercise of these consumer rights, insofar as most consumers would not have the technical ability to make the required modifications.

Unlike the courts, Congress expressly addressed the consumer interest in this area by passing the Family Movie Act of 2005.[49] The Act allows companies to provide consumers with hardware and software that would permit consumers to mask or delete objectionable scenes in movies. Under the Act, companies can sell specially designed DVD players and provide files that the DVD player can use to alter or remove scenes from movies "on the fly," that is, while the movie is being played and without making a permanent altered copy.[50] The Family Movie Act thus represents an interesting example of Congress expressly recognizing this consumer interest, albeit in a limited manner, and enacting a specific privilege furthering it.

III. TRYING THEM ON FOR SIZE

There may be good reasons for the courts in the cases presented above to prevent companies from stepping completely into the shoes of their customers. The involvement of these companies may adversely affect the policies underlying copyright, such as the incentive to create expressive works. At the same time, courts have been too quick to dismiss the interests of consumers in these cases. Section A analyzes and critiques the cases presented above and suggests modifications that would take greater account of consumer interests in fair use. Section B then discusses some situations in which these modifications might be particularly appropriate.

> watching a movie in his or her living room should be forbidden to press the mute button on a remote control in order to block out language that he or she believes is offensive. Nor should someone be forbidden to fast-forward past a scene that he or she does not wish to see. And certainly parents have the right to press the mute and fast-forward buttons to avoid exposing their children to material that they believe is inappropriate.

Id.

48. *But see infra* Section IV.B (discussing effect of the Digital Millennium Copyright Act).

49. Pub. L. No. 109-9, 119 Stat. 218, 223-24 (2005) (amending 17 U.S.C. § 110).

50. *Cf.* Lewis Galoob Toys, Inc., v. Nintendo of Am., Inc., 964 F.2d 965 (9th Cir. 1992) (finding no infringement for device that altered gameplay "on the fly").

A. Critique and Modifications

As a doctrinal matter, it is hard to fault the approach adopted by the courts above. In many of the examples above, a company defended itself against claims of copyright infringement by asserting a fair use defense. When analyzing the entitlement to fair use in these situations, it makes sense to prefer the perspective of the defendant company itself to the perspective of the ultimate consumer. After all, the company, not the consumer, is the party charged with infringement. And nothing in the statutory fair use provision expressly directs a court to consider the interests of third parties such as the consumer.[51]

The fair use defense, however, does not rule out consideration of the interests of third parties, such as the consumer in the above cases. The statutory factors are not expressly limited to actions taken by the defendant.[52] Moreover, fair use is ultimately a very flexible doctrine, and courts are given much discretion in applying it to specific cases.[53]

The question, therefore, is whether copyright policy warrants consideration of third-party interests. From a policy perspective, there may be good reasons not to permit companies to step fully into the shoes of their consumers when raising a fair use defense. Many fair uses are small-scale uses that have little impact, at least individually, on broader copyright incentives. Moreover, the cost of licensing such individual uses may greatly exceed the value of such uses. Thus, permitting small-scale uses may permit greater dissemination of copyrighted works without a corresponding reduction in copyright incentives.[54]

When companies step in to facilitate such uses, however, both sides of this equation change. The defendant companies above make it far more efficient for consumers to engage in the uses in question. Given the reduced cost of the activity to the consumer, this might have the effect of increasing the extent to which consumers engage in such uses. A more widespread practice might pose a greater threat to the direct market for the copyrighted work. Thus, ultimately there may be a greater adverse impact, in the aggregate, on copyright incentives. So, for example, if students had to assemble their own coursepacks, we might expect the inconvenience associated with the practice to limit the extent to which it is adopted. On

---

51. 17 U.S.C. § 107 (2000).

52. *Id.*

53. H.R. REP. NO. 94-1476, at 9-10 (1976) ("Beyond a very broad statutory explanation of what fair use is and some of the criteria applicable to it, the courts must be free to adapt the doctrine to particular situations on a case-by-case basis.").

54. *See* Gordon, *supra* note 11, at 1618.

the other hand, if the copy shops streamline the process, we might expect greater student adoption of this process and, correspondingly, a greater reduction in sales of the underlying books and articles.

In addition, the participation of the company may reduce potential licensing costs. The company acts as a locus for licensing. It has greater resources than the individual consumers and derives a profit from the activity. It can thus afford to seek out the copyright owners and negotiate licenses for the activity. So, for example, a copy shop will find it far easier to negotiate blanket copying licenses than the individual students or professors. Hence, for fair use purposes, there may be good reasons to treat companies differently than the consumers they serve.

Note, however, that this perspective depends on a certain view of consumer fair use. Under this view, fair use by consumers is a very tenuous entitlement. It is justified solely by the fact that there is no efficient way to make the consumers pay for the use. If there were a way to eliminate the inefficiency, then under this view the use would be foreclosed. In the above examples, once a company steps in to eliminate the inefficiency, the entitlement is automatically re-allocated to the copyright owner. Consumer fair use is thus, in many ways, a residual and very contingent entitlement.[55]

If we adopt a different view of consumer fair use, however, the results in the above cases make far less sense. Suppose we viewed consumer fair use as an affirmative entitlement—less like an immunity from liability, and more like an affirmative right. For example, what if we thought that it was an affirmatively good thing for students to be able to assemble their own customized packages of readings from copyrighted articles and books? Or what if we believed that it was an affirmatively good thing for purchasers of DVDs to be able to edit their purchases for personal consumption in ways that they saw fit?

The activities of the companies look very different in this light. Instead of engaging in widespread infringement or free-riding off of the labor of the copyright owners, the companies serve the valuable function of enabling consumers to exercise their rights. They step in to eliminate an inefficiency in the marketplace. Moreover, the profit that they earn from this activity is what motivates them to seek out and address these market inefficiencies. It is both their reward and their incentive.[56]

---

55. *See* Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998).

56. *See* Princeton Univ. Press v. Mich. Document Servs., 99 F.3d 1381, 1393-94 (6th Cir. 1996) (Martin, C.J., dissenting).

Such a perspective addresses one of the somewhat odd results of the existing approach. Under the existing approach, fair use depends on the existence of inefficiency. It is justified by the inefficiency. Thus, once a company steps in to eliminate that inefficiency, the use is no longer fair. This gives rise to some perverse incentives on the part of these companies to maintain some level of inefficiency in their dealings. Thus, in the example of the cable company and the personal video recorder, the doctrine gives the company incentives to maintain a more inefficient method of recording.[57] It is somewhat odd that the doctrine punishes attempts to make a process more efficient for consumers. If we adopt a more consumer-oriented view, however, this tension is resolved, as the cable company is viewed as providing a valuable service to consumers.

B. Some Examples

Of course, this all raises the question: is there a basis for viewing consumer fair use as an affirmative entitlement rather than an entitlement triggered solely by market failure? Here, I think, is where the existing approach falls short in failing to consider that, in some cases, the answer to this question may be yes. That is, there may be reasons in some cases to view the fair use engaged in by consumers as more than merely a residual right that grudgingly exists only when the market has not found a way to make consumers pay.

In some cases, we might view the consumer fair use as an affirmative entitlement because it serves certain non-market values that justify and underlie fair use more generally.[58] Take, for example, the copy shop cases.[59] Unlike the majority opinion, the dissenting opinions view the consumer use as an affirmative entitlement or good. The ultimate users of the coursepacks, the students, are using them for educational purposes. This is a good thing, a broad purpose that fair use is designed to promote.[60] Under this view, then, the copy shops are facilitating this beneficial use by the ultimate consumers. They are enabling the consumers to efficiently exercise their affirmative entitlements.

Under this view, it seems particularly odd to automatically allocate the benefits of this efficiency to the copyright owners. This is what underlies

---

57. *See* Ed Felten, *Cablevision and Anti-Efficiency Policy*, FREEDOM TO TINKER, Apr. 18, 2007, http://www.freedom-to-tinker.com/?p=1144.

58. *See, e.g.*, Lydia Pallas Loren, *Redefining the Market Failure Approach to Fair Use in an Era of Copyright Permission Systems*, 5 J. INTELL. PROP. L. 1 (1997).

59. *See supra*, Section II.A.

60. 17 U.S.C. § 107 (2000) ("[F]or purposes such as criticism, comment, news reporting, teaching, scholarship, or research . . . .").

the difference between the majority and dissenting opinions. The dissenting opinions repeatedly focus on the fact that the copy shops are merely helping the students engage in an ultimately desirable activity. The majority opinion, by contrast, views the student activities more skeptically and accordingly treats the copy shops far less favorably.

In other cases, we might view the consumer fair use from the perspective of consumer autonomy in the consumption of copyrighted works.[61] So, for example, in the bowdlerization cases, there seems to be a persistent belief that consumers should have a basic right to control how and when they view movies on DVDs. The Register of Copyrights testified to this effect,[62] and Congress recognized this in the passage of the Family Movie Act of 1995. If this is the case, then it becomes harder to understand why companies should be prevented from helping consumers exercise this affirmative entitlement. After all, under this view, the companies that provide consumers with edited DVDs are simply enabling consumers to effectively exercise rights that we wish them to have.

Yet another consumer interest might be an interest in being able to manipulate and transform digital works. As many have recognized, consumers have an interest in interacting with copyrighted works in more complex ways.[63] Because this interest is greatly facilitated by digital technology,[64] consumers are able to engage in an unprecedented level of creativity. This results in a broader and richer cultural environment, one with often quirky and unexpected results. If we consider this to be an affirmative good, then companies that facilitate this kind of creativity should be viewed more favorably. At the very least, they should have the opportunity to argue that they are facilitating the exercise of valuable consumer rights.

In this light, take the example of YouTube.[65] Many of the video clips posted by users of YouTube contain copyrighted materials. Some of these materials are merely copies of commercially produced copyrighted works. Others, however, include some degree of additional creative expression. For example, there are many clips in which copyrighted music serves as a backdrop to lip-synching, dancing, or other activities. Such YouTube users

---

61. *See* Joseph P. Liu, *Copyright Law's Theory of the Consumer*, 44 B.C. L. REV. 397 (2003); Julie Cohen, *The Place of the User in Copyright Law*, 74 FORDHAM L. REV. 347 (2005).

62. *Hearing, supra* note 5, at 22 (testimony of Marybeth Peters).

63. *See, e.g.*, Liu, *supra* note 61.

64. *See generally* LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004).

65. *See* YouTube, http://www.youtube.com (last visited August 26, 2007).

can likely assert the defense of fair use, as their use is non-commercial and transformative, and no easily accessible licensing markets for these uses exist. However, YouTube makes the creation and dissemination of this material far more efficient. YouTube could also potentially negotiate some kind of blanket license on behalf of its users. Yet before concluding that YouTube should be required to do so, YouTube should be entitled to argue that it is facilitating the fair use rights of its users.

Now, to say that courts should take the consumer perspective more seriously is not to say that the consumer perspective should always triumph. It may be that, in some cases, the facilitation of fair use by such companies has too great of an adverse impact on copyright incentives. The benefits of recognizing and facilitating consumer fair uses must be weighed against such a potential effect. But as a general matter, the analysis above suggests that courts should at least consider the possibility that the consumer fair use at issue may be an affirmative entitlement and that companies may have a legitimate interest in making the exercise of such an entitlement more efficient.

IV. HOW DO I LOOK?

So how might copyright look in these cases if courts took more seriously the consumer interest? This Part explores and attempts to flesh out the implications of the above analysis for fair use case law and recent copyright legislation.

A. Implications for Case Law

The adoption of a more consumer-conscious perspective on these cases would have several effects on how courts apply fair use analysis in these kinds of cases. First, courts would adjust their view of the purpose and character of the use—the use by the ultimate consumer would be relevant in such an inquiry. Courts would have to expressly consider whether the use engaged in by the consumer was an affirmative entitlement, or whether it was more of a residual right. If it were an affirmative entitlement, then the commercial nature of the company's use would be far less relevant. The compensation to the company would be seen as an appropriate reward for making the exercise of the entitlement more efficient. On the other hand, if the ultimate use engaged in by the consumer occurs more because of an inability to license, then the commercial nature of the company's use would remain quite relevant.

This would require courts to make substantive distinctions between different types of consumer uses. So, for example, in the copy shop cases,

courts would have to affirmatively decide whether student copying of journal articles and book excerpts is, in itself, fair use. A court could certainly conclude that it is not, and therefore the copy shops should get no special consideration. Yet at the very least, courts should be required to engage in this analysis. This would force courts to adopt a broader perspective by preventing the narrow application of the fair use factors to only the company at issue.

Second, courts would look more carefully at the harm to the market factor. In some cases, even if the activities of the companies facilitate exercise of an affirmative fair use right, there might be too great a harm to the direct market for the work. So, for example, in the *MP3.com* case, there might be a quite reasonable fear that the actions of MP3.com not only make space-shifting more efficient, but also facilitate copying that would clearly not be fair use (for example, use of a single CD by several different people to gain access to multiple copies of a copyrighted song). Or, in the copy shop cases, it is possible that facilitating the student use of coursepacks might in the end so undermine the market for books and articles that this would outweigh the benefits from greater exercise of fair use.[66]

However, such claims should be critically examined and not simply uncritically accepted. Viewing a consumer use as an affirmative entitlement would lead courts to more carefully assess claims of market harm by forcing them to weigh that harm against a competing consumer interest. Thus, if it turned out that, due to the peculiarities of the market for academic publishing, coursepacks would not have a significant impact on the production of academic works, this would support the entitlement of the copy shops. At the very least, once a consumer interest is identified, there is a reason for courts to engage in a more thorough inquiry into the impact of the use on the market.

Moreover, courts would more carefully scrutinize claims of lost licensing revenue and would not automatically credit such claims. Viewed from the perspective of the consumer, it is far less clear why the loss of potential licensing revenue should be considered market harm. In effect, this is a question regarding the allocation of the benefits from more efficient consumer fair use. If a court views the consumer fair use as an affirmative

66. *See* Los Angeles News Service v. Tullo, 973 F.2d 791, 797-99 (9th Cir. 1992); Infinity Broad. Corp. v. Kirkwood, 150 F.3d 104, 112 (2d Cir. 1998) (citing *MDS* for the proposition that "large-scale photocopying, even for the statutorily-approved purpose of educational use, can still infringe").

good, then the company facilitating the use may have a greater claim to the proceeds from the increased efficiency.

Consider the bowdlerization example. The companies in these cases are careful to maintain a one-to-one ratio of edited-to-original DVDs. Accordingly, there is no realistic claim of harm to the direct market. Indeed, there is a very good claim that the service benefits the direct market by enabling purchases by consumers who would otherwise have avoided purchasing the DVD in the first place. Moreover, the claim of harm to the market via licensing seems particularly weak, given that the copyright owners have not sought to exploit this market, and the companies in these cases should share in the benefits of a service that enables consumers to more efficiently exercise their right to view movies in the manner they wish.

Finally, courts may consider the possibility of withholding injunctive relief and instead awarding some level of damages. In some cases, a court might well conclude that the benefits from more efficient consumer fair use should be shared between the company and the copyright owner. Where a court believes that bargaining would not result, a court could award damages rather than an injunction. This might give more incentive to companies to look for opportunities to help consumers exercise their fair use rights.

Ultimately, a consumer-conscious perspective would require courts to take more seriously the argument that a supposedly infringing company is instead actually facilitating a consumer's exercise of fair use rights. Although such a result would not always allow companies to step into the shoes of their customers, it would at least allow them to briefly slip the shoes on to see if they fit.

B. Implications for the DMCA and DRM

While the analysis in the preceding section focused on the fair use defense, it is worth asking how recent changes to the copyright laws, namely the enactment of the Digital Millennium Copyright Act, affect this analysis.[67] To some extent, the DMCA places another potential barrier to the more effective exercise of consumer fair use. Many copyright owners are increasingly deploying technologies to restrict the ability of consumers to copy or freely manipulate digital copies of copyrighted works. The DMCA imposes liability for the circumvention of these technological

67. 17 U.S.C. §§ 1201-05 (2000).

measures.[68] It also bars the sale of technologies that have limited uses other than to enable circumvention.[69]

The DMCA thus stands in the way of many attempts by consumers to exercise their fair use rights. Take the bowdlerization example. I have argued above that we should recognize a right on the part of consumers to control how and when they watch a movie, and that this right likely extends to a fair use right to modify movies on DVD for personal consumption. Yet most consumers will not be able to do so because DVDs are encrypted. Thus, they do not have the technical ability to exercise their fair use rights.[70]

Moreover, even if a particular consumer did have such technical ability, he or she would be barred from exercising it by the DMCA, since doing so would constitute the illegal act of circumvention. The DMCA, unlike copyright more generally, does not contain a fair use defense. So even if the underlying use were to be fair, there would be no defense to the act of circumvention unless the use fell within a specific exemption or exclusion.[71] And even if consumers were to somehow obtain an exemption, they would have no access to technologies that would enable them to take advantage of the exemption.

Thus, in the end, the DMCA may obviate much of the above analysis, at least for works that are routinely protected by technological protection measures. In such cases, the role played by companies that facilitate fair uses would be even more vital, since most individuals likely do not have the technical expertise required to overcome the technological protection measures. Yet any company that facilitated such uses by individuals would likely run afoul of the DMCA. And, unlike the case with copyright, there is no general fair use defense available for these companies to leverage.[72]

The effect of the DMCA, therefore, is to largely disable consumers from exercising rights they would otherwise possess under fair use. If fair

---

68. *See* 17 U.S.C. § 1201(a)(1) (2000).

69. 17 U.S.C. §§1201(a)(2), (b) (2000).

70. *Cf.* Llewellyn Joseph Gibbons, *Entrepreneurial Copyright Fair Use: Let the Independent Contractor Stand in the Shoes of the User*, 57 ARK. L. REV. 539 (2004) (noting that end-users may not have technical sophistication to engage in some fair uses).

71. Under the DMCA, the Librarian of Congress may grant exemptions to circumvention liability in a triennial rulemaking proceeding. *See* 17 U.S.C. § 1201(a)(1)(C) (2000). One such rulemaking exempted film professors from liability for circumvention of technological protection measures to compile film clips for class. *See* 37 C.F.R. § 201.40(b)(1) (2006).

72. *See* Universal City Studios, Inc., v. Corley, 273 F.3d 429 (2d Cir. 2001) (holding that there is no fair use defense to DMCA liability).

uses are residual rights justified only by inefficiency, then we might not care about this effect, since new technologies will presumably make licensing less costly and eliminate the justification for fair use. However, if fair uses have independent value and are not just residual rights, then the DMCA acts as a practical limit on the ability of companies to step in and make such uses more efficient and accessible.

V. CONCLUSION

In this Article, I have argued that courts should be more sympathetic to attempts by companies to invoke the fair use rights of their customers. To the extent that we view some consumer fair uses as affirmative entitlements, consumer fair use arguments by the supposedly infringing companies that facilitate the exercise of such entitlements should be treated more favorably. Although such arguments should not always be dispositive, courts should at least carefully evaluate them.

MAKING ROOM FOR CONSUMERS UNDER THE DMCA

By Niva Elkin-Koren[†]

I. **INTRODUCTION** 1119

II. **DRM/DMCA AND POST-PURCHASE CONTROL** 1124

A. CONSUMER INTERESTS IN THE DIGITAL ENVIRONMENT 1125
B. THE CONSUMER PROTECTION APPROACH 1128
C. CONSUMERS UNDER THE DMCA: *LEXMARK* AND *CHAMBERLAIN* 1132

III. **THE INTERESTS OF INFORMATION CONSUMERS** 1138

A. CONSUMERS UNDER COPYRIGHT LAW: THREE CONCEPTUAL FRAMEWORKS 1138
B. CONSUMERS-AS-PARTICIPANTS 1141
C. INCORPORATING CONSUMER PERSPECTIVES INTO COPYRIGHT ANALYSIS 1146

IV. **WHAT COULD BE GAINED BY THE CONSUMER-AS-PARTICIPANT PERSPECTIVE?** 1150

I. INTRODUCTION

This Article seeks to articulate the interests of information consumers in the era of Digital Rights Management Systems (DRMs). The impetus for this inquiry is the growing threat to the interests of information consumers in the digital age. Recent years have seen a growing number of instances where DRMs are used in ways that threaten consumer rights, such as invading consumer privacy, disabling interoperability, causing security breaches, and limiting the ability of users to annotate their copies or to use them in the time and space of their choice.[1] The use of DRMs turns infor-

---

† Professor of Law, Haifa Center for Law and Technology, University of Haifa Faculty of Law. Thanks to Eran Bareket, Abraham Drassinower, Wendy Gordon, Asaf Jacob, Roberta R. Kwall, Gideon Parchomovsky, Jerome H. Reichman, Pamela Samuelson, Kim Treiger and Tal Zarsky for insights and comments. I am grateful to Lital Leichtag and Jennie Lobovski for research assistance.

1. Concerns were raised by several NGOs. *See* ELECTRONIC FRONTIER FOUNDATION, UNINTENDED CONSEQUENCES: SEVEN YEARS UNDER THE DMCA (2006), http://www.eff.org/IP/DMCA/DMCA_unintended_v4.pdf [hereinafter UNINTENDED CONSEQUENCES]. Digital Consumer organizations are focusing on different consumer concerns, such as the ability to time-shift and space-shift and to create copies of purchased media.

mation, once a non-excludable public good, into an excludable commodity. Rightholders can monitor the use of their respective works and collect information on the number of copies, the frequency of use, or the context in which the work was played. DRMs dramatically reduce the cost of long-term inspection of copies and therefore strengthen the hold of rightholders over private use.[2] In fact, digital copies protected by DRMs enable rightholders to exercise unprecedented control over the use of copies after purchase by consumers.[3]

While many concerns raised by the use of DRMs—such as price and consumer friendliness—are relevant to all types of commodities, other concerns are closely connected to information policy. These new mechanisms for physical control over the use of copyrighted works may threaten intellectual freedom and fundamental liberties. It is precisely this dimension, of consuming cultural goods, on which this Article focuses.

A growing body of literature seeks to articulate the rights of *recipients* of copyrighted works: users of embedded software, music fans who purchase songs on iTunes, viewers of downloaded movies, purchasers of ringtones for mobile phones, and subscribers of online journals. As the digital environment enhances the consumers' capacity to actively engage in creative processes, legal scholars have paid growing attention to the rights of *users* of copyrighted materials.[4] However, scholars have only recently be-

---

See, e.g., DigitalConsumer.org, Overview, http://www.digitalconsumer.org/overview.html (last visited July 7, 2007).

2. In the past, the high cost of monitoring private copying made enforcement impractical. Consequently, copyright law focused on public exploitation, prohibiting unauthorized public performance and public distribution. Copyright enforcement further focused on intermediaries such as publishers and printers.

3. Consider, for instance, the Adobe Acrobat eBook platform. This system enables originators of content to distribute text in a digital form, but at the same time to restrict certain operations related to the files, such as editing, copying, printing, or annotating. As explained in the Adobe Acrobat eBook:

> To protect copyrights, publishers establish their own guidelines for how much of their eBooks can be printed or copied. This means that these permissions will differ from book to book. For example, some of the free books from the Adobe Bookstore have no restrictions on copying and printing. Or, a publisher might give users the ability to print several pages of a cookbook within a set period of time.

Adobe.com, Adobe Acrobat eBook Reader Frequently Asked Questions, http://www.adobe.com/support/ebookrdrfaq.html (last visited July 7, 2007) [hereinafter Adobe eBook FAQ].

4. Patterson & Lindberg explicitly addressed users' rights in their seminal book. L. RAY PATTERSON & STANLEY W. LINDBERG, THE NATURE OF COPYRIGHT: A LAW OF US-

gun to focus their attention on consumers, acknowledging the significance of consumers for free speech purposes and for advancing the fundamental goals of copyright law.[5] Conceptualizing the interests of information consumers is crucial for setting limits on the use of DRMs by rightholders, as information consumption becomes central to our everyday lives and post-purchase control of cultural goods becomes more profound.

I offer a view of information consumers that is based on the theoretical framework of copyright law. This perspective situates the interests of information consumers within the general context of information policy. I argue that consumer protection laws cannot fully address the emerging threats to the interests of information consumers.[6] The consumer protection perspective focuses primarily on the economic aspects of consumerism, aiming to resolve some of the primary market failures associated with it. DRMs, however, not only limit certain rights of consumers, but also affect the symbolic meaning of copyrighted works. They shape our practices of consumption and the meaning of cultural artifacts. Such threats to the rights of information consumers often fall outside the radar screen of consumer protection laws. Thus, the use of DRMs may invoke more general considerations arising from information policy. This gap suggests a need to articulate the unique interests of information consumers and to provide a conceptual framework for defining the scope of those interests.

Exploring the interests of information consumers from the perspective of information policy reveals the multi-dimensional relationship between consumers and cultural artifacts. This inquiry may disclose an important dimension of information consumption that, so far, the DMCA and consumer protection laws have failed to address. While some aspects of experiencing informational works relate to the communicative and symbolic

---

ERS' RIGHTS (1991). *See also* Niva Elkin-Koren, *Cyberlaw and Social Change: A Democratic Approach to Copyright in Cyberspace*, 14 CARDOZO ARTS & ENT. L. J. 215, 216 (1996); Niva Elkin-Koren, *It's All About Control: Rethinking Copyright in the New Information Landscape*, *in* THE COMMODIFICATION OF INFORMATION 79, 79 (Niva Elkin-Koren & Neil W. Netanel eds., 2002); Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L. J. 561 (2000).

5. *See* Joseph P. Liu, *Copyright Law's Theory of the Consumer*, 44 B.C. L. REV. 397 (2003); Rebecca Tushnet, *Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It*, 114 YALE L.J. 535 (2004); Julie E. Cohen, *The Place of the User in Copyright Law*, 74 FORDHAM L. REV. 347 (2005); Malla Pollack, *A Listener's Free Speech, A Reader's Copyright*, 36 HOFSTRA L. REV. (forthcoming 2007); Alan L. Durham, *Consumer Modification of Copyrighted Works*, 81 IND. L. J. 851 (2006); Jessica Litman, *Lawful Personal Use*, 85 TEX. L. REV. 1871 (2007).

6. *See infra* notes 33-37 and accompanying text.

values of such works and call upon the recipients as users and speakers, other aspects invoke the nature of informational works as commodities. Identifying and connecting these different dimensions may help us to better understand the process of consuming information and the special needs of information consumers. Furthermore, identifying the interests of information consumers may introduce a new dimension to standard copyright analysis, which often favors copyright owners, by incorporating a legitimate interest in *access* so as to balance the scope of rights shaped by the DRM/DMCA regime.

The inspiration for incorporating consumer discourse within copyright analysis originates from two U.S. decisions, *Lexmark*[7] and *Chamberlain*.[8] These cases demonstrate how the DRM/DMCA regime can be abused to leverage market power and limit consumer choice. *Chamberlain* involved Garage Door Openers (GDOs) and an attempt to stop the distribution of universal transmitters.[9] The Federal Circuit held that consumers have a legal right to use the embedded software they have purchased, in conjunction with competing products. Taking a similar "consumer-friendly" approach, the court in *Lexmark* denied Lexmark's claim under the DMCA, where it sought to prevent an aftermarket for printer cartridges by using an authentication sequence.[10]

Lexmark and *Chamberlain* addressed the interests of consumers in tangible articles of commerce—a printer cartridge in *Lexmark* and a GDO in *Chamberlain*. However, in cases involving the use of DRMs to protect informational works, courts have failed to apply a similar approach.[11] This failure seems puzzling: why would courts opt to protect the interests of consumers in rather mundane commodities but fail to do the same for cultural artifacts? Moreover, cultural artifacts seem to invoke a wide range of

---

7. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2003).

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

9. The universal transmitters distributed by the defendant enabled users to operate Chamberlain GDOs. They simulated the rolling codes, which plaintiff argued were technological measures that control access to copyrighted software incorporated in the openers and transmitters.

10. Lexmark sought to prevent an aftermarket for printer cartridges by using an authentication sequence in the Printer Engine Program, which enabled loading of authenticated toner cartridges only. The court denied Lexmark's claim under the DMCA. *Lexmark*, 387 F.3d at 550-51.

11. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000); RealNetworks, Inc. v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000); Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005).

consumer vulnerabilities that may deserve more careful attention. In addition to being useful commodities with an entertainment value that could be priced, cultural artifacts also possess communicative value and symbolic significance. They engage our minds in a more direct and intimate way than do tangible goods.

If consumers of GDOs are free to use their copies as they choose, why don't we let consumers of songs purchased from iTunes play their music on a platform of their choice?[12] Could it be that we conceive of the freedom of consumers who purchase ink cartridges as greater than the freedom of home viewers to convert their movies to be watched on their cell phones, or even to create a family-friendly version so that they can share them with their kids?

I argue that the same rationale that convinced the courts to limit the scope of anti-circumvention rules in *Lexmark* and *Chamberlain* should be applied in other contexts involving copies of more conventional copyrighted works such as video games, music, video clips, and artistic images. I further argue that the interests of information consumers should not be conceived as simply an external consideration that might limit the scope of copyright in appropriate cases. This approach was taken by the *Chamberlain* court. The court concluded that consumers' rights call for a narrow construction of the DMCA that would be consistent with antitrust laws. I argue that the interests of information consumers should also be considered an integral part of copyright analysis, deriving from its fundamental tenets. This requires, however, an understanding of the interests of information consumers.

Part II discusses DRMs and the legal regime that governs their use. Section A briefly introduces the DRM and anti-circumvention regime, arguing that post-purchase control enabled by DRMs may affect consumer welfare. Section B explores the limits of consumer protection laws for securing the interests of information consumers. Consumer protection laws, I argue, cannot sufficiently address these interests because consumer protection doctrine does not fully capture the threats to the interests of information consumers and because consumer rights may be easily overridden. Section C revisits copyright cases concerning the rights of consumers and

12. *See, e.g.*, Brian Deagon, *EU Lodges Complaint Against Apple's iTunes; Alleges Restrictive Practices; Record Labels Also Named, in a Case Made Complex by Europe's Many Regulations*, INVESTOR'S BUS. DAILY, Apr. 4, 2007, at A05; Dan Carlin, *Europe vs. Apple: Facing the Music*, BUS. WEEK ONLINE, Jan. 31, 2007, http://www.businessweek.com/globalbiz/content/jan2007/gb20070131_492654.htm; Ryan Katz, *Apple 10-Q: Thirteen New Lawsuits, Nine Settled*, THINK SECRET, Jan. 2, 2007, http://www.thinksecret.com/news/0612sec10q.html.

suggests that the courts were attentive to the interests of consumers only when mundane commodities were at stake.

Part III articulates the unique interests of information consumers. Section A identifies the impediments to conceptualizing consumer interests under copyright law and suggests a way to make room for consumers under the copyright regime by re-conceptualizing the notion of "information consumer." It introduces two perceptions of consumers under copyright law (i.e., *consumer-as-shopper* and *consumer-as-author*) and proposes a new one: "*consumer-as-participant*." Section B emphasizes the different dimensions of information consumption, arguing that the perception of *consumer-as-participant* adds a new dimension to standard copyright analysis, which is particularly significant in the environment of user-generated content. Developing a notion of consumer protection of informational products requires expanding the focus on economic consumers (*consumers-as-shoppers*) to incorporate an understanding of consumers as citizens and participants in "meaning-making" processes. Section C demonstrates how consumer interests could be incorporated into copyright analysis.

Part IV identifies some of the advantages arising from incorporating a *consumer-as-participant* perspective into copyright analysis. One advantage is that this perspective may add legitimacy to consumers' claims against restrictions on access to copyrighted materials. Another advantage is that copyright theory provides a conceptual framework for articulating the legitimate interests of consumers. This is particularly crucial in the digital environment, as consumers of informational works perform multiple roles simultaneously, functioning as producers, distributors, and recipients of content. Third, a consumer perspective highlights strategic uses of DRMs for anticompetitive purposes. Fourth, the consumer perspective provides an organizational structure for political action. Finally, expanding copyright analysis to account for the interests of consumers could set limits on the use of the DRM/DMCA regime for post-purchase control.

II. DRM/DMCA AND POST-PURCHASE CONTROL

Many of the latest conflicts and challenges involving copyright law leave us with the feeling that copyright discourse is rather limited and that it does not capture the complexity of emerging information markets and new technologies. The advent of a new copyright regime based on DRMs and anti-circumvention is one example. The use of DRMs enables physical control over the use of cultural artifacts long after purchase by consumers. This shift in the nature of informational works affects the relation-

ship between rightholders and recipients of copyrighted materials. It enables a long-term relationship between suppliers and recipients of copyrighted works. Copyright discourse that focuses on authors often overlooks the consequences for recipients of copyrighted materials. To appreciate this we need to first understand how DRMs affect consumer welfare as well as how the anti-circumvention regime facilitates this influence. We will then examine the legal strategies that could address consumer interest: the consumer protection approach and the copyright approach.

A. Consumer Interests in the Digital Environment

Digital networks, which make it extremely easy to copy and mass distribute copyrighted materials, also enable technological protection of such works. DRMs are technological measures that rightholders increasingly employ to control the use of copyrighted materials distributed in digital format. For instance, DRMs might provide limited access to works for paying users only, limit some functions of digital files (e.g., the number of backup copies), or even prevent certain uses altogether (e.g., saving, printing, or annotating a particular copy).

DRMs allow vendors to exercise control over the use of works, even after they have been purchased by consumers. Such post-purchase control over the use of works was not available to copyright owners in the past and is hardly available to suppliers of other commodities. For instance, region coding prevents the use of a purchased DVD outside the region, so that the owner of a DVD purchased in the US cannot play the movie on a computer that is set for Europe.[13] Similarly, music encoded by a particular DRM could be limited to play on only one music player.[14] In recent years, DRMs were used to prevent gamers from playing legally purchased copies of games on different game consoles,[15] to prevent purchasers of video

13. DVDDemystified.com, DVD Frequently Asked Questions (and Answers), http://www.dvddemystified.com/dvdfaq.html (last visited July 9, 2007). Post-purchase control could be implemented in several ways. One way to implement it is through the copies themselves. Adobe PDF, for instance, allows the distributor of the file to prevent certain uses of the file, such as saving and printing. Adobe.com, Create Adobe PDF Online, http://createpdf.adobe.com/cgi-feeder.pl/help_security (last visited July 9, 2007). Adobe's eBook platform facilitates control of access restrictions which allows access to stored information for a limited time, after which the file would "expire." Adobe eBook FAQ, *supra* note 3.

14. A consumer that purchases music on iTunes and wishes to switch to a different format is restricted from doing so. *iTunes user sues Apple over iPod*, BBC News, Jan. 6, 2005, http://news.bbc.co.uk/1/hi/technology/4151009.stm (last visited July 9, 2007).

15. *See, e.g.*, UNINTENDED CONSEQUENCES, *supra* note 1, at 10 (Sony sues Bleem and Connectix, claiming that PlayStation emulators for Macintosh computers and for Windows PCs constitute circumvention and violate the DMCA).

games from playing their games over the internet,[16] and to prevent the owners of music files purchased on iTunes from transferring their songs to devices other than the iPod.[17] Consumers are therefore often locked into a specific hardware device and might find it cost-prohibitive to switch to a different device, fearing they will lose their sunken investment in their current collection.

Furthermore, DRMs regularly prevent copying, modification, and redistribution of music files, software, images, or textbooks, thereby limiting the ability of consumers to freely experience the copies purchased. E-books, for instance, such as Adobe's Acrobat eBook platform, use encryption to limit the number of copies or prevent any modification of the text.[18]

DRMs may affect consumer welfare indirectly when employed to protect dominance in the market for platforms and applications.[19] For instance, Apple used its DRM to prevent RealNetworks' digital download store from using Harmony, a DRM designed to be compatible with Apple's FairPlay DRM and iPods.[20] iPod, the most popular digital music player, reads only Apple's FairPlay. Incompatibility with formats used by other music distributors makes it difficult for competitors, such as RealNetworks, to compete with Apple. Apple is currently facing a lawsuit in the U.S. over tying the iTunes store to the iPod.[21] Reducing competition

---

16. *Davidson & Assocs.*, 422 F.3d at 635.

17. Songs purchased from iTunes, which is the leading online music store service run by Apple, are formatted with FairPlay, which prevents consumers from playing songs on other devices (and also limits the number of copies and uses of the download songs). RoughlyDrafted.com, How FairPlay Works: Apple's iTunes DRM Dilemma, Feb. 6, 2007, http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351 C60-A4E5-4764-A083-FF8610E66A46.html. Songs (music files) sold on CONNECT, Sony's online music store, are downloadable in ATRAC3 format, which is a proprietary format that can only be played on Sony players. Sandy McMurray, Corante, Connect - Sony's music store, Apr. 19, 2004, http://apple.corante.com/archives/2004/04/19/connect_sonys_music_store.php.

18. Adobe eBook FAQ, *supra* note 3.

19. Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1629 (2002).

20. Apple threatened legal action under the DMCA, forcing RealNetworks to give up its initiative. *See* John Borland, *Apple Fights RealNetworks' 'hacker tactics'*, CNET NEWS.COM, Dec. 14, 2004, http://news.com.com/Apple+fights+RealNetworks+hacker+tactics/2100-1027_3-5490604.html?tag=item; Matt Hines, *'Stunned' Apple Rails Against Real's iPod Move*, CNET NEWS.COM, Jul. 29, 2004, http://news.com.com/Stunned+Apple+rails+against+Reals+iPod+move/2100-1041_3-5288378.html.

21. This suit, filed in July 2006 by user Melanie Tucker in the U.S. District Court for the Northern District of California, was revealed by Apple in a filing with the Securities and Exchange Commission. Tucker, who is seeking class-action status, argues

may lead to an increase in price, rendering access to music more expensive.

However, DRMs do not in and of themselves pose a threat to consumer interests. The fact that a product's design limits some of its functions does not automatically imply that consumer interests have been compromised. By definition, the design of a product always restricts what we can do with it. Yet, we are usually free to adapt our purchased commodities to serve our preferences and needs. This is particularly true in the case of digital content, which can be easily shaped by end users.

Restrictive measures have always been employed by rightholders to strengthen their control over creative works. What actually disables consumer choice is the anti-circumvention regime under the Digital Millennium Copyright Act (DMCA).[22] Under the DMCA, DRMs are immune from technical challenges and equipped with powerful legal sanctions against hacking. The purpose of the DMCA was to tackle piracy and to strengthen the effectiveness of DRMs.[23] It was presumed that technological measures employed by rightholders could only be effective when it is possible to efficiently prevent their circumvention. Once a digital lock has been hacked, the creative work becomes, once again, vulnerable to copying and unlicensed distribution.[24] The DMCA outlaws the circumvention of protective measures[25] at three levels: banning access to a work by cir-

---

that Apple failed to give consumers notice that music purchased from the iTunes Store is incompatible with music and playing devices offered by other vendors. The suit further alleges that Apple violates antitrust laws by the exclusive tie-in between iTunes and the iPod. Apple's motion to dismiss was denied by the court in December 2006. Tucker v. Apple Computer, Inc., 2006 U.S. Dist. LEXIS 96343 (N.D. Cal. Dec. 20, 2006). *See also* Randall Stross, *Want an iPhone? Beware the iHandcuffs*, N.Y. TIMES, Jan. 14, 2007, at § 3, at 3.

22. Digital Millennium Copyright Act, Pub. L. No. 105-304 (1998) (codified in scattered sections of 17 U.S.C.).

23. Zohar Efroni, *Towards a Doctrine of 'Fair Access' in Copyright: The Federal Circuit's Accord*, 46 IDEA 99, 101 (2005).

24. *See* Jane C. Ginsburg, *The Pros and Cons of Strengthening Intellectual Property Protection: Technological Protection Measures and Section 1201 of the U.S. Copyright Act* 17 (Columbia Law Sch. Pub. Law & Legal Theory Working Paper Group, Paper No. 07-137, 2007), *available at* http://ssrn.com/abstract=960724 (assessment of the judicial and administrative construction of Chapter 12 of the 1998 Digital Millennium Copyright Act).

25. Circumvention of a technological protection measure is defined as an act to "avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3) (2000).

cumvention,[26] banning trafficking in devices that circumvent measures protecting copyrights,[27] and banning the manufacturing and distribution of devices designed to circumvent access controls.[28] Thus, the anti-circumvention regulation resulted in a third layer of protection for copyright materials, which enabled excessive control by rightholders over the use of works purchased by consumers.

The DMCA, which was originally enacted to confront piracy, has turned DRMs into an effective means of governing the use of copyrighted works in digital format. Consumers cannot legally hack technical measures that limit their ability to use copies they have legally purchased. The law also makes it illegal to provide circumvention means, thus further limiting the opportunities for consumers to remove technical measures which restrict the functionality of their purchased copies. Indeed, since the enactment of the DMCA, DRMs have been employed to compromise consumer rights in a growing number of cases.[29]

B. The Consumer Protection Approach

The question now becomes, what is the best way to limit post-purchase control facilitated by the DRM/DMCA regime? It has been suggested that DRMs that contradict consumer expectations should be treated as a matter of consumer protection law: a consumer purchasing a copy has some legitimate expectations regarding the use of her copy. For instance, she may expect to use her copy in conjunction with other products. A consumer may also expect to make a backup copy for her personal use, so she can watch it on her personal computer, or listen to it on her portable player.[30] Courts have generally been responsive to consumer interests in cases that

---

26. 17 U.S.C. § 1201(a)(1) (2000) makes it illegal to "circumvent a technological measure that effectively controls access to a work."

27. 17 U.S.C. § 1201(b)(1) (2000).

28. *Id.* § 1201(a)(2). *See generally* Ginsburg, *supra* note 24.

29. Universal City Studios v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. 2000); RealNetworks, Inc. v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000); Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005), Sony Computer Entm't Am., Inc. v. Gamemasters, 87 F. Supp. 2d 976 (N.D. Cal. 1999).

30. The INDICARE report concludes that the legal position of consumers under copyright law is weak, and therefore there is a need to treat DRMs not only as a matter of copyright law but also as a matter of general consumer protection law. Natali Helberger, *It's Not a Right, Silly! The Private Copying Exception in Practice*, 1 INDICARE MONITOR 107, 107-09 (2004), *available at* http://www.indicare.org/tiki-download_file.php?fileId=105.

invoke a traditional consumer claim, such as a lack of notice.[31] Consumer rights claims could be equally effective when DRMs create a security risk for consumers' computers, such as in *Sony BMG*, a consolidated lawsuit in which a DRM was secretly installed on music CDs.[32]

While consumer protection doctrine is often useful for addressing consumer concerns regarding DRMs, it also suffers from several hindrances. These limitations arise first from the nature of claims invoked by consumer protection laws and second from the type of remedies tailored to address those claims. Claims invoked by consumer protection laws are confined by the limited scope of consumer protection doctrine. This results in a rather limited framework for conceptualizing the harm created by DRMs to information consumers and for defining the scope of their rights vis-à-vis copyright owners. The threat to consumer interests posed by DRMs could be easily trivialized, and the banality of mass consumption makes it difficult to understand what issues are at stake. Why should

---

31. For instance, in a recent French decision, the court ruled in favor of consumer groups in France who filed a suit against Sony France and Sony UK. The court found that Sony did not provide sufficient notice and failed to clearly inform the consumers that these files could not be played on other players. The court ruled that a manufacturer's omission from the label of the fact that a CD is incompatible with a few devices, like a car stereo, misleads the consumer. *See* SA EMI Music France v. Association CLCV, Cour d'Appel [CA] [regional court of appeal] Versailles, 1e ch. 1e sec., Sept. 30, 2004 (Fr.), *available at* http://www.juriscom.net/jpt/visu.php?ID=579. The court further held that Sony France did not provide clear information to the consumers of Sony players and failed to disclose that these players are not compatible with other files. The court found Sony's "tying practice" to be contrary to the Code de la Consommation [Consumer Code], art. L122-1 (Fr.). Sony's practice, the court held, compelled consumers who downloaded music files from Connect to buy a Sony player if they wanted to play them. *See* Delphine Strauss, *French court rules against Sony*, FIN. TIMES LTD., Jan. 5, 2007, at 17.

32. The DRM had several functions, which, in addition to limiting the number of copies a user could make, invaded the privacy of users by reporting information to the vendor and further created a serious security risk by installing undisclosed files on users' computers. A number of class action lawsuits were filed against Sony BMG in the United States, the majority of which were consolidated in the United States District Court for the Southern District of New York. *See In re* Sony BMG CD Techs. Litig., No. 1:05-cv-09575-NRB (S.D.N.Y. Dec. 28, 2005), *available at* http://www.girardgibbs.com/sonyconsolidatedamendedcomplaint.pdf. Consumer protection actions against Sony BMG, which were filed by a number of state Attorneys General, were settled in December of 2006. *See* Electronic Frontier Foundation, Sony BMG Litigation, http://www.eff.org/IP/DRM/Sony-BMG/#docs (last visited July 7, 2007). For further discussion of the Sony BMG incident, *see generally* Deirdre K. Mulligan and Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L. J. 1157 (2007).

we care whether the users of iTunes can play their music on another music player?

The consumer protection perspective requires a baseline definition of consumer expectations. It is difficult to define the scope of "legitimate" consumer expectations deserving guardianship by law. Arguments regarding legitimate expectations of consumers in digital media often rely on their comparable ability to use materials in analog format. For instance, record purchasers were able to repeatedly play their records, and therefore, in this context, limiting access to music for the duration of a subscription may seem unfair. This argument, however, does not explain why consumers are entitled to exactly the same functionality when they use content in digital format.[33] Litman proposes a substantive test: the rights of readers and listeners to interact with copyrighted works should be adjusted to accommodate parallel uses made possible by new technologies.[34] Applying this criterion, however, assumes that consumers are entitled to exercise a particular level of interaction with copyrighted material. The definition of such freedom to interact with copyrighted materials cannot derive from consumer protection principles alone.

Another basis for defining consumer expectations is contractual, and it is based on notice and choice. For instance, if a consumer thinks she can use an MP3 file on any media player, and she finds out only after the purchase is already completed that she cannot, courts are likely to perceive this transaction as a violation of her consumer rights. However, defining legitimate consumer expectations based on contractual warranties alone may prove insufficient. After all, the scope of consumer expectations may

---

33. The definition of reasonable consumer expectations is often based on an equivalent use in the analog environment. Consider books, for instance. Book publishers used to exercise no control over the reproduction of books and relied exclusively on copyright law to prevent the preparation and distribution of illegal copies. E-books, by contrast, use encryption to limit the number of copies and prevent modification of the text. DRMs, in this case, prevent continued use. This could implicate the rights of libraries and archives that purchased a subscription for a scientific journal. If they do not continue the subscription they may not only lose access to new issues of the journal, but also lose access to previously purchased copies.

34. Litman, *supra* note 5, at 1911. Litman writes:

> Just as technology spurs evolution in the creation and marketing of works of authorship, it causes parallel evolution in the modes of interaction with those works. We don't want to limit copyright owners to the traditional marketing outlets of bookstores and sheet music sales. Similarly, it makes no sense to limit readers, listeners and player to piano or analog cassette tape.

Id.

be further limited by allowing providers to include disclaimers regarding available uses in the User License Agreement (ULA).[35]

Secondly, consumer protection laws offer a relatively limited set of remedies to consumers of information goods. Consumer protection laws seek to remedy deficiencies in informed consent and therefore consumer interests are often reduced to questions of notice. Consumer protection laws presume that there is an imbalance of power between consumers and suppliers that derives primarily from disparities in information. Suppliers often enjoy a systematic information advantage over consumers, since they are presumably more familiar with the products and services they supply, the markets for these commodities, and particular terms and conditions that govern the relevant transactions. Consequently, consumer protection laws focus on adequately informing consumers regarding their choices. If consumers receive sufficiently conspicuous notice, it is assumed that consumer interests will be reflected in the market through demand.[36] Thus, under the present regime, consumer rights may be easily overridden. To legalize a given restriction under consumer protection laws, it is often sufficient to simply give prior notice.[37]

While providing prior notice may remedy some market deficiencies, it cannot address the harm caused by DRMs to the interests of information consumers. Informational works raise other concerns that should not be simply overridden by a standard contract. Whereas consumer protection

---

35. In *Chamberlain*, the Federal Circuit warned that the broad interpretation of the DMCA suggested by plaintiff "would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial 'encryption' scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing productions." Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004).

36. Studies show, however, that many online music services do not respect consumer expectations of personal use. *See* Deirdre K. Mulligan et al., *How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use", in* PROCEEDINGS OF THE THIRD ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT 77, 77-89 (Moti Yung ed., 2003).

37. In Europe, a French court fined EMI Music France for selling CDs with DRM protection schemes that would not play on car radios and computers. EMI violated consumer protection law because it did not appropriately inform consumers about these restrictions. The court obliged EMI to label its CDs with the text: "Attention—this CD cannot be read by all CD-players or car radios." Cour d'appel [CA] [regional court of appeal] Versailles, 1e ch., 1 sec., Sept. 30, 2004, RG n° 03/04771, F. Bardy, *available at* http://www.legalis.net/jurisprudence-decision.php3?id_article=1344. *See also French Court Forbids DVD Copy Protection*, EDRI, May 4, 2005, http://www.edri.org/edrigram/number3.9/DVD (describing a Paris appeal court case that outlawed the use of DVD copy protection mechanisms).

laws focus primarily on the economic aspects of consumerism, seeking to adjust many of the primary market failures associated with it, informational products require a broader perspective. Informational works are usually not simply useful commodities that may be judged strictly by their utility and price. They engage consumers in ways that may affect their autonomy and freedom of expression.[38] Thus, the interests of information consumers should be addressed within a general framework of information policy. Such a shift demands a better understanding of the virtues of information consumption. Developing a notion of consumer protection for informational products requires adjustment of consumer protection principles by expanding the focus on economic consumers to incorporate an understanding of consumers as citizens.

C. Consumers under the DMCA: *Lexmark* and *Chamberlain*

An initial question is whether the interests of information consumers could be addressed under current copyright law. Indeed, copyright law facilitates post-purchase control, allowing copyright owners to restrict the use by purchasers of copies (i.e., the preparation of copies of a book or the public performance of a DVD). However, copyright law does not permit absolute restrictions. It incorporates checks and balances by recognizing instances in which copying may be permitted. It allows post-purchase restrictions within the limits of the delicate balance between exclusivity and access that defines the scope of copyright.

The cases of *Chamberlain*[39] and *Lexmark*[40] provided an exceptional opportunity to incorporate consumer protection considerations into copyright analysis. The two cases addressed circumstances that were not originally intended by the DMCA. In both cases, DRMs were used to restrict consumer choice in articles of commerce, and the protection of copyright was only secondary. *Lexmark* and *Chamberlain* were dream cases for those of us who had warned against the danger of anti-circumvention legislation back in the 1990's.[41] These cases demonstrated how suppliers

---

38. *See infra* notes 79-89 and accompanying text.

39. *Chamberlain*, 381 F.3d at 1193-94. *Chamberlain* was reaffirmed in Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1318 (Fed. Cir. 2005).

40. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2003).

41. Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 557 (1999); David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 739-42 (2000); John A. Rothchild, *Economic Analysis of Technologi-*

could use the anti-circumvention regime to leverage their market power and compromise consumer welfare. The significance of the *Chamberlain* and *Lexmark* decisions, however, goes beyond the particular circumstances decided in those cases. The decisions expose the vulnerability of information consumers under the DMCA and uncover the threats posed by the anti-circumvention regime to information markets. The decisions further reveal the dual nature of information consumption, involving a material dimension of owning a commodity and controlling an object, and an intangible dimension of using the information, which often entails a symbolic activity of creating and communicating meaning.

In *Chamberlain*, the Federal Circuit addressed the use of Garage Door Openers (GDOs).[42] Defendant Skylink sold universal transmitters that allowed users to operate Chamberlain Security+ GDOs by simulating the rolling code system. (The rolling code is a computer program that constantly changes the transmitter signal needed to open the garage door in order to prevent code grabbing.) Plaintiff Chamberlain alleged that the rolling code was a technological measure that controlled access to its GDO copyrighted software and that Skylink violated the anti-circumvention provisions by interfering with its access control measure. The Federal Circuit dismissed the suit, holding that consumers have a legal right to use the embedded software they have purchased in conjunction with competing products.

The explicit recognition of consumer rights under the DMCA by the *Chamberlain* court is particularly apparent in light of the total absence of such recognition from the copyright discourse in other instances concerning DRMs.[43] In somewhat similar circumstances involving online games, DVDs, and music players, the picture was quite different.

Compare *Chamberlain* to *Universal City Studios v. Reimerdes*,[44] one of the first lawsuits to be decided under the DMCA, which involved the circumvention of DVD encryption. The defendant distributed a program,

---

cal Protection Measures, 84 OR. L. REV. 489, 500-515 (2005); Niva Elkin-Koren, *The Privatization of Information Policy*, 2 ETHICS & INFO. TECH. 201 (2000).

42. *See infra* Section III.C (discussing *Chamberlain*).

43. In several instances unrelated to DRMs, courts have recognized the interests of consumers. *See, e.g.*, Lewis Galoob Toys, Inc. v. Nintendo of Am., Inc., 780 F. Supp 1283, 1291 (N.D. Cal. 1991), *aff'd* 964 F.2d 965 (9th Cir. 1992) ("Once having purchased, for example, a copyrighted board game, a consumer is free to take the board home and modify the game in any way the consumer chooses, whether or not the method used comports with the copyright holder's intent.").

44. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

DeCSS,[45] which enabled users to decrypt DVDs encrypted by rightholders using the Content Scrambling System (CSS).[46] Once a DVD was decrypted, users were able to make an unlimited number of copies of the recorded film. The court held that CSS is a technological measure that effectively controls access to copyrighted materials, and that DeCSS is, therefore, a circumventing device within the meaning of the DMCA.[47] The claim that DeCSS may be used legitimately for decrypting legally purchased DVDs when users wish to play the movie using alternative devices (such as the Linux operating system) was dismissed.[48]

In *Chamberlain*, the court sought to distinguish *Reimerdes*, suggesting that the circumvention in *Reimerdes* enabled the copying of copyrighted works, while Skylink's transmitters "enable only legitimate uses of copyrighted software."[49] In other words, when access also involves a copyright infringement—namely, a violation of protected rights—liability under the DMCA will apply. The end result in *Reimerdes*, however, is that rightholders maintain a right not only to limit copying but also to exercise control over the devices by which their works may be accessed and distributed.[50] Rightholders may control the format in which their work is distributed and the hardware with which it may be played. They are therefore

---

45. DeCSS is a computer program that emulates the CSS algorithm, which operates the "key" and thus enables users to play a DVD even in the absence of the CSS algorithm. In fact, it allows a non-CSS-compliant DVD player to play copies with DVD content. *Id.* at 314-15.

46. The CSS is an encryption-based security system that requires the use of specific hardware (DVD player or computer DVD drive) to decrypt, unscramble, and play back copies of the motion picture on DVDs. The key that is installed on the DVD becomes operative if it is accessed by an algorithm licensed by the DVD Copy Control Association (CCA) and installed in DVD players or in various programs available for PCs. *Id.* at 309-10.

47. *Id.* at 317-19.

48. *Id.* at 319 (The court held that even if this claim were true, which in the court's opinion was questionable, *see id.* at 311 n.79, defendant may still be liable under the DMCA.)

49. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1198 (Fed. Cir. 2004).

50. This end result is particularly troubling when compared to the pre-DMCA regime. In *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 454-55 (1984), for instance, the Supreme Court identified a legitimate use for the VCR, namely copying by television viewers for time shifting. Such use, the Court held, constitutes fair use, and therefore Sony could not be liable for contributory infringement merely by making VCRs available to the public. In *Reimerdes,* the court refused to consider the fair use of DeCSS, holding that fair use is not available under the DMCA. The DMCA, as interpreted by the court in *Reimerdes*, not only provides new powerful rights, but also lacks the checks and balances of copyright law. *See Reimerdes*, 111 F. Supp. 2d at 322.

able to control how the work is being used outside the relatively narrow scope of exclusive rights granted to them under copyright law.

Other courts followed *Reimerdes*. In *RealNetworks*,[51] the court accepted RealNetworks' claim that Streambox's media player, which enabled end users to download copies of audio and video files streamed by RealNetworks' application, violated the DMCA.[52] In *GameMasters*,[53] the court held that a device that allows playing legitimately purchased copies of video games on a platform other than originally intended by the vendor violated the DMCA.[54] The court found that a Game Enhancer allowing players to use imported games originally intended for Japanese or European PlayStation consoles violated the anti-circumvention ban.[55] The DMCA was therefore employed to prevent consumers from using their legitimate copies with competing devices, or to confine their use to a par-

---

51. RealNetworks, Inc. v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

52. Ironically, Apple used DRMs to stop the RealNetworks digital download store from using Harmony, a DRM that was designed to be compatible with Apple's FairPlay DRM so that music purchased on RealNetworks could be played on iPods. *See* Borland, *supra* note 20; Hines, *supra* note 20.

53. Sony Computer Entm't Am., Inc. v. Gamemasters, 87 F. Supp. 2d 976, 987 (N.D. Cal. 1999).

54. The court held that the device "circumvents the mechanism on the PlayStation console that ensures the console operates only when encrypted data is read from an authorized CD-ROM." *Id.*

55. Sony, like many other vendors of DVDs and videogames, such as Nintendo and Microsoft, uses a region code to restrict use in certain authorized areas. Ginsburg, *supra* note 24, at 8. The platform is designed to comply with a certain region code, and consumers in one region can only play content that is authorized for that region. In the case of PCs, definitions are incorporated into the operating system. GWEN HINZE, ELECTRONIC FRONTIER FOUNDATION, IN RE EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES: POST-HEARING COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION (2003), *available at* http://www.copyright.gov/1201/2003/post-hearing/post10.pdf. The stability of this business model therefore depends on the ability to prevent the manufacturing and distribution of software and devices that allow users to bypass the region code and play a DVD or a video game outside the region. Robert Silva, DVD Region Codes - What You Need To Know, http://hometheater.about.com/cs/dvdlaserdisc/a/aaregioncodesa.htm (last visited July 9, 2007). Recently, Sony brought a suit in Australia against the manufacturers of "mod chips" which allow users of Sony PlayStations to play games purchased in different regions. The Australia High Court distinguished between pirating a game and playing with legitimate copies using a mod chip: while making a pirated copy of a game is illegal, playing a game using a mod chip is not. The High Court held that regional coding intentionally reduces global market competition and limits consumers' rights. *See* Stevens v. Kabushiki Kaisha Sony Computer Entm't [2005] H.C.A. 58, 2005 WL 2450272, paras. 101-104 (Austl.).

ticular platform, allowing vendors to leverage their market power and compromise consumers' freedom.

Now, we return to this rather puzzling paradox: why would courts protect the interests of consumers in rather mundane commodities, and yet fail to do the same for cultural artifacts? If consumers of GDOs have a legitimate interest in using their products in conjunction with competing products, why don't the consumers of Sony PlayStation possess a similar legitimate interest? Why is it considered undesirable for a company to be able to "leverage its sales into aftermarket monopolies—a practice that both the antitrust laws and the doctrine of copyright misuse normally prohibit"[56] when it relates to GDOs, and yet the same practice is acceptable in the market for video games? If intellectual property rights do not confer the right to violate consumer rights and antitrust laws, why don't they apply equally to all works protected by copyright laws?

Presumably, attempts to stop unauthorized copying of DVD and computer games are justified by the need to secure incentives to invest in future creation. The consequential decline in competition is considered part of the package designed by intellectual property laws and is therefore justifiable under its premises. However, this justification did not equally apply to Lexmark's attempt to use DRMs for dominating the market for toner cartridges, or to Chamberlain's use of DRMs to impede competition in GDO apparatuses. Competition policy would render these attempts undesirable. What's more, since markets for content are based on intellectual property monopolies, the risk to competition and to consumer welfare in such markets is even greater. Whereas many markets for consumer devices are presumably competitive, markets for copyrighted materials are governed by owner exclusivity, and therefore the risks to competition associated with legally immune DRMs are even larger.

It seems that consumer interests in cultural artifacts might actually deserve more attention than the interests of consumers of mundane commodities. Cultural artifacts are not simply useful commodities. While they often have an entertainment value that could be quantified, they also possess a *communicative value* and a *symbolic significance*.[57] They engage our minds in a more direct and intimate way than do mundane commodi-

---

56. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1201 (Fed. Cir. 2004).

57. Cohen, *supra* note 5, at 370 (the situated user appropriates cultural goods found within her immediate environment for four primary purposes: consumption, communication, self-development, and creative play); Elkin-Koren, *It's All About Control*, *supra* note 4, at 80; Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 5, 46 (2004).

ties and, therefore, expose consumers to a higher risk of deeper and more intrusive restrictions of freedom. This particular vulnerability of information consumers is often overlooked.

Addressing consumer interests under copyright law raises several difficulties, the first of which is that consumers are almost entirely absent from copyright discourse.[58] A few exceptions include the first-sale doctrine, which allows the owner of a copy to resell or otherwise dispose of it;[59] the rights of owners of copies of software to make backup copies or adapt them where adaptation "is an essential step in" using the program;[60] and some fair use exemptions developed by courts, such as the *Sony* time-shifting exemption.[61]

The second reason for the difficulty in addressing the interests of consumers under standard copyright law is conceptual—the terms "consumer" and "consumption" do not fit informational works. We do not "consume" a book in the same way we "consume" chocolate. Both reading a book and eating a piece of chocolate may involve pleasure, but the novel—the copyrighted informational work that is embodied in a book—is never consumed. It can never be used up like all other tangible goods.[62] Consumption of informational works does not exhaust the resource. Moreover, consumption is itself productive. As will be explained further below, readers and viewers always benefit by experiencing the work in a way that contributes to social dialogue. Consumption of informational works is therefore nurturing an essential mechanism in the production of new content—human capital.

Thus, incorporating a consumer's perspective into copyright analysis requires taking a closer look at copyright laws and the multiple meanings assigned to the recipients of copyrighted materials.

---

58. *See* Liu, *supra* note 5, at 431.

59. 17 U.S.C. § 109(a) (2000).

60. *Id.* § 117(a). Similarly, a building owner has the right under section 120(b) of the Copyright Act to make "alterations to such building, and destroy or authorize the destruction of such building" notwithstanding the exclusive right of adaptation of the copyright owner in the architectural work. *Id.* § 120(b).

61. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429, 454-55 (1984). Note, however, that the Supreme Court in *Sony* failed to recognize a general right of private copying. *See* Jessica Litman, *The* Sony *Paradox*, 55 CASE W. RES. L. REV. 917, 957, 960-61 (2005). A privilege codified in the Audio Home Recording Act authorizes consumers to record music for personal noncommercial use. Audio Home Recording Act, 17 U.S.C. §§ 1001-1010 (2000).

62. Tushnet argues that "the greatest trick the content industry ever pulled was getting people to believe that readers and listeners are 'consumers,' as if they swallowed speech like candy." Tushnet, *supra* note 5, at 566.

III. THE INTERESTS OF INFORMATION CONSUMERS

A. Consumers Under Copyright Law: Three Conceptual Frameworks

Traditional conceptions of copyright deal with two aspects of consumers of copyrighted works: the *consumer-shopper* and the *consumer-author*. The *consumer-shopper* is a passive consumer, in the pure economic sense—a person who purchases commodities based on price and utility. As such, the consumer-shopper is generally absent from the copyright discourse. In contrast, the *consumer-author* creates new works by building on preexisting works. The consumer-author plays a central role in copyright discourse due to the significance of productivity and creativity in copyright ethos. A third aspect of copyright consumer, the aspect developed in this Article, is that of the *consumer-participant*, who helps position copyrighted works in a larger cultural framework.

The consumer-shopper lies outside the productive ethos of copyright law, which aims at promoting creativity.[63] Consumers have no role under copyright law and cannot aid in achieving its goals except by creating the ultimate market for informational goods and selfishly consuming the outcome of the creativity that was generated by others.[64] Consumers and consumerism have negative connotations associated with passive behavior. Consumption itself is often perceived as a problem and is sometimes despised for being unproductive. This might render consumers' complaints "illegitimate." To the extent that consumers are present under a traditional copyright framework, they are treated as purchasers of copies who, by paying for access to copyrighted materials, provide just compensation and secure incentives to authors so that authors will invest in further creation.

Copyright law does include, however, a broad notion of consumers-as-authors.[65] Creation is presumed to be incremental—new works are built upon previous works—and the rights of current authors are balanced against those of subsequent authors. Balance is implemented by various doctrines, such as the *idea/expression* dichotomy and *fair use* doctrine. Consumers-as-authors transform preexisting works. They contribute to the

63. The theoretical foundation of copyright emphasizes productive use. From a utilitarian perspective copyright law is a legal mechanism for promoting creativity in the arts and science. It presumes that informational works require expensive investment that could be easily taken by free-riders. Therefore the law seeks to secure continuous incentives to create by granting to authors a set of exclusive rights over their works of authorship.

64. Liu, *supra* note 5, at 402.

65. *Id.* at 405.

productive endeavor by adding something original to preexisting materials.[66] Over the past decade, many commentators have argued that consumers of cultural goods are actually productive users, who are entitled to certain privileges under copyright law.[67] Recently it has been suggested that this category of users should be further expanded to cover instances where a use does not amount to original authorship—what Joseph Liu calls "mini-authorship"[68] or even simply non-transformative copying.[69]

But the *consumer-as-author* perspective has only limited significance for advancing consumer rights because it only covers consumers who make a productive contribution. We ask consumers of informational works to *earn* their entitlement for certain freedoms by proving that their use is productive and adds something new for the benefit of all.[70] Missing from this analysis are all those instances in which consumers make use of works for self-consumption—in other words, for their personal benefit alone.

Therefore, there is room to introduce a third concept of consumers-as-participants who take part in creative processes ("meaning-making" processes).[71] From this perspective, both authors and consumers of information actively participate in advancing the ultimate goal of copyright law, which is promoting progress.

This view is based on the following premises. First, the purpose of copyright law, as defined by the U.S. Constitution, is to "promote the Pro-

---

66. *See generally* Pamela Samuelson, *Challenges in Mapping the Public Domain*, *in* THE FUTURE OF THE PUBLIC DOMAIN 7, 7 (P. Bernt Hugenholtz & Lucie Guibault eds., 2006).

67. *See* Benkler, *supra* note 4, at 568-72; Elkin-Koren, *It's All About Control*, *supra* note 4, at 102.

68. Liu, *supra* note 5, at 415.

69. Litman proposes "to look at the place of readers, listeners, viewers and the general public in copyright through the lens of personal use." Litman, *supra* note 5, at 1878. Cohen proposes the notion of a *situated user*, who "engages cultural goods and artifacts found within the context of her culture through a variety of activities ranging from consumption to creative play." The situated user, she argues, appropriates cultural goods for four primary purposes: *consumption*, *communication*, *self-development*, and *creative play*. Cohen, *supra* note 5, at 370; *see also* Tushnet, *supra* note 5, at 556 ("nontransformative uses" could be a form of self-expression, persuasion, participation and affirmation).

70. *See* Litman, *supra* note 5, at 1919; Liu, *supra* note 5, at 420-21. Tushnet argues that the focus on transformation has left out of the copyright debate important non-transformative copying activities which are also instances of free speech. Tushnet, *supra* note 5, at 555-56.

71. Elkin-Koren, *It's All About Control*, *supra* note 4, at 102; Balkin, *supra* note 57; PAUL DU GAY ET AL., DOING CULTURAL STUDIES: THE STORY OF THE SONY WALKMAN 84-85 (Sage Publications 1997).

gress of Science and the useful Arts . . . ."[72] The Constitution mandates an instrumentalist approach that authorizes the grant of rights to authors only to the extent that it promotes public welfare. *Progress* is served by providing authors with sufficient incentives to invest in producing new works. *Progress* further requires, however, that the public gain access to these works and be able to extract their value.[73] As Jessica Litman reminds us, "copyright law encourages authorship at least as much for the benefit of the people who will read, view, listen to, and experience the works that authors create, as for the advantage of those authors and their distributors."[74]

Copyright law does not simply provide incentives to maximize the number of works produced. In fact, it promotes independent creation. One of the main differences between patent law and copyright law is that while an independent discovery may infringe a patent, an independent creation does not infringe copyright. Copyright law expressly qualifies the rights granted to copyright owners—owners can only protect their works against copying. If a similar or even an identical work is independently created, it does not constitute copyright infringement.[75] An independent creative action, even if it resulted in a work identical to another one that already exists, would merit protection. This suggests that copyright law encourages engagement in the creative process rather than focusing on encouraging the creation of new works.

Second, the creative process involves two means of production: preexisting works and human capital. Human capital is not simply a natural resource of inborn intelligence and creative minds; rather, it requires nurturing in order to flourish. Nurturing is achieved by engagement with existing works—reading books, listening to music, watching a film, or working with computer programs. Consumption, in this sense, cultivates the work-

72. U.S. CONST. art. I, § 8, cl. 8.

73. Niva Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, 12 BERKELEY TECH. L.J. 93, 98-101 (1997); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 326-27 (1989); Julie Cohen, *Copyright and the Perfect Curve*, 53 VAND. L. REV. 1799 (2000).

74. Litman, *supra* note 5, at 1882.

75. Sheldon v. Metro-Goldwyn Pictures Corp., 81 F.2d 49, 54 (2d Cir. 1936), *aff'd*, 309 U.S. 390 (1940); Richard A. Posner, *Intellectual Property: The Law and Economics Approach*, J. ECON. PERSP., Summer 2005, at 57 (2005).

force for further creation: it educates; it stimulates our minds; it expands our understanding of the world around us; it provides inspiration.[76]

Therefore, to promote creativity it is insufficient to provide incentives to authors by empowering them to exclude second-comers. It is also inappropriate to exempt only transformative uses of copyrighted materials. Promoting creativity requires expanding *access* to creative works. Copyright law must therefore expand the balance it strikes between authors and users to cover not only subsequent authors but also simply consumers of cultural goods who might become authors in the future.

Another virtue of consumption of informational works is the creation of a *common cultural language*. Novels, poems, and songs have no meaning outside their interaction with readers and listeners. The *sociology of knowledge* teaches us that cultural artifacts are conditioned by the society in which they are experienced.[77] What we call "consumption" of informational works is never a passive behavior—it is a conversation, or a social activity of interaction. When a reader engages with an artistic expression, she contributes to its meaning. Thus, consumption of informational works, even for one's sole benefit, promotes copyright goals. Consumers are no less a means of production than authors.[78]

This reality of exchange and interaction suggests that in order to promote creativity it is insufficient to simply provide incentives to authors to produce. It is also necessary to expand access to creative works. Access, in this sense, becomes a central means for promoting production, creation, and progress.

B. Consumers-as-Participants

What are the legitimate expectations of consumers-as-participants? What kinds of access to informational works must the law secure in order to facilitate consumer rights? Certainly information consumers should at least enjoy the rights of consumers of GDOs and printer cartridges: the

---

76. Similarly, Tushnet focuses on the free speech value of pure copying, arguing that "ordinary copying serves multiple speech values, from simple access to self-expression to political persuasion . . . ." Tushnet, *supra* note 5, at 546.

77. *See* PIERRE BOURDIEU, DISTINCTION 2 (Routledge, 1984) ("A work of art has a meaning and interest only for someone who possesses the cultural competence, that is, the code, into which it is encoded.").

78. *See* Elkin-Koren, *It's All About Control*, *supra* note 4, at 102. *See also* Tushnet, *supra* note 5, at 566 ("We tend to divide people into 'producers' and 'consumers' of copyrighted works and to devalue the act of consumption. Yet what consumption means in this context is reading, watching, listening, and talking about copyrighted works—all valuable expressive activities that can be extremely important to people, both as individuals and as part of a community.")

freedom to use a copy of the work that they have purchased in conjunction with competing products. However, informational works may raise additional concerns.[79] While the *consumer-as-shopper* perspective emphasizes individualism and instrumentalism consistent with the principles of economic theory, *consumer-as-participant* (the citizen-consumer) explores the ramifications of consumption for citizenship and examines issues such as autonomy, participation, and self-determination.

As pointed out by scholars of cultural studies, the production of culture involves the construction of meaning. The meaning of a cultural artifact is not inherent in the work itself, but arises from the way it is represented through our language and practices.[80] Consumption itself produces meaning. Consumers creatively express themselves through the choices they make on what to consume and how to use their cultural goods.[81] As noted by Paul du Gay, "meanings are not just 'sent' by producers and 'received,' passively, by consumers; rather meanings are actively made in consumption, through the use to which people put these products in their everyday lives."[82]

Participation in the production of culture—the meaning-making process—is a significant political action. It allows self-expression of the citizen-consumer and therefore engages consumers in public discourse. Participation may take the form of actively communicating one's positions, preferences, taste, values, and ideas. It may also involve, however, viewing, reading, listening, absorbing, and making use of content that reflects one's ideas, or those with which an individual identifies.[83] Meaning emerges through a process that involves an interaction with cultural ingredients: watching a film, reading a book, or playing a song. The process is discursive. Not everything that is read or watched is automatically internalized. The way in which cultural artifacts affect meaning is far more

---

79. As Joseph Liu argues, consumers of informational works have interests in autonomy, communication with others, and self-expression that cannot be captured by seeing them either as passive or as new authors. Liu, *supra* note 5 at 399.

80. While the Frankfurt school perceived consumers of cultural goods as passive victims of homogenized mass culture (e.g., THEODORE W. ADORNO, THE CULTURE INDUSTRY: SELECTED ESSAYS ON MASS CULTURE (Routledge, 1991)), others emphasized the role of consumers in the production of meaning, by selection, appropriation, and recontextualization (e.g., JOHN FISKE, UNDERSTANDING POPULAR CULTURE 24 (Routledge, 1991)).

81. For theorists like Mackay the act of consumption is not merely absorption of predetermined symbols, but rather an active process of creative expression. HUGH MACKAY, CONSUMPTION AND EVERYDAY LIFE 9 (The Open University, 1997).

82. du Gay, *supra* note 71, at 5.

83. Elkin-Koren, *It's All About Control, supra* note 4, at 103.

complicated and dynamic. When we are reading a book or watching a film, we reinterpret the themes within our own cognitive framework and our own narratives. The meaning of cultural texts is therefore interactive and depends on the social context in which consumers have acquired the text and integrated it into their lives. Participation by consumers, in these senses, requires a minimal level of freedom in forming one's own reading of the artifact and communicating one's independent voice. From this perspective, DRMs could affect intellectual liberties and freedom.

Consumers of cultural artifacts may need some breathing space to secure their intellectual freedoms. They need space to formulate their own independent reading of, for example, a news report. Consumers must be able to experience the work on their own or share it with others in order to form independent views and identify their own voice.

This breathing space may include the freedom to choose the work one wishes to consume or any part of it (and, likewise, the freedom to ignore or refuse other parts); the freedom to choose where to experience the work and how; the freedom to experience the work in privacy without the fear of surveillance; and the freedom to make one's own reading of the work, to experiment with it, and to share that reading.

Viewed from this perspective, DRMs might have the effect of weakening the role of consumer-as-participant in several ways. DRMs regulate the behavior of consumers, physically preventing consumers from carrying out certain unauthorized actions. Therefore they restrain the freedom of consumers to integrate the cultural artifacts they have purchased into their lives.

DRMs redefine the relationship between consumers and rightholders. The power to determine the terms of use resides entirely in the design of the DRM, which is governed by rightholders. Consumers may not even be aware of some restrictions that apply to them. Some uses will simply not be available. Other functions, such as monitoring, might not be transparent. This may weaken consumer sovereignty and freedom of choice.

DRMs further compromise intellectual freedom. DRMs allow rightholders to govern the format of the work, thereby enabling them to exercise more control over what individuals may do with cultural texts. For instance, DRMs can limit the ability to make changes to and adapt works to reflect consumers' own agendas.[84] They may also prevent consumers from annotating or editing a work for personal use or from making any

84. Compare to practices used by ClearPlay (not involving DRMs) in Clean Flicks of Colo., LLC v. Soderbergh, 433 F. Supp. 2d 1236 (D. Colo. 2006), where the court found that editing films for private viewing violated the copyright of film producers.

other form of transformative use to adapt the work to reflect their private taste or self-expression. Additionally, monitoring access and compromising consumer privacy may further threaten consumer autonomy, creating a chilling effect on the use of informational works.[85]

DRMs can also prevent consumers from making copies for private use, such as for backup purposes or for later consumption. They may additionally limit the ability to copy works for which copyright has expired or the ability of consumers to make copies for the purpose of quoting a work in the course of preparing a new work. Restriction on the use of copies actually turns the transactions of supplying information goods from sales into services that increase the consumer's dependency on vendors and require an ongoing consumer-vendor relationship.[86] Post-purchase control may be ongoing and dynamic and may last long after the content is purchased or even transferred to third parties.[87] To achieve this dependency, all a vendor has to do is make changes in the platform or facilitating codes.

DRMs may further affect the freedom of users to use a work in conjunction with other cultural artifacts or on different platforms. One such restriction relates to the portability of artifacts—the ability to select how a work will be experienced and whether it may be played or delivered on a certain device. Another limitation on user freedom results from restrictions on space-shifting by regional codes, which protect regional market segmentation, embedded in DVD and DVD players. When individuals can

---

85. Julie E. Cohen warns that the anti-circumvention regime established by the DMCA compromises the "breathing space for thought, exploration, and personal growth." Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 577-78 (2003). *See also* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981 (1996). As demonstrated by the Sony BMG case, DRMs could directly threaten consumer privacy by enabling the monitoring of every use of the copyrighted material in real time. A consumer may legitimately expect to use her copy, legally purchased, without any monitoring, as she is free to use any other type of property.

86. Napster's online music store offers its users music "any way you want it," as long as the users keep paying for it over and over again. For a monthly subscription fee, the Napster Unlimited music rental service offers the users the ability to stream and download as much as they like from its entire catalog. However, if the users decide to stop their subscription, Napster's DRM renders the downloaded music unplayable. *See generally* Electronic Frontier Foundation, *The Customer is Always Wrong: A User's Guide to DRM in Online Music*, http://www.eff.org/IP/DRM/guide/ (last visited on July 9, 2007) (outlining the usage restrictions of various digital music services).

87. For instance, Apple reserves the right to change at any time what users are able to do with the music they purchase at the iTunes Music Store. In addition, in order to enjoy the privilege accorded to the user under the first sale doctrine, a user must give the buyer her username and password.

use an artistic work in a context of their choice and adapt it to reflect their own agenda, they are able to contest the original meanings attached to it. Copies detached from their original context could be freely experienced (heard, read, watched) in a variety of ways that would allow individuals to attach new meanings.[88] Information represented digitally—that is, disentangled from physical formats—could be adapted to its surroundings and facilitate a plurality of voices.

The ability to communicate the informational work is another interest of consumers that might be compromised by DRMs. DRMs can limit the resale and distribution of copies, or any form of sharing. Restrictions on sharing with others, excerpting, lending, or reselling could interfere with the ability of consumers to make use of the work's communicative value. This constraint may also reduce the economic value of the work if it cannot be resold as used.

DRMs should not be viewed, however, as simply limiting certain functions and therefore compromising consumer expectations. They also shape our practices by guiding our overall consumer experience with informational works and thereby defining a normative framework.[89] In a DRM/DMCA regime, consumers have no rights in a cultural artifact except as permitted by the DRM. Consumers internalize a variety of practices through the consumption of content controlled by DRMs that might affect their views and values. The way DRMs are designed shapes the consumption of cultural artifacts and affects our attitudes toward informational works and our relationship with them. The more restricted the use is, the less we think of informational works as self-expression, as a form of speech or conversation. We learn to view them as any other commodities. We learn that even though we hold a copy, the work is owned by someone else who exercises absolute control over its use. And we learn to normalize and legitimize these restrictions.

---

88. This was long recognized by Walter Benjamin in his seminal paper on mechanical reproduction. Walter Benjamin, *The Work of Art in the Age of Mechanical Reproduction*, *in* ILLUMINATIONS 217, 221 (Hannah Arendt ed. & Harry Zohn trans., 1968). Benjamin clearly describes this liberating potential of mechanical reproduction of works of art ("One might generalize by saying: the technique of reproduction detaches the reproduced object from the domain of tradition . . . in permitting the reproduction to meet the beholder or listener in his own particular situation, it reactivates the object reproduced.").

89. Theorists of consumption of the Frankfurt School focus on the forms of knowledge and identity which are produced by consumer practices. From this perspective the question is how our experiences as consumers, the terms which were designed for consuming a particular cultural good, affect our relationships with those informational works and with our self-consciousness. *See* KEY CONCEPTS IN CULTURE THEORY 80-83 (Andrew Edgar & Peter Sedgwick eds., Routledge 1999).

Thus, DRMs promote homogeneity. Most users do not challenge DRMs and instead conform to the prescribed use. Consumers cannot change and adapt their own consumptive experiences. Consequently, we should expect little diversity in consumer experiences of informational goods and little room for personal manifestation and choice.

C. Incorporating Consumer Perspectives into Copyright Analysis

Expanding copyright analysis to account for the interests of consumers could help us set limits on the use of DRMs for post-purchase control. Such considerations could be incorporated into copyright analysis in several ways. One way is external, balancing the interests of copyright owners with those of consumers, who are often protected by competition law and consumer protection regulation. Another way is internal, making room for consumers by narrowly applying the bans of the DMCA.[90]

The decisions in *Chamberlain* and *Lexmark* demonstrate how consumer considerations could be included in the courts' analysis of the DMCA for limiting the scope of post-purchase control enabled by DRMs. In *Chamberlain*, the court outlined a six-part test to determine whether a particular device violates Section 1201(a)(2):

> (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commer-

90. Others believe that users' interests call for a reconsideration of copyright law's fundamental mechanisms. Cohen argues:

> Scholars and policy makers should ask how much latitude the situated user needs to perform her functions most effectively, and how the entitlement structure of copyright law might change to accommodate that need. In particular, they should be prepared to ask whether the situated user is well served by the current copyright system of broad rights and narrow, limited exemptions, or whether she would be better served by a system that limits the rights of copyright owners more narrowly in the first instance. This is not, to use Michael Madison's terminology, a choice to emphasize the 'primacy of the actor' over the 'primacy of the pattern.' The choice is *not either/or, but both/and; it is actors within contexts who produce 'progress.'*

Cohen, *supra* note 5, at 374 (emphasis added) (citations omitted).

> cial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.[91]

This test reflects the court's opinion that the anti-circumvention provisions of section 1201 did not establish a new property right, but rather provided copyright owners with "new ways to secure their property."[92] Therefore, an illegal circumvention must be "reasonably related to protected rights."[93] The court found that section 1201 "prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners."[94] The central issue in the *Chamberlain* construction of the DMCA is the linkage between *access* and *protection*. Not every access is prohibited, but only that which is illegitimate. Accordingly, to make a successful claim under the DMCA, a plaintiff must prove a reasonable link between access facilitated by the circumvention device and a violation of traditional copyrights.[95] The court reasoned that: "[w]hile such a rule of reason may create some uncertainty and consume some judicial resources, it is the only meaningful reading of the statute. Congress attempted to balance the legitimate interest of copyright owners with those of consumers of copyrighted products. The courtsmust adhere to the language that Congress enacted to determine how it attempted to achieve that balance."[96]

The *Chamberlain* decision introduced two key developments regarding consumer protection under the DMCA: recognizing consumer interests and defining the scope of consumer rights. First, the court explicitly recognized that consumers have legitimate expectations in products containing copyrighted works and defined these expectations as an integral part of

---

91. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

92. *Id.* at 1194.

93. *Id.* at 1195. The court emphasized the difference between defendants whose accused products enable illegal copying, and those, like the defendant in the *Chamberlain* case, whose products enable only legitimate uses of copyrighted software. *Id.* at 1198. Thus, the court distinguished other cases previously decided under the DMCA, in which the defendant was found liable, concluding that "the access alleged in all three cases was intertwined with a protected right." *Id.* at 1199.

94. *Id.* at 1202. The Federal Circuit decision was criticized by some commentators for developing an independent doctrine of "fair access" that is not traceable to the statute. *See, e.g.,* Efroni, *supra* note 23, at 136-41. In fact, however, the court's reasoning is well grounded in the legislative history and public policy underlying the DMCA. The court also explained how this holding is consistent with previous case law interpreting the DMCA. *Chamberlain,* 381 F.3d at 1201-02.

95. *Chamberlain*, 381 F.3d at 1195.

96. *Id.* (citation omitted).

the balance reflected by the law. Citing the legislative history,[97] the court held that "[t]he DMCA balances the legitimate interests of copyright owners with those of consumers of copyrighted products."[98] In denying Chamberlain's claim that the "DMCA overrode all pre-existing consumer expectations about the legitimate uses of products containing copyrighted embedded software,"[99] the court held that "the DMCA emphatically did not 'fundamentally alter' the legal landscape governing the reasonable expectations of consumers or competitors."[100]

Second, the court defined the scope of legitimate consumer expectations, explicitly upholding the rights of consumers who purchased a copy to use that copy. Purchasers of copies are entitled to use them, as long as they do not violate any of the exclusive rights of copyright owners:

> *Copyright law itself authorizes the public to make certain uses of copyrighted materials.* Consumers who purchased a product containing a copy of embedded software have the *inherent legal right to use* that copy of the software. What the law authorizes Chamberlain cannot revoke.[101]

Furthermore, aware of the ease with which copyright owners could place restrictions by a combination of contractual terms and technological measures, the court held that "[the] DMCA cannot allow Chamberlain to retract the most fundamental right that the Copyright Act grants consumers: the right to use the copy of Chamberlain's embedded software that they purchased."[102]

The Federal Circuit further implied that consumers have a legitimate interest in using their products in conjunction with competing products. The court rejected plaintiff's interpretation of the statute, holding that it leads to absurd results. The plaintiff's construction which separates *access* from *protection* "would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial 'encryption' scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with

97. *Id.* at 1203 (citing H.R. REP. NO. 105-551, at 26 (1998)).

98. *Chamberlain,* 381 F.3d at 1203.

99. *Id.* at 1193-94.

100. *Id.* at 1194.

101. *Id.* at 1202 (emphasis added).

102. *Id.* at 1203.

competing products."[103] This outcome, the court held, would be contrary to antitrust laws and the doctrine of copyright misuse.[104]

It follows that consumers who own copies of a copyrighted work are entitled to some rights, such as the right to make use of the copies they purchased. It may also follow that circumvention would not be considered a violation of the DMCA if it only enables a legitimate use of a copy, such as using software with a different device or playing music on different platforms.

One should note, at the outset, that copyright law does not grant consumers any rights in copies—at least not explicitly. Section 106 of the Copyright Act defines the set of exclusive rights granted to copyright owners,[105] which cover only the intangible copyrighted work and in most cases do not affect rights in tangible copies.[106] In fact, copyright law distinguishes between the work that is copyrighted and its tangible copies, which are left outside the scope of copyright law.[107] Therefore, when the court refers to the rights granted to consumers under copyright law, it presumes that anything that is not explicitly prohibited by copyright law is something that consumers are free to do.[108] Furthermore, according to the Federal Circuit, a consumer does not need to acquire authorization to do anything that she is already free to do. If consumers are free to use their GDOs with any compatible device, it is the plaintiff's burden to demonstrate that they have done so without authority.

Taking a similar "consumer-friendly" approach, the court in *Lexmark*[109] denied Lexmark's claim under the DMCA, where it sought to prevent an aftermarket for printer cartridges by using an authentication sequence. Lexmark embedded an authentication sequence in the Printer En-

---

103. *Id.* at 1201.

104. *Id.*

105. 17 U.S.C. § 106 (2000).

106. Section 202 provides that "[o]wnership of a copyright, or of any of the exclusive rights under a copyright, is distinct from ownership of any material object in which the work is embodied." *Id.* § 202. One major exception is the exclusive right to distribute copies to the public. *Id.* § 106(3). This right is limited by the first sale doctrine, codified in section 109, which provides that notwithstanding section 106(3), "the owner of a particular copy or phonorecord lawfully made under this title . . . is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord." *Id.* § 109(a).

107. *Chamberlain,* 381 F.3d at 1202.

108. In Hohfeldian terminology, this is a right in the sense of privilege, namely the freedom from any limiting duties.

109. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 550-51 (6th Cir. 2003).

gine Program, which enabled the loading of authenticated toner cartridges only.[110] The court denied Lexmark's claim under the DMCA since the sequence that was allegedly circumvented did not "effectively control access" to copyrighted materials.[111] It only protected the functionality of the program, which was held by the court to be an *unprotected idea*, rather than an expression protected under copyright law.[112] Therefore, the court concluded that the defendant was free to circumvent.

The construction of the DMCA in cases such as *Chamberlain* and *Lexmark* establishes the basis for defining consumer liberties under copyright: consumers are free to use a copy of the work in ways that cannot be unilaterally overridden by copyright owners.[113] This reading of the DMCA confines DRMs and the anti-circumvention regime to its appropriate size—DRMs cannot allow owners to protect more than what copyright entitles them to.

IV. WHAT COULD BE GAINED BY THE CONSUMER-AS-PARTICIPANT PERSPECTIVE?

Consumer protection discourse, as distinct from users discourse, could add a new dimension to the copyright analysis. Conceiving of users of copyrighted works as consumers in the same sense as consumers of tangible goods better captures many of the conflicts between copyright owners and the recipients of copyrighted works. In modern times, creation often

---

110. *Id.* at 530.

111. *Id.* at 546-47.

112. *Id.* at 549. Jane Ginsburg distinguishes between the rationales in these two decisions: "Where the *Lexmark* court focused on the 'work' that is the object of the access control, the court in *Chamberlain v Skylink* addressed the *purpose* of the access that the technological measure controls." Ginsburg, *supra* note 24, at 5.

113. The court held that Chamberlain was not entitled to prohibit legitimate purchasers of its embedded software from accessing the software by using it. The court explained:

> Such an entitlement, would go far beyond the idea that the DMCA allows copyright owner to prohibit "fair use . . . as well as foul." Chamberlain's proposed construction would allow copyright owners to prohibit exclusively fair uses even in the absence of any feared foul use. It would therefore allow any copyright owner, through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work . . . . Again, this implication contradicts Section 1201(c) (1) directly.

Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1202 (Fed. Cir. 2004) (citation omitted).

involves mass production and distribution of copies embodying the work. Production and distribution is often organized by large corporations. Consumers of copies of mass-produced content (e.g., DVD movies, music, television shows) suffer from the same disparities of power, asymmetric information, and systematic disadvantage experienced by consumers of mass-produced tangible goods.

Moreover, information consumers suffer from further vulnerabilities that require even stronger protection. The intimate tie of informational works to consumers' minds makes disparities of power and control even more crucial. DRMs that monitor the consumption of copyrighted materials may weaken consumer sovereignty, threaten individual autonomy, and chill intellectual freedom. These consequences might compromise the goals of copyright law. As explained above[114], traditional copyright analysis often reflects a balance between authors and subsequent authors (i.e. "users"). Within the productive framework of copyright law, consumers who become subsequent authors are considered active contributors to the overall goal of promoting progress. However, this productive framework neglects the interests and contributions of consumers who do not become subsequent authors but, nevertheless, participate in the meaning-making processes. The notion of *consumers-as-participants* highlights the legitimate interests of information consumers, which may deserve protection, and provides a perspective that could help identify additional uses that should be privileged vis-à-vis the claims of copyright owners.

Incorporating a *consumer-as-participant* perspective into copyright analysis has advantages that render it more useful than a legal strategy that relies exclusively on consumer protection laws.[115] The first advantage is that the notion of *consumers-as-participants* may add legitimacy to users' demands. The balance between owners and users often tilts toward owners, based upon the notion that authors generate new works out of thin air over which users have no claim. However, when users are cast as consumers of goods mass-produced by a corporation, their demands might enjoy more legitimacy because, under such a paradigm, consumer expectations in purchased copies would be protected to the same extent consumers are protected in other contexts.

---

114. *See supra* notes 64-68 and accompanying text.

115. One concern, however, is that introducing consumer discourse to informational works would deteriorate the status of consumers of informational works and weaken their rights.

A second advantage of incorporating a consumer perspective into copyright law arises from the need to adjust the tenets of consumer protection to the information age.

On the one hand, introducing consumers into copyright discourse may better capture the reality of modern information markets and protect consumers of mass-produced content from the same disparities of power and asymmetric information suffered by consumers of tangible goods. On the other hand, the premises of consumer protection doctrine, which are rooted in the industrial revolution, may no longer fit the digital environment, as online social networks grow in popularity and scope and as consumers increasingly drive both the production and distribution of new content and applications. The emergence of Web 2.0 and user-generated content causes the roles of consumer and producer to converge. Digital networks facilitate collaborative production of content based on non-hierarchical voluntary participation.[116] Users are able to share their own content (i.e., news reports, opinions, pictures, movies, and music) as well as form social networks that collaborate in producing information goods, such as computer programs (i.e., Linux), encyclopedias (i.e. Wikipedia), and other content. Consumers of content also actively participate in making content available to others, thus undertaking the roles of publishers and distributors.[117] Consequently, recognizing the virtues of *consumption-as-participation* in this environment is especially important to ensure that consumers can use information products to express themselves by using cultural goods in ways that would reflect their own agendas. The new opportunities for participation make it important to guarantee that creativity can emerge at all levels.

Furthermore, interpreting the constitutional purpose of copyright law in light of these emerging opportunities may entail adjustment of our legal institutions that promote progress. Copyright law ostensibly facilitates a market in copyrighted materials, but user-generated content emerges outside traditional market mechanisms. Thus, promoting *progress* takes on a new meaning in the Web 2.0 environment. The goal of progress is no longer advanced solely by providing incentives to industries that engage in mass production of copies served to consumers. True progress is increasingly achieved by wide participation of individuals and collaborative communities. At the same time, however, there is an increasing danger

116. YOCHAI BENKLER, THE WEALTH OF NETWORKS 121 (Yale University Press 2006).

117. Jessica Litman, *Sharing and Stealing*, 37 HASTINGS COMM. & ENT. L.J. 1 (2004).

that the robust protection provided by the DMCA/DRM regime could become widespread and be employed by individual users to enforce restrictions on access to their works. Such widespread use of DRMs may seriously threaten access to content. Consumer protection laws, however, could hardly mediate such restrictive use of DRMs in transactions among consumers. It is therefore necessary to conceptualize consumers' right of access to cultural goods within the conceptual framework of copyright policy. Access rights would be justifiable as long as they are necessary for securing the legitimate interests of *consumers-as-participants*.

Finally, the ascendancy of user-generated content requires reexamining consumer protection doctrine, perhaps to the extent of adjusting fundamental consumer protection principles. With adjustment, the consumer perspective could remain constructive for addressing the rights of information consumers in the online environment. User-generated content is often provided on commercial platforms where users generate and distribute their own content while simultaneously consuming content and services provided by the facility.[118] These new methods of experiencing media are coordinated and facilitated by new intermediaries such as search engines (e.g., Google and Yahoo), distribution platforms (e.g., YouTube and Flickr), social networks (e.g., MySpace and Friendster), and virtual worlds (e.g., Second Life).[119] To secure the interests of information consumers on these platforms, we need to better understand the parameters that affect access on these platforms as well as the way that access to information on such platforms is designed.

The third advantage of incorporating a *consumer-as-participant* perspective into copyright is its impact on the market dimension and issues of price and competition. Paying attention to consumers may allow courts to adequately address the use of DRMs for anticompetitive strategies. Tying hardware and content together makes it difficult for consumers to switch to a different platform. These barriers to competition may further increase prices and harm consumer welfare.[120] When viewed as simply a copyright

118. WORKING PARTY ON THE INFORMATION ECONOMY, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, PARTICIPATIVE WEB: USER-CREATED CONTENT (2007), *available at* http://www.oecd.org/dataoecd/57/14/38393115.pdf.

119. *Id.* at 15-20.

120. *See* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1201 (Fed. Cir. 2004). The court observed:

> In a similar vein, Chamberlain's proposed construction would allow any manufacturer of any product to . . . gain the right to restrict consumers' rights to use its products in conjunction with competing products. In other words, Chamberlain's construction of the DMCA would

dispute, claims against anticompetitive practices are more difficult to make because copyright law by definition creates a monopoly and therefore, by its very nature, impedes competition. The consumer discourse highlights the market dimensions of copyright policy and the risks created by copyright abuse.[121]

Fourth, incorporating consumer perspectives under copyright may create a political advantage. The interests of recipients of cultural goods often suffer from under-representation in legislative processes. Copyright owners are a small, homogeneous, well-organized, and well-financed group of repeat players, representing the entertainment, software, and publishing industries. Recipients of copyrighted materials, by contrast, are represented by the general public. That is a heterogeneous group, consisting of consumers, nonprofit and for-profit users, subsequent authors, and potential competitors, representing dispersed interests. Therefore, while all major copyright industries have developed effective lobbying arms over the past decades (e.g., RIAA, MPAA), most consumers have not even been aware of the implications of copyright reforms. This basic asymmetry resulted in extensive legislation towards stronger and expanded copyrights.[122] The consumer perspective could help recipients of cultural goods articulate their interests more effectively.[123]

> allow virtually any company to attempt to leverage its sales into aftermarket monopolies—a practice that both the antitrust laws, and the doctrine of copyright misuse, normally prohibit.

Id. (citations omitted).

121. Antitrust laws have failed so far to provide a remedy. In Europe, VirginMega, which runs an online music service, argued in a complaint before the French Competition Council that Apple's refusal to allow access to its DRM was an abuse of dominant position. The Competition Council held that an abuse of dominant position occurs only when denying access to an essential facility. The Council held that Apple had no obligation to grant access to its FairPlay DRM solution, since FairPlay is not essential for the development of music download platforms. Among other things, the council noted that songs that are protected by other DRMs could still be played on the iPod if consumers burned it on to a CD and re-encoded it in unprotected MP3 format. Conseil de la Concurrence, Décision n° 04-D-54 du 9 novembre 2004 [Competition Council, Decision 04-D-54, Nov. 9, 2004], *available at* http://www.conseil-concurrence.fr/pdf/avis/04d54.pdf.

122. For a recent analysis of public choice and intellectual property see WILLIAM M. LANDES & RICHARD A. POSNER, THE POLITICAL ECONOMY OF INTELLECTUAL PROPERTY LAW (American Enterprise Institute-Brookings Joint Center for Regulatory Studies, 2004).

123. European consumer protection organizations undertook a leading role in advancing the rights of consumers of copyrighted materials. *See European Consumer Protection Organizations Join Forces Against iTunes,* Jan. 23, 2007, http://www.heise.de/english/newsticker/news/84138 (last visited Aug. 6, 2007). For a discussion of political action

The consumer protection agenda could help copyright users get organized, taking advantage of existing NGOs and consumer organizations, and relying on international institutions to advance consumer-oriented agendas.

A final reason that the *consumer-as-participant* perspective could be a better strategy for securing consumer interests is that the framework provides a practical strategy for addressing consumer rights under the DMCA. In particular, such a perspective would limit the ban on circumvention to the boundaries of copyrights, leaving consumers with the right to do whatever copyright itself allows them to do. Once we conceptualize consumer interests in terms of copyright goals and public welfare, we can offer consumers a more effective remedy under the DMCA: *self-help.*

Consumers, and others on their behalf, could simply circumvent DRM that violates their freedoms. Or, to rephrase the language of the court in *Chamberlain*: *consumers-as-participants* have rights under copyright law with which DRM cannot interfere, and, to the extent that it does so, they are free to circumvent it.

---

and resistance to the expansion of intellectual property, see DEBORA HALBERT, RESISTING INTELLECTUAL PROPERTY LAW (Routledge, 2005).

THE MAGNIFICENCE OF THE DISASTER: RECONSTRUCTING THE SONY BMG ROOTKIT INCIDENT

By Deirdre K. Mulligan[†] *& Aaron K. Perzanowski*[‡‡]

I. **INTRODUCTION** 1158

II. **UNDISCLOSED HARM AND EXTERNALITIES** 1166

A. DIRECT HARM TO SONY BMG, ITS ARTISTS, AND ITS CUSTOMERS 1166
B. EXTERNALITIES ARISING FROM THE ROOTKIT INCIDENT 1171

III. **MARKET INFLUENCES** 1177

A. THE ROOTKIT INCIDENT AS MISTAKE 1178
B. THE ROOTKIT INCIDENT AS CALCULATED RISK 1181

IV. **THE ROLE OF TECHNOLOGY** 1188

A. TECHNOLOGY AS ENCOURAGEMENT 1189

---

† Clinical Professor of Law; Director, Samuelson Law, Technology & Public Policy Clinic; Director, Clinical Program, University of California, Berkeley School of Law (Boalt Hall).

‡‡ Associate, Fenwick & West LLP; J.D., University of California, Berkeley School of Law (Boalt Hall), 2006.

Much appreciation to Pamela Samuelson, Chris Hoofnagle, Fred B. Schneider, Matt Blaze, Edward Felten, Aaron Burstein, Ka-Ping Yee, Joseph Lorenzo Hall, Nathaniel Good, Fred von Lohmann, Jennifer M. Urban, Jack I. Lerner, the participants at the Copyright, DRM Technologies, and Consumer Protection Conference, and the TRUST (The Team for Research in Ubiquitous Secure Technology) Industrial Advisory Board members for insight, comment, and discussion; Edward Felten and J. Alex Halderman for giving us the opportunity to advise them on legal aspects of their research; Sara Adibisedeh, Azra Medjedovic, and Brian W. Carver for their assistance in providing that advice; Victoria Bassetti and others in industry for answering questions and providing helpful direction; and Sarala V. Nagala and Rebecca Henshaw for their able research. This paper would not have been possible without the support for interdisciplinary research provided by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422). Finally, the authors wish to thank Rebecca M. Fisher for providing the inspiration for the title of this article.

1. *The PC as Playback Device* 1189
2. *The Lack of an Encrypted Format* 1192
B. TECHNOLOGY AS ENABLEMENT 1194
V. **EXISTING LAW AND SKEWED INCENTIVES** 1196
A. THE DMCA'S VEIL OF SECRECY 1198
B. THE INSUFFICIENCY OF CONSENT 1205
C. DEFINING DECEPTIVE AND UNFAIR ACTS: THE PROBLEM WITH SOFTWARE DOWNLOADS AND PRIVACY 1211
VI. **REALIGNING SKEWED INCENTIVES** 1218
A. ENABLING SECURITY RESEARCH AND SELF-HELP THROUGH A STATUTORY EXEMPTION TO THE DMCA 1221
B. DEVELOPING MEANINGFUL NOTICE AND CONSENT MECHANISMS THROUGH INTERDISCIPLINARY INSIGHT AND AGENCY ACTION 1224
VII. **CONCLUSION** 1231

I. INTRODUCTION

Late in 2005, as many as two million[1] computer users learned that software unknowingly installed on their machines effectively ceded control of their computers and data to any enterprising hacker with the necessary ill intent. This software tool, known as a rootkit, enabled a host of attacks on individual users and both private and public network infrastructure. But the rootkit, a tool rarely employed by legitimate software developers,[2] was not installed by a virus attached to unscanned e-mails, nor was it bundled with adware developed by a disreputable vendor. It was instead distributed by Sony BMG Music Entertainment (Sony BMG), the world's second largest record label,[3] on millions of Compact Discs (CDs) sold to an unsuspecting public. The unwitting recipients of this software, Sony BMG's own customers, did no more than attempt to listen to lawfully purchased music on their computers.

---

1. Jefferson Graham, *Sony to Pull Controversial CDs, Offer Swap*, USA TODAY, Nov. 15, 2005, at 1B; Tom Zeller Jr., *Sony BMG Stirs a Debate Over Software Used to Guard Content*, N.Y. TIMES, Nov. 14, 2005, at C1.

2. Rootkits have been used in some instances by anti-virus software developers to protect their software from attack, but this incorporation of a rootkit into otherwise legitimate software sparked significant debate. *See* MCAFEE, ROOTKITS, PART 1 OF 3: THE GROWING THREAT (2006), http://download.nai.com/products/mcafee-avert/WhitePapers/AKapoor_Rootkits1.pdf.

3. Bertelsmann.com, BMG—A Passion for Music, http://www.bertelsmann.com/bertelsmann_corp/wms41/bm/index.php?ci=26&language=2 (last visited Sept. 6, 2007).

By the time the Sony BMG rootkit found its way to store shelves, CD-based copy protection schemes were nothing new. A variety of protection measures had been introduced on previous major label releases.[4] Although they differed in technological detail, these measures all aimed to disable or limit the ability of customers to access and copy music contained on CDs.

XCP, a CD-based protection measure developed by First4Internet and distributed by Sony BMG,[5] initially appeared to be no different than its predecessors. XCP created generally unwanted and unexpected restrictions on the ability to use lawfully purchased CDs. But in October of 2005, after CDs protected by XCP had been on the market for several months, computer engineer and security expert Mark Russinovich discovered that XCP incorporated a rootkit.[6] While Russinovich was not the first security researcher to uncover problems with Sony BMG's protection measures, he was the first to publicly disclose the presence of the rootkit because of the pall hanging over research in this field.[7] A blog post authored by Russinovich, and the media response it prompted,[8] alerted the public to the presence of the rootkit, offering the first glimpses into the potential security disaster enabled by Sony BMG's DRM.

As the public learned in the wake of Russinovich's disclosure, rootkits are software tools, frequently employed by developers of malicious soft-

---

4. *See, e.g.*, J. ALEX HALDERMAN, PRINCETON UNIVERSITY, ANALYSIS OF THE MEDIAMAX CD3 COPY-PREVENTION SYSTEM 1 (2003), ftp://ftp.cs.princeton.edu/techreports/2003/679.pdf; Evan Hansen, *Celine Dion Disc Could Crash European PCs*, ZDNET.CO.UK, Apr. 5, 2002, http://news.zdnet.co.uk/internet/0,1000000097,2107848,00.htm; John Leyden, *Marker Pens, Sticky Tape Crack Music CD Protection*, THE REGISTER, May 14, 2002, http://www.theregister.co.uk/2002/05/14/marker_pens_sticky_tape_crack/ (discussing how a Celine Dion CD can prevent Macs from rebooting); Tony Smith, *BMG to Replace Anti-Rip Natalie Imbruglia CDs*, THE REGISTER, Nov. 19, 2001, http://www.theregister.co.uk/2001/11/19/bmg_to_replace_antirip_natalie/.

5. The other three major labels—Universal Music Group, Warner Music Group, and EMI—were also First4Internet customers and had included XCP on certain prerelease materials. *See Sony Tests Technology to Limit CD Burning*, CNET.CO.UK, June 1, 2005, http://news.cnet.co.uk/digitalmusic/0,39029666,39189658,00.htm.

6. Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx (Oct. 31, 2005, 11:04 PST).

7. *See infra* Part II.

8. *See* Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx (Oct. 31, 2005, 11:04 PST); Paul F. Roberts, *Sony BMG Hacking Into CD Buyers' Computers*, FOXNEWS.COM, Nov. 03, 2005, http://www.foxnews.com/story/0,2933,174334,00.html; Francis Till, *Sony Plants Secret Controls on PCs*, NAT'L BUS. REV., Nov. 3, 2005, http://www.nbr.co.nz/home/column_article.asp?id=13371&cid=3&cname=Technology.

ware (malware),[9] that allow programmers to cloak files and processes, effectively hiding their existence and operation from both a computer's user and the machine's operating system.[10] These cloaking devices can facilitate any number of attacks on individual computers including coordinated offenses against websites, computer networks, and the internet itself. Once installed, a rootkit can be used to hide any code, regardless of its author's original purpose. As such, a hacker's ambition and imagination serve as the primary constraints on the destructive effects rootkits enable.[11]

While Sony BMG's customers first became aware of the dangers posed by the rootkit through media reports following Russinovich's October 31 announcement, the company was on notice that its product contained a rootkit, at the very least, four weeks earlier.[12] Finnish anti-virus software developer F-Secure contacted Sony BMG on October 4, 2005, alerting it to the presence of the rootkit.[13] Of course, First4Internet, as the developer that chose to incorporate the rootkit into its design, necessarily knew of its presence from the outset.

---

9. "Malware," short for malicious software, is a catch-all term that refers to any software designed to cause damage to a single computer, server, or computer network, and includes spyware, viruses, and other varieties of harmful software. Robert Moir, *Defining Malware: FAQ,* Oct. 1, 2003, http://www.microsoft.com/technet/security/alerts/info/malware.mspx; *see also* Adam Baratz & Charles McLaughlin, *Malware: What is It and How to Prevent It*, ARS TECHNICA, Nov. 11, 2004, http://arstechnica.com/articles/paedia/malware.ars.

10. GREG HOGLUND & JAMES BUTLER, ROOTKITS: SUBVERTING THE WINDOWS KERNEL 4, 8-10 (Addison-Wesley ed., 2005). Within the computer security community, there was some debate over the proper classification of XCP. Some deemed XCP a rootkit, while others applied the more ambiguous label of Potentially Unwanted Program. *See* MCAFEE, *supra* note 2, at 3.

11. Hackers could exploit the cloaking capabilities of the XCP rootkit simply by adding the prefix "sys" to the name of any files they chose to obscure. J. Alex Halderman & Edward W. Felten, *Lessons from the Sony CD DRM Episode*, *in* USENIX ASS'N, PROCEEDINGS OF THE 15TH USENIX SECURITY SYMPOSIUM 77, 18 (2006), *available at* http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf (updated version).

12. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=937 (Nov. 30, 2005, 06:41 EST).

13. Steve Hamm, *Sony BMG's Costly Silence*, BUS. WK., Nov. 29, 2005, http://www.businessweek.com/technology/content/nov2005/tc20051129_938966.htm. In fact, according to Thomas Hesse, President of Sony BMG's Global Digital Business group, the alert from F-Secure was seen as a "routine matter" and "did not suggest that this software was anything but benign." *Id.* Even after F-Secure explained that the rootkit posed a major security risk, Sony BMG "didn't seem inclined to do anything about the CDs that were already in circulation" and "wanted to keep the problem quiet." *Id.*

Although Sony BMG claimed it was taking steps to address the issue,[14] it took no discernible action until Russinovich made the threat posed by the software a matter of public knowledge. And even then, Sony BMG attempted to downplay the importance of the rootkit discovery. As Thomas Hesse, Sony BMG's President of Global Digital Business, rhetorically asked, "Most people, I think, don't even know what a rootkit is, so why should they care about it?"[15]

Subsequently, in an attempt to mollify customers who had already purchased the infected CDs, Sony BMG offered tools to uninstall XCP.[16] But, as discussed *infra*, those tools did more harm than good.[17] In order to stem the tide of public outcry and potentially mitigate further damages, Sony BMG finally announced in mid-November its intention to recall the millions of XCP-infected CDs that remained in the retail chain.[18]

But even before the XCP recall was announced, the focus of scrutiny began to shift to Sony BMG's other preferred technological protection measure, SunnComm's MediaMax software. Unlike XCP, MediaMax did not employ a rootkit, but it did, however, introduce other significant security vulnerabilities.

MediaMax enabled a dangerous privilege escalation.[19] When installed, MediaMax created a directory called "SunnComm Shared" on the user's hard drive.[20] MediaMax set file permissions for this directory and its contents that enabled any user of the computer, whether she had administrator privileges or not, to read, modify, or delete the contents of the directory.[21] These permissions enabled a guest or remote user to replace the Media-

---

14. *Id.*

15. Neda Ulaby, *Sony Music CDs Under Fire from Privacy Advocates* (National Public Radio Program broadcast Nov. 4, 2005), *available at* http://www.npr.org/templates/story/story.php?storyId=4989260.

16. *Id.*

17. *See infra* notes 40-42 and accompanying text.

18. Tom Zeller, Jr., *CD's Recalled for Posing Risk to PC's*, N.Y. TIMES, Nov. 16, 2005, at C1.

19. *See* Wikipedia, Privilege Escalation, http://en.wikipedia.org/wiki/Privilege_escalation (last modified July 26, 2007) ("Privilege escalation is the act of exploiting a bug in an application to gain access to resources which normally would have been protected from an application or user. The result is that the application performs actions with a higher security context than intended by the application developer or system administrator.").

20. Jesse Burns & Alex Stamos, Information Security Partners, Media Max Access Control Vulnerability 1 (2005), http://www.eff.org/IP/DRM/Sony-BMG/MediaMaxVulnerabilityReport.pdf.

21. *Id.*

Max files with malicious code, either intentionally or inadvertently. When a user with administrator privileges later inserted a MediaMax disc, that malicious code would be activated, triggering all manner of potential attacks.[22] When SunnComm released a patch to address this threat, it created vulnerabilities similar to those caused by the XCP uninstall tool.[23]

Second and more fundamentally, MediaMax requires a user to possess administrator privileges simply to listen to a CD.[24] Requiring the use of an administrator account for such mundane purposes is both "unnecessary and dangerous."[25] Further compounding the security vulnerabilities created by MediaMax, one component of the software, a kernel process capable of altering any aspect of the system, is loaded into memory at all times, regardless of the presence of a MediaMax CD.[26]

Although the technological source of the security threats introduced by XCP and MediaMax differed, as researchers soon discovered, the creators of both protection measures exhibited other behavior typically associated with the purveyors of spyware. For example, the software End User License Agreements (EULAs) were rife with overreaching terms.[27] More troublingly, some of the EULA terms were simply untrue. The EULAs professed that the software would collect no information about the user or her computer,[28] as did assurances offered by SunnComm and Sony BMG on their websites[29] and in the press.[30] But despite the obvious sensitivity to

---

22. *Id* at 5.

23. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=942 (Dec. 7, 2005, 10:33 EST). The original patch was later replaced with one that avoided these problems. *Id.*

24. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=934 (Nov. 22, 2005, 03:51 EST).

25. *Id.*

26. *Id.*

27. The Sony BMG EULA terminated the rights of consumers if, *inter alia*, the original CD was stolen or the user filed for bankruptcy. The EULA also prohibited users from using the CD on an office computer, limited Sony BMG's liability to $5.00, and permitted Sony BMG to install and use backdoors in the copy protection software or media player to enforce its rights at any time, without notice. *See* Fred von Lohmann, *Now the Legalese Rootkit: Sony-BMG's EULA*, DEEP LINKS, Nov. 9, 2005, http://www.eff.org/deeplinks/archives/004145.php.

28. *See infra* text accompanying note 214.

29. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST).

30. *See, e.g.*, *Sony Sued Over Controversial CDs*, BBC NEWS, Nov. 22, 2005, http://news.bbc.co.uk/2/hi/technology/4459620.stm; Carrie Kirby, *Sony Gets an Earful Over CD Software; Program to Block Music Piracy Prompts Privacy, Security Worries*, S.F. CHRON., Nov. 11, 2005, at A1; Bruce Schneier, *Real Story of the Rogue Rootkit*,

privacy concerns reflected in the public statements issued by these companies,[31] the behavior of their protection measures told a different story. Each time a user listened to a MediaMax or XCP-protected CD, data were collected and transmitted to Sony BMG that included the user's IP address and a code corresponding to the particular CD title.[32]

Even if a user declined the Sony BMG EULA, thereby forgoing the ability to access the CD on a computer,[33] components of the MediaMax software were loaded temporarily onto the user's machine.[34] One component—a device driver that interfered with the ability of the computer's CD-ROM drive to copy data—was often permanently installed despite the computer owner's explicit refusal of the EULA terms.[35] This driver was loaded as part of the Windows kernel and could potentially "control virtually any aspect of the computer's operation."[36]

Compounding these concerns, both First4Internet and SunnComm, like many malware vendors, initially failed to provide users with an uninstaller to remove their software in its entirety.[37] After news of the XCP

WIRED, Nov. 17, 2005, http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601.

31. This sensitivity was likely due, in part, to earlier controversy over media players that report users' listening and viewing habits. After a security consultant discovered that the RealJukebox transmitted to RealNetworks a unique code corresponding to each customer and the names of the CDs to which each user listened, Real quickly issued a patch that disabled the transmission of this data. *See* Stuart J. Johnston, *RealPrivacy in the New Millennium?*, PCWORLD, Dec. 17, 1999, http://www.pcworld.com/article/id,14419-page,1/article.html.

32. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=923 (Nov. 10, 2005, 08:25 EST); Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx (Nov. 4, 2005 12:04 PST); posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST). At least in part, this software served a fairly benign function—namely, to update images and lyrics displayed while users listened to the CD.

33. If a user declined to accept the EULA, the CD was automatically ejected. Halderman & Felten, *supra* note 11, at 6.

34. *Id.* at 7; Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005 12:30 EST); Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005 14:23 EST).

35. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005 14:23 EST).

36. *Id.*

37. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=923 (Nov. 10, 2005, 08:25 EST); Halderman & Felten, *supra* note 11, at

rootkit broke, Sony BMG initially offered a software update that, in its words, "remove[d] the cloaking technology component that has been recently discussed in a number of articles."[38] Given the size of the update and its creation of new files on the user's computer, some suggested that the update simply replaced one cloaking mechanism with another.[39]

Once mounting public pressure demanded that uninstallers be provided, Sony BMG required customers to endure a Byzantine series of webpages, e-mails, and downloads before finally ridding themselves of XCP.[40] But Sony BMG's missteps were not limited to a lack of transparency and convenience. The web-based XCP uninstaller created security threats equal in magnitude to the rootkit it was intended to eliminate, permitting malicious code embedded in any website to attack unsuspecting customers who took steps to protect their machines by uninstalling the rootkit.[41] Days later, when SunnComm announced a web-based uninstaller for its Media Max DRM, it suffered from a nearly identical flaw.[42]

The temptation to write off Sony BMG's long and unfortunate series of missteps as a display of utter disregard, or even contempt, for user security and privacy is a strong one. Although the truth likely contains some traces of these simple narratives, any reconstruction of the rootkit incident that approaches reality reveals a more complicated story. Casting Sony BMG as a hapless licensee of flawed protection measures developed by irresponsible third party vendors does not shed any light on the possible

---

14; Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST).

38. Sony BMG Music Entertainment, Software Updates/Plug-ins (Nov. 7, 2005), http://cp.sonybmg.com/xcp/english/updates.html, *available at* http://web.archive.org/web/20051107020216/http://cp.sonybmg.com/xcp/english/updates.html (last visited Sept. 6, 2007).

39. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=921 (Nov. 3, 2005, 07:35 EST).

40. Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/11/09/sony-you-don-t-reeeeaaaally-want-to-uninstall-do-you.aspx (Nov. 9, 2005, 11:31 PST); Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=923 (Nov. 10, 2005, 08:25 EST). SunnComm required similar steps. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=931 (Nov. 17, 2005, 13:46 EST).

41. Posting of J. Alex Halderman & Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=927 (Nov. 15, 2005 07:07 EST); Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=928 (Nov. 15, 2005, 15:46 EST).

42. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=931 (Nov. 17, 2005, 13:46 EST).

failures of internal procedures to identify and prevent such mishaps and the misalignment of interests that cause them. Understanding the complex array of factors that contributed to Sony BMG's actions and reactions is an essential first step toward the adoption of policies and mechanisms to prevent similar incidents in the future.

This Article aims to identify the market, technological, and legal factors that appear to have led a presumably rational actor toward a strategy that in retrospect appears obviously and fundamentally misguided. Part II begins by considering the harm that resulted from Sony BMG's DRM strategy—both the damage to Sony BMG and its customers as well as the negative externalities imposed on a broad range of third parties. Part III examines potential market-based rationales that influenced Sony BMG's deployment of these DRM systems and reveals that even the most charitable interpretation of Sony BMG's internal strategizing demonstrates a failure to adequately value security and privacy. After taking stock of the then-existing technological environment that both encouraged and enabled the distribution of these protection measures in Part IV, we examine law, the third vector of influence on Sony BMG's decision to release flawed protection measures into the wild, in Part V. We argue that existing doctrine in the fields of contract, intellectual property, and consumer protection law fails to adequately counter the technological and market forces that allowed a self-interested actor to inflict such harms on the public.

Finally in Part VI, we present two recommendations aimed at reducing the likelihood of companies deploying protection measures with known security vulnerabilities in the consumer marketplace. First, we suggest that Congress should alter the Digital Millennium Copyright Act (DMCA) by creating permanent exemptions from its anti-circumvention and anti-trafficking provisions in order to enable security research and the dissemination of tools to remove harmful protection measures. Second, we offer promising ways to leverage insights from the field of human computer interaction security (HCI-Sec) to develop a stronger framework for user control over the security and privacy aspects of computers. The Federal Trade Commission (FTC), under its existing authority to protect consumers from deceptive and unfair practices, could develop best practices and regulations regarding the installation of software and the collection and transmission of information about users, their computers, and their actions. In addition, we recommend that the FTC explore the development of standards for security in the context of software and online data collection activities.

II. UNDISCLOSED HARM AND EXTERNALITIES

Before attempting to reconstruct the system of incentives that impelled Sony BMG to distribute the XCP and MediaMax protection measures, a clear accounting of both the actual and potential damage wrought by these technologies is in order. The harms flowing from the rootkit incident were varied and wide-reaching. The security flaws inherent in Sony BMG's DRM left users open to attack, and the DRM collected data about users' private activities without proper disclosure. Moreover, Sony BMG, as well as its artists, suffered damage to their reputation and bottom line as a result of the rootkit incident. But the effects of the rootkit extended well beyond the parties to these transactions. The rootkit incident threatened both the security of the network infrastructure and the future of DRM technology.

This Part briefly summarizes the harms suffered by the parties directly involved in the rootkit incident and then considers the broad social costs that resulted from Sony BMG's failure to fully account for the impact of its technology.

A. Direct Harm to Sony BMG, its Artists, and its Customers

The vulnerabilities created by Sony BMG's DRM gave rise to an array of potential abuses. The XCP rootkit permitted a hacker to write malicious code that, once installed on a user's computer, would run undetected so long as the name of the file containing that code began with the prefix "sys."[43] Similarly, the MediaMax privilege escalation allowed an attacker to replace code installed on users' machines and automatically executed upon insertion of a MediaMax disc.[44] Practically any malicious code authored by a hacker could take advantage of these general purpose security holes. The user's data could be altered, deleted, or even held for ransom; the machine could be rendered inoperable; a program could sniff sensitive passwords or collect financial records and other personal data; trade secrets and other corporate information could be collected; illegal data could be downloaded and stored on the user's machine. In short, these protection measures provided the means for remote attackers to take control of customers' computers.

Although these attacks represent worst case scenarios, the threats posed by Sony BMG's DRM were far from theoretical. Within days of the public rootkit announcement, malicious code leveraging the XCP protection scheme to hide from antivirus programs and system administrators

43. Halderman & Felten, *supra* note 11, at 18.
44. *Id.* at 17.

was spreading across the internet. A Trojan Horse[45] discovered early in November of 2005[46]—variously referred to as Backdoor.Ryknos,[47] Breplibot,[48] and Stinx-E[49]—attempted to take advantage of the cloaking capabilities of the rootkit.[50] Backdoor.Ryknos was transmitted via spam e-mail messages. Once on a user's system, it opened a back door to connect to an IRC[51] channel where the attacker could remotely control the user's system.[52] The remote attacker could download, delete, and execute files,[53] and send information about the compromised machine.[54] Antivirus and security software providers, already on the lookout for code intended to take advantage of the rootkit, quickly mobilized to identify and remove this Trojan. The high profile of the Sony BMG rootkit, coupled with this speedy response, likely discouraged others from attempting to further exploit the rootkit vulnerability.

To make matters worse, Sony BMG's surreptitious software installation and undisclosed data collection impeded the ability of computer users to make informed choices about security and privacy. The "phone home" feature of Sony BMG's DRM undermined customer privacy by collecting and transmitting information about users' interactions with protected CDs, including users' IP addresses.[55] But the EULA governing DRM-protected

---

45. Trojan Horses are programs that may appear benign or useful but in fact harbor malicious code. *See* MCAFEE, *supra* note 2, at 4.

46. Elia Florio, Symantec.com, Backdoor.Ryknos—Technical Details, http://www.symantec.com/security_response/writeup.jsp?docid=2005-111012-2048-99&tabid=2 (last updated Feb. 13, 2007).

47. *See* Elia Florio, Symantec.com, Backdoor.Ryknos—Summary, http://www.symantec.com/security_response/writeup.jsp?docid=2005-111012-2048-99&tabid=1 (last updated Feb. 13, 2007).

48. *See* Jarkko Turkulainen, F-Secure.com, *F-Secure Virus Descriptions: Breplbot.b*, http://www.f-secure.com/v-descs/breplibot_b.shtml (last updated Nov. 11, 2005); McAfee Threat Center, W32/Brepibot, http://vil.nai.com/vil/content/v_133091.htm#VirusChar (last updated Feb. 1, 2006).

49. *See* Sophos Threat Analysis, Troj/Stinx-E, http://sophos.com/virusinfo/analyses/trojstinxe.html (last visited Sept. 6, 2007).

50. Florio, *supra* note 47.

51. Internet Relay Chat ("IRC") is an open protocol used for text-based internet communication. *See generally* Wikipedia, Internet Relay Chat, http://en.wikipedia.org/wiki/Internet_Relay_Chat (last updated May 11, 2007).

52. Florio, *supra* note 46.

53. *Id.*; Turkulainen, *supra* note 48.

54. Florio, *supra* note 46.

55. In some instances the IP addresses collected by these protection measures could provide sufficient data to identify the user's location and identity. PETER ECKERSLEY ET

Sony BMG CDs explicitly disavowed any collection or dissemination of data related to customers or their computers. These misleading terms rendered Sony BMG customers incapable of offering informed consent to the data collection engaged in by XCP and MediaMax. Through this duplicity, Sony BMG deprived its customers of the ability to protect their own privacy.

Sony BMG also failed to disclose adequately the security failures of its DRM. Components of these measures were installed—sometimes permanently—before customers were confronted with the EULA terms.[56] The CD packaging, which was the only means of pre-installation notice, contained precious few indicia of the DRM contained within. The CD jewel cases featured the International Federation of the Phonographic Industry (IFPI) "Content Protected" logo on their spines[57] and a small nondescript "content protection grid" that provided general information and system requirements on their back covers.[58] These half-hearted disclosures failed to provide Sony BMG customers with fair warning of the security and privacy threats created by these DRM schemes or the scope of the limitations that they imposed on the use of the media.

Once the public became aware of the undisclosed costs of XCP and MediaMax, Sony BMG discovered that it was not insulated from the fallout of its own DRM strategy. CDs distributed with these protection measures experienced a steep drop-off in sales within some market segments. Later, the recall of millions of XCP and MediaMax discs led to significant expense and further lost sales opportunities.[59] In addition, Sony BMG

AL., ELECTRONIC FRONTIER FOUNDATION, SIX TIPS TO PROTECT YOUR ONLINE SEARCH PRIVACY (2006), http://www.eff.org/Privacy/search/searchtips.pdf.

56. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST); Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005, 14:23 EST).

57. Electronic Frontier Foundation, A Spotters' Guide to XCP and SunnComm's MediaMax, http://www.eff.org/IP/DRM/Sony-BMG/guide.php (last visited Sept. 6, 2007).

58. *See* Figure 1, *infra* Part V; *see also* Sony BMG Music Entertainment, CD's Containing XCP Content Protection Technology, http://cp.sonybmg.com/xcp/english/titles.html (last visited Sept. 6, 2007).

59. Tom Zeller Jr., *Sony BMG to Recall Copy-Restricted CDs*, INT'L HERALD TRIB., Nov. 17, 2005, Finance at 13; Tom Zeller, Jr., *Technology; CD's Recalled For Posing Risk to PC's*, N.Y. TIMES, Nov. 16, 2005, at C1; *Sony BMG Recalls Discs With Flawed Protection System (Update4)*, BLOOMBERG.COM, Nov. 16, 2006, http://www.bloomberg.com/apps/news?pid=10000101&sid=aVhY_TwrFjQI&refer=japan; Paul Taylor, *Sony BMG Bows to Pressure*, FT.COM, Nov. 16, 2005, http://www.ft.com/cms/s/e9e41f72-56f4-11da-b98c-00000e25118c.html.

spent millions to settle the steady stream of lawsuits arising out of the rootkit incident.[60] Less quantifiably, the resulting backlash from artists and customers significantly damaged the reputations of Sony BMG and its parent corporations.

Potential customers who were aware of the existence and dangers posed by Sony BMG's protection measures steered clear of XCP discs. The sales history of *Get Right with the Man*, an XCP-infected album by Van Zant that was released some six months prior to the rootkit announcement, is emblematic of the online retail impact of the rootkit incident. On November 2, just two days after the initial public announcement of the rootkit, *Get Right with the Man* ranked at number 887 on the music charts at Amazon.com.[61] The next day, after Amazon user reviews alerted shoppers to the dangers posed by XCP, the album dropped to number 1,392.[62] By the Thanksgiving holiday weekend, the XCP recall was underway and the album plummeted to number 25,802.[63] In contrast, in retail environments in which customers had less immediate access to information about the dangers of XCP, sales of *Get Right with the Man* were relatively undisturbed.[64] Since brick and mortar retailers like Wal-Mart, the nation's leading seller of CDs,[65] do not facilitate the sort of customer feedback common to online retailers, this outcome is hardly surprising.

Once Sony BMG instituted the recall of the remaining XCP-protected discs, and later MediaMax CDs, its albums were largely unavailable for purchase. In total, Sony BMG recalled 4.7 million XCP-protected CDs, roughly 2.6 million of which had not yet been sold.[66] The XCP recall cost

---

60. *See infra* note 69.

61. Lorraine Woellert, *Sony's Escalating "Spyware" Fiasco*, BUS. WK., Nov. 22, 2005, http://www.businessweek.com/technology/content/nov2005/tc20051122_343542.htm?campaign_id=rss_tech.

62. *Id.*

63. *Id.*

64. John Borland, *Sony Sailing Past Rootkit Controversy*, CNET NEWS.COM, Nov. 21, 2005, http://news.com.com/Sony+sailing+past+rootkit+controversy/2100-1027_3-5965243.html.

65. Max Fraser, *The Day the Music Died*, THE NATION, Nov. 27, 2006, http://www.thenation.com/doc/20061211/fraser.

66. Hiawatha Bray, *New Security Flaw Vexes Sony BMG Piracy Battle*, BOSTON GLOBE, Dec. 8, 2005, http://www.boston.com/business/technology/articles/2005/12/08/new_security_flaw_vexes_sony_bmg_piracy_battle; Brian Garrity & Ed Christman, *Sony BMG Recalls Copy Protected CDs*, BILLBOARD.COM, Nov. 18, 2005, http://billboard.com/bbcom/news/article_display.jsp?vnu_content_id=1001524942. Even after the recall, the copy-protected CDs were still available in many states. Arik Hesseldahl, *Spitzer Gets*

Sony BMG roughly $6.5 million in return fees and manufacturing costs.[67] Although the twenty million MediaMax discs it distributed were never officially recalled,[68] Sony BMG ceased production of MediaMax discs in December of 2005.[69] Various state Attorneys General negotiated the destruction of the remaining stock of MediaMax CDs at Sony BMG's expense.[70] In addition, Sony BMG's subsequent settlement with the FTC established an incentive program to prompt retailers to return any remaining discs.[71]

Not surprisingly, Sony BMG artists and their management lashed out at the label for its use of these protection measures.[72] Even before news of the rootkit broke, artists expressed their frustration with protected CDs, which among other things, prevented fans from transferring music to their iPods.[73] In a message to fans, Tim Foreman, of Sony BMG band Switchfoot, wrote,

> We were horrified when we first heard about the new copy-protection policy that is being implemented by most major labels . . . and immediately looked into all of our options for removing this from our new album . . . . It is heartbreaking to see our blood, sweat, and tears over the past 2 years blurred by the confusion and frustration surrounding this new technology."[74]

This dissatisfaction only grew once artists and fans learned of the dangers posed by these technologies. The manager for Sony BMG artist Trey Anastasio, whose November 1 album release was marred by the inclusion

---

on Sony BMG's Case, BUS. WK., Nov. 29, 2005, http://businessweek.com/technology/content/nov2005/tc20051128_573560.htm.

67. Brian Garrity & Ed Christman, *supra* note 66.

68. Juan Carlos Perez, *FTC Seeks Public Comment on Sony Rootkit Settlement*, COMPUTER WORLD, Jan. 30, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9009719&source=rss_news50.

69. Settlement Agreement at 27, *In re* Sony BMG CD Techs. Litig., No. 1:05-CV-09575 (S.D.N.Y. Dec. 28. 2005), *available at* http://www.eff.org/IP/DRM/Sony-BMG/sony_settlement.pdf.

70. Respondent Assurance of Voluntary Compliance or Discontinuance at 16, *In re* Sony BMG Music Entertainment (S.D.N.Y. Dec. 21, 2006), *available at* http://www.nj.gov/oag/newsreleases06/sony-bmg-agrmnt-12.21.06.pdf.

71. Press Release, Federal Trade Commission, Sony BMG Settles FTC Charges (Jan. 30, 2007), *available at* http://www.ftc.gov/opa/2007/01/sony.shtm.

72. Brian Hiatt, *Sony XCP Bomb Sparks Rage*, ROLLING STONE, Nov. 28, 2005, http://www.rollingstone.com/news/story/8878184/sony_xcp_bomb_sparks_rage.

73. Halderman & Felten, *supra* note 11, at 15.

74. Tim Rogers, *Stupid CD Copy Protection—Switchfoot Responds*, BLOGCRITICS MAGAZINE, Sept. 22, 2005, http://blogcritics.org/archives/2005/09/22/013800.php.

of XCP, called the incident "a complete fiasco that will impact the entire industry," and an "inexcusable blunder on the labels' part."[75] Another Sony BMG artist, My Morning Jacket, not only provided instructions on its website that enabled fans to bypass the MediaMax software on the band's album *Z,* but also sent over one hundred burned copies of the album to fans dissatisfied with the DRM.[76] In a New York Times Op-Ed, Damian Kulash, of the band OK Go, who narrowly avoided the inclusion of DRM on their EMI release *Oh No* in part because of the band's protestations, described copy protection software as "at best a nuisance, and at worst a security threat."[77]

The outcry from fans, artists, and consumer advocates alike gave rise to a palpable shift in the public perception of Sony BMG and its parent corporations.[78] Online petitioners called for a boycott of not only protected Sony BMG CDs, but Sony products generally.[79] In the fallout of the rootkit incident, one leading technology media outlet ranked Sony BMG's protected discs fifth in its list of the worst technology products in history.[80] The incident earned Sony BMG further distinction by being named one of the top ten "dumbest moments in business" for 2005.[81] Although the financial impact of this public relations disaster is difficult to estimate, Sony BMG remains, in the eyes of many consumers, inextricably associated with its misguided attempts at content protection.

B. Externalities Arising from the Rootkit Incident

Aside from its impact on Sony BMG and its customers, the rootkit incident inflicted broadly dispersed costs on individuals and institutions oth-

---

75. Hiatt, *supra* note 72.

76. James Montgomery, *My Morning Jacket Tackle Copy-Protection Software Problems—By Burning CDs For Fans*, MTV.com, Dec. 16, 2005, http://www.mtv.com/news/articles/1518240/20051215/%20my_morning_jacket.jhtm.

77. Damian Kulash Jr., *Buy, Play, Trade, Repeat*, N.Y. TIMES, Dec. 6, 2005, at A27.

78. Olga Kharif, *For Sony, a Pain in the Image*, BUS. WK., Dec. 2, 2005, http://www.businessweek.com/technology/content/dec2005/tc20051202_241333.htm; *Sony BMG Hits the Wrong Note*, COMPUTER BUS. REV. ONLINE, Nov. 16, 2005, http://www.cbronline.com/article_feature.asp?guid=44AF133B-9126-4207-A80C-60286AFAB943.

79. The Sony Boycott Blog, http://www.boycottsony.us/ (last visited Sept. 6, 2007); Boycott Sony!!! Petition, PetitionOnline.com, http://www.petitiononline.com/bcsony/petition.html (last visited Sept. 6, 2007).

80. Dan Tynan, *The 25 Worst Tech Products of All Time*, PC WORLD, May 26, 2006, http://www.pcworld.com/article/id,125772-page,2/article.html.

81. Adam Horowitz et al., *101 Dumbest Moments in Business*, BUSINESS 2.0, Jan. 2006, at 98, *available at* http://money.cnn.com/magazines/business2/101dumbest/2006.

erwise unconnected to Sony BMG's DRM strategy. First, the insecurity introduced into individual computers led to network-wide vulnerabilities. Second, the rootkit incident undermined consumer acceptance of digital rights management technology. The first of these externalities foisted the costs of network insecurity onto the public, while the second decreased the value and viability of DRM strategies and forced Sony BMG's partners and competitors within the content protection industry to rethink their practices.[82]

Because of the distributed nature of the information infrastructure, overall network security is, in part, a function of the security of the millions of private and personal computers that comprise it.[83] As a result, attacks on individual computers endanger, by extension, the network itself. Improving and maintaining the security of our collective information infrastructure is an established national priority[84]—a national priority directly threatened by Sony BMG's DRM.

These network vulnerabilities could manifest themselves in a number of ways. First, XCP-infected machines could be exploited by attackers to penetrate otherwise secure corporate, university, government, or military networks. In the weeks following the public announcement of the rootkit, the number of networks containing at least one installation of XCP topped half a million.[85] These networks suffered an increased risk of attack, leaving the sensitive data they stored subject to theft or tampering.

Second, computers infected with Sony BMG's DRM could serve as launching points for attacks on third party machines. An attacker could utilize the vulnerabilities created by these DRM systems to enlist thou-

82. While network insecurity almost certainly functions as a negative externality, the impact of the lessened value of DRM is more difficult to classify in terms of overall social utility.

83. *See* JAMES ELLIS ET AL., SOFTWARE ENG'G INST., REPORT TO THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (1997), http://www.cert.org/pres_comm/cert.rpcci.body.html.

84. *See, e.g.*, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES (Stewart D. Personick & Cynthia A. Patterson eds., National Academies Press 2003); PRESIDENT'S CRITICAL INFRASTRUCTURE PROT. BD., THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_ strategy.pdf.

85. Quinn Norton, *Sony Numbers Add Up to Trouble*, WIRED, Nov. 15, 2005, http://wired-vig.wired.com/politics/security/news/2005/11/69573; Dan Kaminsky, *Welcome To Planet Sony*, DOXPARA RESEARCH, Nov. 15, 2005, http://www.doxpara.com/?q=/node/1129.

sands of machines, unbeknownst to their owners, into massive botnets[86]—armies of so called "zombie" computers—which are directed to relay spam or conduct crippling distributed denial of service (DDOS) attacks.[87] Past DDOS targets have included corporations and national security assets, including the infrastructure of the internet itself.[88] Zombies may also be used to relay anonymous messages and hide the activities and communications of criminal and terrorist organizations from law enforcement.[89]

Whether through direct access to protected networks or through distributed attacks, Sony BMG's DRM threatened the basic operation of critical services that rely on the network infrastructure, among them, financial, communications, and disaster response services. The worst-case scenarios of rootkit-enabled attacks were nothing short of catastrophic. Although these potential outcomes may smack of doomsday prognostication, the Department of Homeland Security took note of the public threat posed by Sony BMG's DRM, cautioning that the XCP rootkit or similarly misguided attempts to control copyrighted works could interfere with the response to public health crises by compromising the security of the information infrastructure.[90]

---

86. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=1150 (Apr. 26, 2007, 10:41 EST) (discussing botnet threats in general).

87. A distributed denial of service attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. *See, e.g.*, Press Release, U.S. Department of Justice, Man Pleads Guilty to Infecting Thousands of Computers Using Worm Program then Launching them in Denial of Service Attacks (Dec. 28, 2005), *available at* http://www.cybercrime.gov/clarkPlea.htm; Ellen Messmer, *Web Sites Unite to Fight Denial-of-Service War*, NETWORK WORLD, Sept. 25, 2000, http://www.networkworld.com/news/2000/0925userdefense.html?nf&_ref=858966935; Jaikumar Vijayan, *VeriSign Details Massive Denial-of-Service Attacks*, COMPUTER WORLD, Mar. 16, 2006, http://www.computerworld.com/developmenttopics/websitemgmt/story/0,10801,109631,00.html.

88. *See, e.g.*, Tim Weber, *Criminals 'may overwhelm the web'*, BBC NEWS, Jan. 25, 2007, http://news.bbc.co.uk/2/hi/business/6298641.stm; John Leyden, *Telenor Takes Down 'massive' Botnet*, THE REGISTER, Sept. 9, 2004, http://www.theregister.co.uk/2004/09/09/telenor_botnet_dismantled/; Gregg Keizer, *Dutch Botnet Suspects Ran 1.5 Million Machines*, TECHWEB TECH. NEWS, Oct. 21, 2005, http://www.techweb.com/wire/security/172303160.

89. Comment of Edward W. Felten & J. Alex Halderman to the United States Copyright Office, concerning RM 2005-11—Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Dec. 1, 2005), *available at* http://www.copyright.gov/1201/2006/comments/mulligan_felten.pdf.

90. *Homeland Security Warns Against Anti-Piracy*, WASHINGTONPOST.COM, Nov. 11, 2005, http://www.washingtonpost.com/wp-dyn/content/video/2005/11/11/VI2005111101160.html. Stewart Baker, assistant secretary of policy at the Department of Home-

Aside from the social cost of decreased security of the information infrastructure, the rootkit incident resulted in a second externality. By dramatically increasing public awareness of the restrictions on access and copying imposed by DRM technologies, while simultaneously corroding consumer confidence in their safety, the rootkit incident likely undermined the significant investments of both content providers and protection measure vendors in such technology. In the wake of the rootkit fiasco, major labels abandoned the use of DRM on CDs,[91] and leading protection measure vendors ceased development of new CD-based DRM systems.[92] But unlike the collective costs to security imposed by the rootkit incident, the reduced viability of DRM in the consumer music market may well represent a positive externality, rather than a negative one. To the extent the constraints and risk DRM imposed on consumers outweighed any benefits they conferred on copyright owners and the public, the reduction of DRM in the consumer marketplace could increase overall utility.

The impact of the rootkit incident has extended beyond the CD market, coloring consumer perception of the desirability of DRM and forcing copyright owners and technology companies to rethink their content protection strategies. DRM, of course, faced criticism long before the rootkit

---

land Security, warned copyright holders against overly aggressive efforts to protect copyrighted material:

> I wanted to raise one point of caution as we go forward, because we are also responsible for maintaining the security of the information infrastructure of the United States and making sure peoples' [and] businesses' computers are secure. . . . There's been a lot of publicity recently about tactics used in pursuing protection for . . . CDs in which questions have been raised about whether the protection measures install hidden files on peoples' computers that even the system administrators can't find. It's very important to remember that it's your intellectual property; it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days.

Id.; Brian Krebs, *DHS Official Weighs In on Sony*, WASHINGTONPOST.COM, Nov. 11, 2005, http://blog.washingtonpost.com/securityfix/2005/11/dhs_official_weighs_in_on_sony.html.

91. Robert Thompson & Tom Ferguson, *Copy-Protection Curtailed*, BILLBOARD, Dec. 16, 2006, at 27 ("EMI Music Group has dropped copy-protection technology from new CD releases internationally amid concerns it was not slowing piracy. The decision means that no major labels are currently releasing copy-protected discs.").

92. *Macrovision Scraps CD Protection Software, Readies New Download Service*, CONSUMER ELECTRONICS DAILY, Feb. 23, 2007 ("[Macrovision CEO Fred] Amoroso conceded that the discovery in late 2005 of a rootkit in Sony BMG CDs containing First4Internet's copy protection software 'spooked the industry.'").

incident.[93] But after the general public became more attuned to the presence and effects of DRM, in part through the debate sparked by the XCP rootkit, these criticisms came from not only consumer advocates, but from leading technology companies with intimate ties to the music industry as well. In December of 2005, Bill Gates decried the lack of "simplicity and interoperability" of the DRM technologies protecting music downloads.[94] Others like Yahoo! Music chief David Goldberg urged the industry to drop DRM on downloads.[95] These early critiques of DRM led the music industry to implement limited experiments in legitimate DRM-free downloads.[96]

These experimental DRM-free releases gave way to calls for more fundamental changes. In February of 2007, Apple CEO Steve Jobs published an open letter in which he called for the major record labels to "abolish DRMs entirely."[97] Less than a month later, EMI and Apple announced that EMI's entire digital catalog would be available without DRM on iTunes and through other retailers.[98] During the joint Apple/EMI

---

93. *See, e.g.*, Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519, 556 (1999).

94. *Gates: Digital Locks Too Complex*, BBC NEWS, Dec. 15, 2006, http://news.bbc.co.uk/1/hi/technology/6182657.stm; Michael Arrington, *Bill Gates On The Future Of DRM*, TECHCRUNCH, Dec. 14, 2006, http://www.techcrunch.com/2006/ 12/14/bill-gates-on-the-future-of-drm/.

95. Ian C. Rogers, *Dave Goldberg to Record Labels: No DRM, Please*, YAHOO! MUSIC BLOG, Feb. 25, 2006, http://ymusicblog.com/blog/2006/02/25/dave-goldberg-to-record-labels-no-drm-please/; John Borland, *Yahoo Exec: Labels Should Sell Music Without DRM*, CNET NEWS.COM, Feb. 23, 2006, http://news.com.com/8301-10784_3-6042756-7.html?part=rss&tag=6042756&subj=news.

96. Jessica Simpson, Jesse McCartney, and Lily Allen were among the artists included in these initial trials for DRM-free downloads. Ian C. Rogers, *Buy A Customized MP3 At Yahoo! Music*, YAHOO! MUSIC BLOG, July 19, 2006, http://ymusicblog.com/blog/2006/07/19/buy-a-customized-jessica-simpson-mp3-at-yahoo-music/; *Is EMI Experimenting With MP3's?*, HYPEBOT, Nov. 29, 2006, http://hypebot.typepad.com/hypebot/2006/11/is_emi_experime.html; Ben Fritz, *Yahoo Tests 'Right' to MP3 Downloads*, VARIETY.COM, Sept. 18, 2006, http://www.variety.com/article/VR1117950324.html?categoryid=1009&cs=1&nid=2570.

97. STEVE JOBS, THOUGHTS ON MUSIC (2007), http://www.apple.com/hotnews/thoughtsonmusic/.

98. Press Release, EMI, EMI Music Launches DRM-free Superior Sound Quality Downloads Across its Entire Digital Repertoire (Apr. 2, 2007), *available at* http://www.emigroup.com/Press/2007/press18.htm; Press Release, Apple, Apple Unveils Higher Quality DRM-Free Music on the iTunes Store (Apr. 2, 2007), *available at* http://www.apple.com/pr/library/2007/04/02itunes.html. The first DRM-free EMI release, the album *The Good, The Bad & The Queen*, by the innominate EMI band, was made available im-

press conference, Jobs noted the rootkit as an example of the failure of CD-based DRM.[99] Other digital music retailers, including Microsoft, followed suit and agreed to provide DRM-free EMI music.[100]

Obviously, the fear of rootkit-like security vulnerabilities was not the sole, or even primary, impetus for this shift in the market for digital music downloads. But the rootkit incident contributed to the creation of an environment amenable to this change in the prevailing wisdom among record labels and their online content distributors. The rootkit incident thrust the negative implications of DRM into the public consciousness on a broader scope than had previous rounds of criticism. These implications included not only the privacy and security interests directly at stake in the rootkit incident, but also more general concerns over restrictions on noninfringing uses, portability, and platform independence. As a validation of the long-standing and frequently marginalized critiques of DRM, the rootkit incident made it more difficult for these criticisms to be dismissed out of hand. If the rest of the music industry follows EMI in its march away from DRM, the rootkit incident may prove, in retrospect, to have been a major strategic turning point.

But even copyright holders that continue to insist upon DRM recognize its public relations pitfalls in the current marketplace. In a transparent effort to divert attention away from the restrictions placed on users by technological protection measures, some have called for a shift in terminology, dropping "Digital Rights Management"—a term once thought consumer-friendly—and replacing it with the euphemistic "Digital Consumer Enablement."[101] Whether substantive changes in current business

---

mediately. The remainder of the EMI catalog was scheduled for DRM-free release on iTunes in May of 2007.

99. Eric Nicoli, CEO, EMI Group & Steve Jobs, CEO, Apple, Q&A at EMI Press Conference (Apr. 2, 2007), *audio available at* http://w3.cantos.com/07/pjxrobbi-703-5zvx0/interviews.php?task=view; *Jobs Talks New iTunes Functions, DRM and Video, iPod Storage*, APPLEINSIDER, Apr. 2, 2007, http://www.appleinsider.com/articles/07/04/02/jobs_talks_new_itunes_functions_drm_and_video_ipod_storage_transcript.html. Apple's position was likely influenced, at least in part, by growing international opposition to its iTunes DRM. See Apple DRM illegal in Norway: Ombudsman, The Register, http://www.theregister.co.uk/2007/01/24/apple_drm_illegal_in_norway/?TB_iframe=true&height=650&width=950 (Jan. 24, 2007); Thomas Crampton, iTunes legal attacks spread from France, International Herald Tribune, http://www.iht.com/articles/2006/06/08/business/apple.php (June 9, 2006).

100. *See, e.g.*, Elizabeth Montalbano, *Microsoft Will Sell DRM-free Songs*, PC WORLD, Apr. 6, 2007, http://www.pcworld.com/article/id,130472/article.html.

101. Glen Dickson, *NCTA: HBO's Zitter Says DRM Is Misnomer*, BROADCASTING & CABLE, May 9, 2007, http://www.broadcastingcable.com/article/CA6440876.html.

models prevail or the industry instead adopts cosmetic fixes, the market for DRM has undergone an important shift, in part as the result of the rootkit incident.

The harms that resulted from the rootkit incident affected all parties to the sale and licensing of protected Sony BMG CDs. Customers received a product tainted by reduced functionality, undisclosed invasions of privacy, and increased vulnerability to security breaches. Sony BMG and its artists hardly benefited from this deal, suffering both financial and reputational repercussions. The externalities that flowed from the rootkit incident undermined collective investments in network security and DRM technology for parties entirely removed from Sony BMG and its ill-designed protection measures. In the end, it appears safe to conclude that no one's best interest—especially not that of Sony BMG—was served by the distribution of XCP and MediaMax. The next Part attempts to surmise what market considerations could have convinced Sony BMG that the distribution of these protection measures was a reasonable, self-interested decision.

III. MARKET INFLUENCES

Failures of software developers to adequately safeguard the security of their users' systems and information come as no shock to those familiar with the state of computer security. The values and incentives that give rise to these failures are well documented.[102] Users frequently undervalue their own privacy and security,[103] and even those who claim to place a high value on these interests often act inconsistently with those values.[104] Because increased security provides little or no competitive advantage through product differentiation, firms recognize that the significant investments in time and resources needed to identify and eliminate the bugs that create insecurity will not be recouped.[105] As a result, firms systematically under-invest in software security and fail to eliminate vulnerabilities.

---

102. *See* Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610 (2006), *available at* http://www.cl.cam.ac.uk/~twm29/science-econ.pdf.

103. *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SECURITY & PRIVACY, Jan.-Feb. 2005, at 26.

104. *See id.*

105. *See* Bill Thompson, *Taking Computer Insecurity Seriously,* BBC NEWS, Sept. 17, 2004, http://news.bbc.co.uk/2/low/technology/3666702.stm; Jeordan Legon, *As Net Attack Eases, Blame Game Surges*, CNN.COM, Jan. 28, 2003, http://www.cnn.com/2003/TECH/internet/01/27/worm.why/; Brendan I. Koerner, *Ain't No Network Strong Enough*, SALON.COM, Aug. 31, 2000, http://archive.salon.com/tech/review/2000/08/31/schneier/;

However, these incentives to under-invest in security cannot fully explain the Sony BMG rootkit incident. Typically, software vulnerabilities result from a developer's failure to remove incidental and unintended infirmities in its code. But the rootkit incident in large part resulted from the *intentional* introduction of components and functionality that undermined user security and privacy in the service of content protection.[106] From the perspective of protection measure developers and content owners, these security and privacy flaws served as features rather than bugs.[107] In this sense, the motivations underlying the rootkit incident share some common features with those that spur the development of spyware. Because it differs so fundamentally from the longstanding understanding of how insecure software makes its way to market, the Sony BMG rootkit incident raises new questions about the incentives to protect or subvert user security and privacy in the context of DRM technology.

This Part examines two basic sets of market-based explanations of Sony BMG's decision-making process. The first considers possible failures to grasp the likely impact of its technology, and suggests systematic inadequacies in Sony BMG's review of the DRM systems it licenses. The second countenances more informed and, consequently, more deliberate cost-benefit calculations that could encourage the use of cloaking technologies and inadequate disclosures. Ultimately, although we conclude that this second set of explanations is the more plausible, both likely contributed, to varying degrees, to the release of these protection measures.

A. The Rootkit Incident as Mistake

Imperfect information and bounded rationality offer perhaps the most charitable explanations of Sony BMG's decision to distribute XCP and MediaMax. Given the resources and sophistication of Sony BMG, this explanation seems at best incomplete. But even if Sony BMG lacked critical

---

Mindy Blodgett, *Is Your Business as Safe as You Think?*, CNN.COM, July 16, 1999, http://www.cnn.com/TECH/computing/9907/16/security-ent.idg/index.html.

106. Some of the risks created as a result of the rootkit incident were the result of failures to eliminate bugs rather than the intentional introduction of risk. This more traditional narrative, for example, explains the flaws in the uninstaller tools and patches released after the disclosure of the harms of XCP and MediaMax. MediaMax's privilege escalation vulnerability likewise can be explained without implying any harmful intent on the part of its developers.

107. As Professor Felten has explained, these vulnerabilities are "caused not by any flaws in [the] execution of their copy protection plan, but from the nature of the plan itself." Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=934 (Nov. 22, 2005, 03:51 EST).

information about the dangers posed by its protection measures or miscalculated their likelihood and severity, its decision points to a culpable failure of internal procedures to safeguard against the wide-scale distribution of flawed protection measures.

A good-faith mistake on the part of Sony BMG could have arisen in two ways. First, Sony BMG could have been unaware of the objectionable features of its DRM—at least those not directly related to the constraints placed on accessing and copying music. Second, Sony BMG could have been misinformed or misled about the dangers posed by the various components of its protection measures.

Both of these explanations depend on a lack of adequate pre-release security reviews of protection measures. Sony BMG has offered no public indication that any pre-release security review occurred. Assuming Sony BMG did not intentionally distribute software with knowledge of the dangers it posed, any such review must have failed to identify the threats inherent in XCP and MediaMax. It is unlikely that Sony BMG lacked sufficient in-house security expertise to meaningfully examine the functionality of the protection measures it licensed. Given that Sony Corporation of America, whose holdings include Sony Electronics and Sony Computer Entertainment America, controls a 50% interest in Sony BMG, more than adequate technical analysis was within reach. Moreover, external security review of new DRM schemes is common within the music industry. And as demonstrated by the research of F-Secure[108] and Mark Russinovich,[109] as well as by the analysis of Ed Felten and J. Alex Halderman,[110] trained security professionals could have easily identified the security risks posed by these protection measures.

Aside from a disregard for user security,[111] another explanation for the lack of meaningful security review is overconfidence in the protection measure vendors who provided these technologies. In retrospect, any such confidence was obviously misplaced. But even without the benefit of hindsight, Sony BMG had good reason to subject its vendors' products to scrutiny. Prior to inking the deal to provide XCP to Sony BMG, First4Internet's business focused on content filtering, particularly the

108. *See* Hamm, *supra* note 13.

109. *See* Mark's Blog, *supra* note 8 (Oct. 31, 2005, 11:04 PST).

110. *See* Halderman & Felten, *supra* note 11.

111. As discussed *infra* in Section III.B, an undervaluing of user security and privacy could explain Sony BMG's decision.

automated recognition of pornographic images.[112] Aside from an earlier revision on XCP used by a number of labels on a smattering of pre-release CDs,[113] First4Internet had no apparent expertise or experience in content protection software.

SunnComm, the company that delivered MediaMax, offered even more cause for concern. The company began as a provider of Elvis impersonation services.[114] After a change in management following a false press release announcing a non-existent $25 million production deal with Warner Brothers,[115] the company purchased a 3.5" floppy disk factory in 2001, displaying a disturbing dearth of technological savvy.[116] After two employees announced their intention to leave the fledgling company to develop copy protection software, SunnComm convinced the pair to lead a new division, leaving both Elvis and floppy discs behind in order to develop what would become MediaMax.[117]

Sony BMG—perhaps realizing too late its misplaced trust in SunnComm, or perhaps simply hoping to recoup some of its financial and public relations losses—filed a lawsuit against the Amergence Group (a re-branded SunnComm)[118] in July of 2007. Sony BMG's claims include

---

112. *See First 4 Internet Powers New Anti-Porn Solutions at Europe's Biggest Security Show; Major New Products from PixAlert, Pure Content and Green Technology Meet Growing Corporate Need to Filter Pornography*, TMCNET, Apr. 20, 2005, http://www.tmcnet.com/usubmit/2005/apr/1136356.htm. After the rootkit incident, First4Internet continued to do business under the name Fortium Technologies. *See* Robert Lemos, *Sony BMG Sues Copy-protection Maker*, SECURITYFOCUS, July 13, 2007, http://www.securityfocus.com/brief/547.

113. *See* Sion Barry, *Controlling Illicit Internet Content Drives F4I Success*, ICWALES, June 15, 2005, http://icwales.icnetwork.co.uk/0300business/0100news/tm_objectid=15631868&method=full&siteid=50082-name_page.html.

114. Ashlee Vance, *Is SunnComm a Sham or the Next, Big DRM Success?*, THE REGISTER, Sept. 27, 2004, http://www.theregister.co.uk/2004/09/27/sunncomm_death_or_glorry/print.html.

115. Complaint for Injunctive and Other Relief, U.S. Sec. and Exch. Comm'n v. Paloma (D.D.C. Apr. 11, 2002), *available at* http://www.sec.gov/litigation/complaints/complr17462.htm.

116. SunnComm purchased the floppy drive company, which was formerly a failed oil and gas company, in part to avoid SEC scrutiny by merging with a fully reporting company. *See* Vance, *supra* note 114.

117. *Id.*

118. SunnComm, too, underwent something of a re-branding after the rootkit incident, rechristening itself the Amergence Group. Press Release, The Amergence Group, SunnComm Establishes New Subsidiary—The Amergence Group (Jan. 26, 2007), *available at* http://www.amergencegroup.com/news/amergingnews.asp?grammid=200701261030.

negligence and breach of contract, alleging that MediaMax was defective and failed to satisfy SunnComm's warranty.[119] The Amergence Group contends that Sony BMG retained "final authority" over the functional specifications of MediaMax, and that SunnComm simply delivered the product demanded by Sony BMG.[120] This litigation, as it proceeds, may well reveal the extent of Sony BMG's knowledge of the objectionable features of its DRM.

Until such information is available, Sony BMG's sophistication[121] and access to both internal and external resources offer good reasons to question the likelihood that it was in the dark as to the existence of the dangers posed by the rootkit and the other objectionable features of XCP and MediaMax. Even assuming Sony BMG was oblivious as to the details of its DRM, the failure to act expeditiously once notified by F-Secure of the rootkit and its dangers suggests that a lack of knowledge alone fails to fully explain Sony BMG's actions. In any case, to the extent that ignorance of the functionality and likely effects of its DRM influenced Sony BMG's decision-making, its failure to independently review these technologies evinces an undervaluation of the documented potential effects of DRM on user security and privacy.

B. The Rootkit Incident as Calculated Risk

Since characterizations of the rootkit incident as the result of a good-faith mistake by Sony BMG fail to fully account for its internal decision-making, explanations that presume some degree of knowledge present more plausible scenarios. Understanding why Sony BMG would knowingly distribute protection measures that carried the risks associated with XCP and MediaMax requires consideration of the relative value propositions presented by CD-based DRM to content owners and customers. Although DRM, in theory, offers copyright holders some benefit from reduced copying, consumers generally see DRM as a poor bargain since it requires them to pay the same price for a product with diminished func-

---

119. *See* Summons Notice, Sony BMG Entm't v. Amergence Group, No. 602201-2007 (N.Y. Sup. Ct.) (on file with authors).

120. Press Release, The Amergence Group, Sony-BMG Files Suit Against Amergence Group (July 11, 2007), *available at* http://www.marketwire.com/mw/release.do?id=750315.

121. Sony, along with Philips, owns the rights to the core DRM patents of Intertrust. In theory, at least, Sony BMG could have implemented a suite of better technical solutions. *See* Press Release, Sony Corporation of America, Philips and Sony Lead Acquisition of Intertrust, *available at* http://www.sony.com/SCA/press/021113.shtml (Nov. 13, 2002).

tionality. Underhanded tactics such as those used by Sony BMG offer one way to overcome this skepticism, although this story should counsel against their future use.

Although the precise amounts are uncertain, the music industry loses revenues each year as a result of copyright infringement.[122] Songs copied on peer-to-peer networks, BitTorrent, and other lesser-known corners of the darknet contribute to these losses, as does large-scale CD piracy and the casual physical copying of CDs by everyday consumers.[123] DRM is intended to serve as a partial solution to the widespread infringement of music industry copyrights, but, as the industry is likely aware, CD-based DRM cannot hope to address two of these three sources of infringement. Since only a single unrestricted copy of a particular track is necessary to rapidly populate peer-to-peer and other networked methods of file transfer, measures like XCP and MediaMax are all but worthless when it comes to preventing infringement on the internet.[124] And protection measures that can be easily thwarted[125] pose no genuine hurdles for the sophisticated, large-scale commercial pirates that press upwards of one billion counterfeit CDs each year.[126]

The value of CD-based DRM like XCP and MediaMax, therefore, flows from its ability to prevent the casual schoolyard trading of burned CDs and other varieties of personal copying. The precise scope of financial harm caused by such purported infringement is unclear.[127] Nor does

---

122. RIAA, Piracy: Online and on the Street, http://www.riaa.com/physicalpiracy.php?content_selector=piracy_details_online (last visited July 30, 2007).

123. *Id. See also* Peter Biddle & Paul England, *The Darknet and the Future of Content Distribution*, ACM SIGCOMM COMPUTER COMM. REV., Oct. 2001, at 140, *available at* http://msl1.mit.edu/ESD10/docs/darknet5.pdf (describing the darknet as "a collection of networks and technologies used to share digital content [and] an application and protocol layer riding on existing networks" and citing as examples of darknets "peer-to-peer file sharing, CD and DVD copying, and key or password sharing on email and newsgroups.").

124. *See* Halderman & Felten, *supra* note 11, at 2.

125. As discussed *infra* in the text accompanying note 179, MediaMax can be defeated by simply holding down a computer's shift key. Earlier DRM systems could be circumvented using just adhesive tape or a felt tip pen. HALDERMAN, *supra* note 4, at 4, 5.

126. *Pirate CD Sales Top 1 Billion*, CNN.COM, July 10, 2003, http://edition.cnn.com/2003/BUSINESS/07/10/music.piracy/; *Pirate CD Sales Hit Record High*, BBC NEWS, July 22, 2004, http://news.bbc.co.uk/2/hi/entertainment/3916681.stm.

127. Industry research indicates that such "social sharing" accounts for as much as 37% of music acquisition by volume. NPD GROUP, NARM/NPD 2007, PHASE ONE, CONSUMERS & MUSIC DISCOVERY 4 (2007), *available at* http://www.digitalmusicnews.com/research/npd_presentation_narm. However, as with earlier projections of harm aris-

any available evidence reveal the effectiveness of these measures in limiting such activity. Perhaps in recognition of the tenuous argument for the utility of these measures, even on this single front of the war against infringement, the music industry is quick to downplay its expectations for CD-based DRM, typically referring to these protection measures as mere "speed bumps" or inconveniences intended to keep honest customers honest.[128] But given their rudimentary design, these protection measures disproportionately affect those customers with the least knowledge of the operations of their computers, precisely those reasonably expected to pose the least threat of infringement. From the content owners' own perspective, these protection measures offer only marginal value, and even this valuation may be the result of overestimates of the effectiveness of CD-based DRM.

If the value of CD-based DRM to content owners is low, albeit positive, the value of these protection measures to customers is almost unquestionably negative. Even at the time of the rootkit incident, the overwhelming majority of CDs were sold without DRM;[129] customers were, as a technological matter, free to copy songs from these discs to their hard drives, transfer them to iPods, burn them to CDs, and listen to them using the software of their choice.[130] XCP and MediaMax altered long-standing consumer expectations[131] by placing technological and contractual limits on customers' ability to use their CDs in the manner to which they were accustomed.

---

ing from peer-to-peer downloads, estimates of the relative proportion of these burned and ripped copies that translate to lost sales would likely vary significantly.

128. Sony spokesman Nathaniel Brown characterized SunnComm's first copy protection scheme in the following manner after J. Alex Halderman reported that it was easily disabled: "Copy management is intended as a speed bump, intended to thwart the casual listener from mass burning and uploading. We made a conscious decision to err on the side of playability and flexibility." John Borland, *Shift Key Breaks CD Copy Locks*, CNET NEWS.COM, Oct, 7, 2003, http://news.com.com/2100-1025_3-5087875.html.

129. In 2005, over 600 million CDs were sold in the United States. *See US CD Album Sales Show 7% Slide*, BBC NEWS, Dec. 29, 2005, http://news.bbc.co.uk/2/hi/entertainment/4566186.stm. Of those, the millions of CDs protected by XCP and MediaMax represented only a small percentage.

130. *See infra* notes 132-136.

131. Consumer expectations flow from prior experience with similar objects and information. These experiences are in turn a result of the capacity of the technology, laws, norms, and markets. Consumer expectations of interacting with DVDs today reveals how these forces can come together in ways that create expectations different from those which prevailed during the CD era.

Empirical research has cataloged the deep-seated expectations of consumers with respect to their interaction with digital music. In a study conducted in the European Union, consumers indicated uniform and strong beliefs in their right to move digital music between devices.[132] Similarly, individuals shared a strong conviction that copying for their own purposes is legal,[133] and a high percentage of the survey population had burned their own music mixes in the prior six months.[134] While survey participants' belief in the legality of "sharing" music was less strong and consistent,[135] they reported a significant amount of sharing with family and friends.[136]

These consumer expectations are firmly rooted in the pre-digital patterns of consumption and use of recorded music. Concerns over private copying enabled by new technologies are, of course, nothing new. Nearly every advance in the recording and distribution of music has sparked near hysteria from then-dominant rights holders. Music publishers balked at the player piano,[137] the phonograph[138] and radio of both the terrestrial[139] and internet[140] varieties. And long before the music industry feared peer-to-peer infringement, reel-to-reel copying led the industry to infamously proclaim that "Home Taping is Killing Music."[141] The concerns that motivate

---

132. According to the study, 81% of those surveyed thought it legal to play a purchased file on different devices. NICOLE DUFFT ET AL., INDICARE, DIGITAL MUSIC USAGE AND DRM: RESULTS FROM AN EUROPEAN CONSUMER SURVEY 42 (2005), *available at* http://www.indicare.org/tiki-download_file.php?fileId=110.

133. In the study, 73% of users surveyed thought it was legal to make a copy of a CD or file which they had bought for themselves, for their own use. *Id.*

134. Of all digital music users surveyed, 80% had burned their own mixes to CD over the past 6 months, 39% had done so several times per month or more often. The share of teens that burn their own CDs several times per month or more often is 46%, compared to 34% of the 40+ group. *Id.* at 16. In Germany, almost 90% of the digital music users like to burn their own mixes on CD compared to "only" 75% in the UK. *Id.* at 18 tbl. 3.2.

135. *Id.* at 42.

136. More than three quarters of digital music users have shared music files with their family members and friends over the past 6 months; 60% have shared music files with other people. Again, teens are the most active music file sharers; about half of them share music files with friends and family several times per month or more often. *Id.* at 16.

137. LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 55-56 (2004), *available at* http://www. jus.uio.no/sisu/free_culture.lawrence_lessig/portrait.pdf.

138. *Id.*

139. *See id.* at 58-59.

140. *See id.* at 195-99.

141. Neil Strauss, *THE POP LIFE; 2 Big Forces Converging To Change the Sale of Music*, N.Y. TIMES, Dec. 10, 1998, at E1.

DRM are simply a continuation of this pattern of hostility to disruptive technologies.

Although engineering constraints have historically limited the copying of music, digital works are trivially copied without any loss of quality. In part driven by the lack of practical constraints on digital copying, DRM proactively introduces technological hurdles that exceed those available to earlier generations of copyright holders, displacing the traditionally porous enforcement of copyright with limits embedded in and enforced by software code.[142] In contrast, previous mechanisms for addressing infringement intruded less far less on the consumer's experience of the purchased music. For example, the Serial Copy Management System, which controlled downstream copying of the ill-fated Digital Audio Tape format, did not impede the use of the original tape or even the recording of first-generation copies.[143] DRM, on the other hand, frequently constrains the portability of music by tethering it to particular devices or platforms. Consumers are limited in their ability to experience the music on their own terms, in the time, place, and even sequence of their choice. Their ability to copy, share, and recode content is likewise constrained in a manner that offends many users' perceptions of fairness, if not law.

The constraints imposed by DRM generally reduce the value to consumers of protected content. Information goods typically increase in value as the number and extent of their possible uses increase.[144] With respect to DRM, consumers will, in principle, pay more for goods with liberal usage rules. In addition, more consumers can be expected to purchase such goods.[145] Consumers regard media with very limited uses as the equivalent of damaged goods[146] and will pay less for them, if they are willing to purchase them at all.[147] In short, CD-based DRM renders the protected discs

142. *See* Radin, Margaret Jane, *Regulation by Contract, Regulation by Machine*, 160 J. Inst. & Theoretical Econ. 142, 151-153 (2004); *see generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

143. *See* Digital Audio Recording Devices and Media Act of 1992, 17 U.S.C. §§ 1001-1010 (2000).

144. CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 97-102 (1998).

145. This principle is borne out by the INDICARE survey results, which indicate that people are willing to pay substantially more for digital music with more functionality. *See* DUFFT ET AL., *supra* note 132, at 25.

146. *See* SHAPIRO & VARIAN, *supra* note 144.

147. *See* NATALI HELBERGER ET AL., FIRST UPDATE OF THE STATE-OF-THE-ART REPORT: DIGITAL RIGHTS MANAGEMENT AND CONSUMER ACCEPTABILITY: A MULTI-DISCIPLINARY DISCUSSION OF CONSUMER CONCERNS AND EXPECTATIONS 33-34 (2005), *available at* http://www.indicare.org/tiki-download_file.php?fileId=111.

less valuable to consumers. Yet this reduction in functionality is not counterbalanced by any proportionate decrease in cost. DRM-protected CDs are sold at roughly the same price as standard non-protected CDs.[148] Some protected CDs include bonus features like music videos or interactive artist biographies, but for most consumers these features were likely insufficient to compensate for the reduction in basic functionality of the protected discs.

Another factor in choosing to surreptitiously deploy DRM, beyond skirting consumer resentment, was that Sony BMG likely underestimated the public reaction to the security and privacy threats created by its DRM. Both research and market history have demonstrated that many users are willing to trade security and privacy for ease of use, desired functionality, or even small sums of money.[149] These results could lead a firm to place minimal value on user security and privacy in its risk calculus. In the rootkit incident, these assumptions proved incorrect. Consumers, it would appear, care enough about privacy and security to want to make the decision about when and whether to trade it away for themselves. In part, the strong reaction to these faulty protection measures could stem from deeply ingrained expectations about our experience of music. In contrast to browsing the internet or downloading software, consumers consider the playing of a CD to be a private and passive act and one that carries no risk of attack from the outside world. When security and privacy threats intruded upon this zone of safety, consumers reacted with unexpectedly intense indignation. The particularly strong reaction may also have stemmed from the lack of any perceptible fair trade-off between the benefits gained by consumers and the risks they faced. A user who downloads a free game or screensaver from the internet may suspect a risk of unwanted adware, but justifies that risk by the benefit of a free program. Here customers paid the expected price, and not only received less than they bargained for in terms

148. *Id.* at 28, 33.

149. For an overview of surveys and experiments revealing divergence in consumers' privacy attitudes from their behavior during transactions, see Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behaviors: Losses, Gains, and Hyperbolic Discounting*, in THE ECONOMICS OF INFORMATION SECURITY 165 (L. Jean Camp & Stephen Lewis eds., 2004). For specific examples of this phenomena, see Sarah Spiekermann, Jens Grossklags, & Bettina Berendt, *E-privacy in 2nd Generation E-commerce: Privacy Preferences Versus Actual Behavior*, in PROCEEDINGS OF THE 3RD ACM CONFERENCE ON ELECTRONIC COMMERCE 38-47 (2001) (discussing lab study finding inconsistencies between participants' self-reported privacy concerns and behavior in online shopping experiences).

of CD functionality, but were also saddled with undisclosed privacy and security risks.

XCP and MediaMax presented unique marketing challenges for Sony BMG. Since fully-informed customers were unlikely to pay full price for what they would view as an inferior product, Sony BMG faced a choice. It could either develop a product that included DRM but was nonetheless attractive to consumers—most likely by significantly reducing retail prices—or it could obfuscate the nature of the product it sold and prevent its customers from excising the unwanted DRM post-purchase. All evidence suggests that Sony BMG adopted the latter approach.

These same market conditions, however, existed for all major record labels, yet most of Sony BMG's competitors were content to implement less invasive technological protection measures, knowing full well that they would fail to prevent infringement.[150] The other major labels, unlike Sony, did not insist upon maximum effectiveness at the risk of harm to users.

The history of Sony, one of the two parent companies of Sony BMG, in its attempts to restrict access to and copying of its content may offer some insight into why Sony BMG, unlike its competitors, accepted these risks in return for an uncertain and at best marginal increase in the effectiveness of its DRM. The aggressive stance adopted by Sony in halting innovative consumer-driven uses of products like the Aibo robotic dog[151] and the Playstation[152] suggest a willingness to seek maximum protection of Sony intellectual property, even at the risk of consumer alienation.

---

150. *See* Jefferson Graham, *CD Woes May Have Had Roots in Merger*, USA TODAY, Nov. 18, 2005, at 1B. Some have suggested that shifts in management and massive staff cuts at Sony BMG may have contributed further to the breakdown that led to the release of XCP. *See id.*

151. The Aibo, which retailed for $1299, came preprogrammed with a limited set of functions. John G. Spooner, *Sony Aibo to Spread More Puppy Love*, CNET NEWS.COM, Oct. 10, 2002, http://news.com.com/2100-1040-961536.html. One enterprising Aibo owner and hobbyist decrypted the software code that defined the Aibo's abilities and distributed new software to Aibo owners that "taught" the dogs to dance and speak, among other things. David Labrador, *Teaching Robot Dogs New Tricks*, SCIENTIFIC AMERICAN.COM, Jan. 21, 2002, http://www.sciam.com/print_version.cfm?articleID=0005510C-EABD-1CD6-B4A8809EC588EEDF. Despite the fact that the software was of use only to Aibo owners and arguably increased the product's value, Sony demanded removal of the software, contending that decryption of the Aibo code violated the DMCA. *Id.*

152. When Connectix developed its Virtual Game Station, a software emulator that enabled owners of Sony PlayStation games to play titles on Apple computers, Sony filed a copyright infringement suit, alleging that Connectix, by reverse engineering Sony's game console, infringed the copyright in the PlayStation BIOS. Sony Computer Entm't

In light of this corporate heritage, the difficulty of convincing consumers of the value of DRM-protected CDs, and its underestimation of public reaction to degraded security and privacy, Sony BMG's decision to deploy XCP and MediaMax, its attempts to cloak its technology and its failures of disclosure emerge as explicable, if irresponsible, reactions to market conditions. But while its motivations are apparent, the long-term strategic benefit of this approach is difficult to discern, especially with the benefit of hindsight. The limitations and strengths of both the CD and the personal computer as platforms for the dissemination and playback of content, which we examine next, constrained and enabled Sony BMG's choices, further explaining, but not excusing, its actions.

IV. THE ROLE OF TECHNOLOGY

The technological landscape encouraged Sony BMG's decision to deploy its DRM through stealth measures. The personal computer, in theory, allows users broad choice over the operating system and applications that run upon it. The universal nature of the PC sits in stark contrast to the single-purpose devices historically used by individuals to enjoy music. This flexibility limits the control that Sony BMG and other copyright owners

---

Am., Inc. v. Connectix Corp., 203 F.3d 596, 598-99 (9th Cir. 2000). After the Ninth Circuit reversed the district court's finding of infringement, *id.* at 609-10, Sony acquired all rights to the Virtual Game Station from Connectix and ceased development rather than allow consumers to access its games on a competitor's platform. Phillip Michaels, *Emulation Sensation: Microsoft Buys Virtual PC from Connectix*, MACWORLD, May 2003, at 25, 25, *available at* 2003 WLNR 8626928. Sony also filed suit against Bleem, the manufacturer of a PC-based PlayStation emulator, claiming that by using screenshots of Sony games in its advertising, Bleem infringed Sony's copyrights. The Ninth Circuit vacated the district court's preliminary injunction, holding that Bleem's use was likely fair. Sony Computer Entm't Am., Inc. v. Bleem, LLC, 214 F.3d 1022, 1029 (9th Cir. 2000).

After the release of the PlayStation 2, Sony brought suit against Gamemasters, the manufacturer of the Game Enhancer, a device that enabled PlayStation owners to play games from other countries by bypassing region code restrictions encoded on game discs. Sony Computer Entm't Am., Inc. v. Gamemasters, 87 F. Supp. 2d 976 (N.D. Cal. 1999). Sony succeeded in obtaining a preliminary injunction on both contributory infringement and anti-trafficking theories, precluding U.S. customers from playing games legally purchased in Asia and Europe. *Id.* at 989.

In hopes of exerting further control over the video game aftermarket, Sony obtained a patent in connection with its latest video game console, the PlayStation 3, on a technology that would tie each copy of a game to a single console, effectively eliminating the resale and rental market for PlayStation 3 games. Dawn C. Chmielewski, *Furor Over Sony Patent: Technology That Could Prevent Resale of Games and Other Digital Goods Raises Speculation, Fears*, L.A. TIMES, July 10, 2006, at C1. That technology has yet to be implemented.

can exert over the applications that will be used to access and copy their CDs. As a result of the inability to control the platform for content delivery, Sony BMG was encouraged to consider preemptively limiting potential infringement through the use of invasive software countermeasures. Further complicating efforts to control content, the music industry's longtime distribution medium of choice, the CD, is an unencrypted format. These inescapable features of the playback device and distribution medium encouraged the adoption of invasive DRM techniques such as those employed by Sony BMG.

Technology not only animated Sony BMG's strategy, it also enabled it. Sony BMG likely banked on its ability to keep the existence and functionality of its DRM relatively secret from the general public. The rootkit itself was designed to maintain secrecy, but equally importantly, the standard configuration of many personal computers allows third parties to surreptitiously install code, including the DRM at issue here, without alerting the user or requiring affirmative steps to proceed with installation.

A. Technology as Encouragement

In conjunction, two features of the technological landscape encouraged, if not required, the use of intrusive technological protection measures such as those employed by Sony BMG. Given the combination of a general purpose, multifunctional networked playback device with an entrenched but unencrypted digital distribution medium, the music industry's adoption of software-based technological protection measures seems, in hindsight, unavoidable.

1. The PC as Playback Device

From the perspective of many copyright holders, the PC is perhaps the least-desirable device imaginable for the playback of unprotected CDs. Unlike the single-purpose devices that consumers have traditionally used to listen to music, the PC is a general-purpose device, a machine with nearly unbounded functionality, limited primarily by the software running on it. As a result, PC users are able to not only listen to the music contained on a CD, but to copy, transcode, edit, remix, and distribute it as well.

Contrast this range of user freedoms with those permitted by analog playback devices like the phonograph—particularly in the days before reel-to-reel and cassette recorders—and modern digital playback devices, like the DVD player. Phonograph users, even well into the twentieth century, were constrained in their ability to make copies of recordings by the

dictates of the state of the art—the equipment required to press phonograph records was simply not feasible for consumer use.

While the limitations of early analog media were primarily the result of engineering hurdles that would be overcome by subsequent innovations, limitations on modern digital playback devices are largely the result of intentional design decisions targeted at curtailing the relative ease of digital copying. The functionality of DVD players, for example, is tightly controlled by the DVD Copy Control Association (DVD CCA), the industry body that licenses the Content Scramble System (CSS) and holds the keys necessary to manufacture devices and software that legally play DVDs. Indeed both the DVD medium and its playback devices were designed from the ground up to permit increased control over consumer use of content. By insisting that CSS licensees conform to rigid specifications, content owners enjoy some increased assurance that devices that copy DVDs will not be appearing on store shelves any time soon. And when its licensees offer product features that test the bounds of this control, the DVD CCA has brought suit to maintain its grip over the medium.[153]

Unlike the DVD player, the personal computer was not developed with copy control and content protection in mind. Computer users are free to add or replace hardware, to substitute one operating system for another, and to install or uninstall software—or, if sufficiently skilled, to write their own. A system that permits this level of flexibility does not lend itself to the sort of control to which copyright holders aspire when designing playback devices. Any restriction imposed by software can be removed by software. As a result, skilled and determined users are capable of defeating any software-based content protection scheme deployed on a standard PC.

In recognition of this fact, content owners have sought to embed protection measures at deeper levels of the machine's architecture. The development of trusted computing platforms was in essence an attempt to reinvent the PC in a manner that wrested control from the hands of users and entrusted it to hardware manufacturers, software developers, and content owners.[154] While some touted this approach for its potential security

153. Kaleidescape, the producer of a high-end home entertainment server that allowed customers to store hundreds of DVDs on a networked device, prevailed in a lawsuit alleging that it violated the terms of its DVD CCA license. Transcript of Proceedings at 66, 67, 70, DVD Copy Control Ass'n, Inc. v. Kaleidescape, Inc., No. 1-04-CV031829 (Cal. Sup. Ct. Mar. 29, 2007), *available at* http://www.kaleidescape.com/files/legal/DVDCCA-vs-Kaleidescape-Statement-of-Decision.pdf.

154. *See* Ross Anderson, *Cryptography and Competition Policy—Issues with "Trusted Computing,"* at 3-5, http://www.cl.cam.ac.uk/~rja14/Papers/tcpa.pdf; *see also*

benefits, others suspected that DRM was the true driving force behind trusted computing.[155] Microsoft's Palladium, for example, was intended to take advantage of specially developed Intel hardware to integrate digital rights management into the CPU itself.[156] By embedding features like remote attestation,[157] sealed storage,[158] and memory curtaining[159] into the trusted computing environment, this approach held some promise for content owners who hoped to exercise greater control over copyrighted material on PCs. But despite widespread adoption of the Trusted Platform

---

Chad Woodford, Comment, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management*, 75 U. COLO. L. REV. 253 (2004).

155. *See id.*

156. Electronic Privacy Information Center, Microsoft Palladium - Next Generation Secure Computing Base, http://www.epic.org/privacy/consumer/microsoft/palladium.html (last updated Nov. 11, 2002).

157. Remote attestation is a process by which software authenticates itself to a remote host. The user's local machine would share information about its hardware and software configuration in order for a remote machine to determine whether it will be trusted. Vivek Haldar et al., *Semantic Remote Attestation - A Virtual Machine Directed Approach to Trusted Computing*, *in* USENIX ASS'N, PROCEEDINGS OF THE THIRD USENIX VIRTUAL MACHINE RESEARCH & TECHNOLOGY SYMPOSIUM 29 (2004), *available at* http://www.usenix.org/events/vm04/tech/haldar/haldar.pdf. For example, users whose machines contained unauthorized software could be refused access by a remote website or service.

158. Sealed storage is a means by which the cryptographic keys necessary to access encrypted data are generated by authorized software rather than stored in the open on the user's machine. This approach is meant to ensure that content cannot be accessed by unauthorized software that could circumvent the limits imposed by authorized software. SETH SCHOEN, TRUSTED COMPUTING: PROMISE AND RISK (2003), http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.pdf; Arnd Weber & Dirk A. Weber, *Legal Risk Assessment of Trusted Computing. A Review*, INDICARE MONITOR, Feb. 24, 2006, at 58, *available at* http://www.indicare.org/tiki-download_file.php?fileId=174.

159. Memory curtaining is a technique that prevents one application from accessing the memory used by another application, preventing, for example, unauthorized programs from capturing content being played by an authorized program that enforces restrictions on use of that content. SCHOEN, *supra* note 158; *see also* Mike Burmester & Judie Mulholland, *The Advent of Trusted Computing: Implications for Digital Forensics*, *in* ACM ASS'N, PROCEEDINGS OF THE 2006 SYMPOSIUM ON APPLIED COMPUTING 283 (2006), *available at* http://www.cs.fsu.edu/~burmeste/tc.pdf. There are stronger methods for isolating memory and resources. Andrew Whitaker, Marianne Shaw, and Steven D. Gribble, *Scale and Performance in the Denali Isolation Kernel*, ACM SIGOPS OPERATING SYS. REV, Winter 2002, at 195, *available at* http://portal.acm.org/citation.cfm?doid=844128.844147.

Module specifications,[160] trusted computing has yet to yield any radical transformation of the computing environment.

2. *The Lack of an Encrypted Format*

For the majority of its nearly 30-year history, the Compact Disc format, first developed in the late 1970s by Philips and Sony, has enabled consumers to freely access and copy CD content.[161] The CD, unlike later-developed digital formats like the DVD,[162] includes no content encryption.[163] Digital audio tracks on CDs can be read and copied by any compatible hardware, even in the absence of any cryptographic key. But by the late 1990s, after recordable CD media and hardware became commonplace and use of peer-to-peer networks became widespread, copyright holders sought to exercise greater control over the post-sale use of CDs. Given the massive user base of the CD and the investments of both content owners and consumer electronics manufacturers in the format, record labels faced a difficult task. They needed to devise methods to prevent unwanted PC-based copying while simultaneously maintaining usability on standard audio equipment. This required grafting protection measures onto a preexisting unencrypted format while retaining backwards compatibility.

Two general approaches to this problem emerged and can be broadly categorized as either passive or active. Passive protection measures rely on changes to the structure and data contained on the CD to prevent copying.[164] Active protection measures, like XCP and MediaMax, on the other hand, rely on the installation of software on the user's computer to interfere with the accessing and copying of audio files.[165]

---

160. For details on the Trusted Platform Module specifications, see Trusted Computing Group, Trusted Platform Module (TPM) Specifications, https://www.trustedcomputinggroup.org/specs/TPM (last visited July 30, 2007).

161. *See* J. Alex Halderman, *Evaluating New Copy-Prevention Techniques for Audio CDs*, *in* ACM ASS'N, PROCEEDINGS OF THE 2002 ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT 101 (2002), *available at* http://www.cs.princeton.edu/~jhalderm/papers/drm2002.pdf.

162. The vast majority of commercially available DVDs utilize CSS, a method of encryption meant to ensure that only authorized devices and software can be used to access content. The DVD CCA's tight control over licensing of the keys necessary to access DVDs has successfully prevented the distribution of devices that enable users to copy DVDs. *But see DVD Copy Control Ass'n, Inc.*, *supra* note 153.

163. *See* Halderman, *supra* note 161.

164. For a study of the effectiveness of passive protection measures, see *id.*

165. Halderman & Felten, *supra* note 11, at 4.

Each song on a CD is stored as an individual track. Each track comprises a number of frames, each of which holds 1/75 second of audio.[166] In addition, parallel data streams, called subchannels, are multiplexed with each track's main data.[167] These subchannels mark the divisions between tracks, the track number, and the current track running time.[168] Aside from the track data, each CD contains a table of contents (TOC) which indicates the number of tracks and the starting position of each track.[169]

By introducing errors into CD data and the TOC, passive protection measures attempt to exploit subtle differences in the hardware and software of standard audio equipment and PCs.[170] For example, because the CD specification requires a two second gap before the beginning of the first track,[171] many PC CD drives specify time 00:02.00 as frame 0. By altering a TOC to indicate that the first track starts at time 00:01.74, passive protection measures can cause failure when a PC attempts to read the disc.[172] But since standard CD players use a different frame address scheme, the altered TOC typically does not interfere with playback.[173] Other passive measures rely on changes to the track data itself. Most CD players, for example, interpolate over errors caused by corrupt audio samples.[174] But since most PC CD-ROM drives cannot correct for such errors, by intentionally including corrupt samples, passive measures can interfere with the ability of PC drives to properly read protected discs without affecting playback on standard audio equipment.[175]

For a variety of reasons, passive protection measures proved to be at best an incomplete solution. First, some common audio components were unable to play back CDs with passive protection. Car stereos and DVD players with CD playback functionality often encountered difficulties with passively protected discs.[176] Second, not all PC drives were susceptible to

166. *Id.*
167. *Id.*
168. *Id.*
169. Halderman, *supra* note 161.
170. *Id.*
171. *Id. See also* INTERNATIONAL STANDARD NO. 60908, Audio Recording—Compact Disc Digital Audio System (Int'l Electrotechnical Comm'n 1999).
172. Halderman, *supra* note 161.
173. *Id.*
174. *Id.*
175. *Id.*
176. Will Knight, *Philips Says Copy-Protected CDs Have No Future*, NEW SCIENTIST, Jan. 11, 2002, http://www.newscientist.com/article.ns?id=dn1783; *Sony's 'Copy-Proof' CD Fails to Silence Hackers*, USA TODAY, May 20, 2002, http://www.usatoday.com/money/tech/2002-05-20-copyproof-cd.htm.

the rather crude methods relied upon by passive protection.[177] And as these methods became more prevalent, new drives were designed to eliminate the shortcomings of earlier hardware.[178] Even for computer users whose drives had difficulty reading passively protected discs, the careful application of tape or a felt tip pen could defeat passive DRM.[179] As a result, passive protection was largely abandoned in favor of active protection measures, which leave audio playback devices wholly undisturbed while providing greater and more flexible control over PCs.[180] However, unlike passive protection measures, active protection measures introduced an additional difficulty for content owners and developers of protection measures: since active measures operate by means of software running on users' machines, these measures needed to guarantee the installation of software most users would reject if given the choice. Luckily for copy protection proponents, the Windows computing environment made such installation without consent surprisingly easy.

B. Technology as Enablement

Technology not only motivated Sony BMG's choice to deploy invasive software-based DRM, but also provided the means to execute this strategy. Once installed, the rootkit itself helped to ensure that average consumers remained unaware of the software Sony BMG had installed on their machines. What enabled the stealth installation of the DRM software in the first place, however, was a standard feature of the dominant PC operating system: Sony BMG relied on the AutoRun feature of the Windows operating system to run and install code on users' machines without notice or consent.

AutoRun allows software code contained on removable media, like CDs, to run automatically when inserted into a computer. When a CD is inserted into a computer, Windows scans the disc for a file named "AutoRun.inf."[181] If that file is present, Windows faithfully executes its instructions.[182] The file could instruct the computer to launch a program, open a particular website, or take some other more harmful action. Despite the

177. *See* Halderman, *supra* note 161.

178. Halderman & Felten, *supra* note 11, at 8.

179. *See* Halderman, *supra* note 161.

180. Some later discs used a combination of active and passive protection measures. Edward W. Felten & J. Alex Halderman, *Digital Rights Management, Spyware, and Security*, IEEE SECURITY & PRIVACY, Jan.-Feb. 2006, at 18, *available at* http://www.computer.org/portal/cms_docs_security/security/2006/v4n1/18-23.pdf.

181. Halderman & Felten, *supra* note 11, at 5.

182. *Id.*

potentially destructive power ceded by AutoRun, Microsoft included no meaningful safeguards for computer users.

Using AutoRun, Sony BMG was able to install DRM software on computers without the knowledge or consent of users. Upon insertion of an XCP disc, AutoRun launched an installer program that presented users with the terms of the XCP EULA. If the user "accepted" the EULA terms, XCP installed software to play the CD and copy DRM-protected Windows Media files. These files, unlike MP3 files, cannot be copied to Apple's iPod or other portable media players. If a user instead rejected the EULA, the CD was ejected from the machine. Furthermore, if a user launched an audio program prior to accepting the EULA and installing XCP, the auto-launched installer gave the user thirty seconds to exit that program before the disc was ejected.[183] For many, if not most, users, this procedure meant that the only way to listen to a protected disc on a computer was to install XCP.

MediaMax employed even more aggressive tactics with the help of AutoRun. When inserted, MediaMax discs used AutoRun to install, without notice or consent, a device driver that altered the user's CD-ROM drive to prevent playback of MediaMax discs. Next, the installer presented the EULA. If accepted, the MediaMax software was installed. But if the user instead refused the terms of the EULA, the disc was ejected. Even if the user refused to accept the EULA, and the CD was ejected, SunnComm's MediaMax technology often remained installed on the user's computer—saddling users with all of the security and privacy vulnerabilities but providing no access to the music they purchased.[184]

In the face of predictable user reluctance to actively impede their own lawful uses of legally purchased CDs, Sony BMG and its DRM vendors leveraged the dominant operating system's lack of end user control over software installation decisions to clandestinely alter the personal computing environment of millions of users. In doing so, Sony BMG relied in part on methods used by spyware distributors to spread malicious code and seize remote control of users' computers. Arguably, the decision to use these stealth techniques was motivated by the same desires—limiting user knowledge, engagement, and choice—that motivate their use in the spyware and malware contexts.

Sony BMG's use of these techniques occurred against a backdrop of efforts by companies, including Microsoft, to bolster user control over

183. *Id.* at 6.
184. *Id.* at 7.

software installation through industry-wide efforts to create more meaningful and effective consent mechanisms[185] and product design to prevent the installation of spyware.[186] These efforts recognized that the categorization of products as malware or spyware depends as much on the consent experience and on satisfying user expectations as it does on a product's functionality. Since the rootkit incident, Microsoft has taken at least one step that increases end user control over software installation. In Windows Vista, its most recent operating system, Microsoft has altered the AutoRun mechanism. On first encounter with an AutoRun disc, the user has the opportunity to permit or deny the automatic execution of code and can set defaults for future AutoRun discs.[187] The lessons learned from Sony BMG's decision to use AutoRun, and its misuse in other "drive-by" download exploits no doubt influenced this redesign. It is more consistent with the principles of usable security discussed below, and will likely assist users in avoiding the installation of some insecure software.

V. EXISTING LAW AND SKEWED INCENTIVES

Sony BMG has paid dearly for its deployment of XCP and MediaMax through the investigations, litigation, and settlements that came in the wake of the rootkit incident.[188] The example made of Sony BMG will

185. The difficult of delineating "spyware" solely on the basis of software behavior has led legislators and industry to focus increasingly on the quality of the notice and consent procedures around a software program's installation in addition to its behavior. The Anti-Spyware Coalition's Best Practices Guide is an example of this revival of interest in constraining reasonable notice and consent mechanisms and procedures. *See* ANTI-SPYWARE COALITION, BEST PRACTICES: GUIDELINES TO CONSIDER IN THE EVALUATION OF POTENTIALLY UNWANTED TECHNOLOGIES (2007), *available at* http://www.antispywarecoalition.org/documents/documents/best_practices_final_working_report.pdf.

186. *Id.*; ANTI-SPYWARE COALITION, BEST PRACTICES: FACTORS FOR USE IN THE EVALUATION OF POTENTIALLY UNWANTED TECHNOLOGIES (2007), *available at* http://www.antispywarecoalition.org/documents/documents/best_practices_public_comment_draft.pdf.

187. MICROSOFT CORPORATION, WINDOWS VISTA SECURITY GUIDE ch. 3 (2006), http://www.microsoft.com/technet/windowsvista/security/protect_sensitive_data.mspx; CD AutoRun Basics: Windows Vista AutoPlay and AutoRun, http://www.phdcc.com/shellrun/AutoRun.htm#vista (last modified Dec. 19, 2006).

188. *See, e.g.,* Settlement Agreement, *supra* note 69; Robert McMillan, *Second Sony Rootkit Settlement Ups Payout to $5.75M*, COMPUTER WORLD, Dec. 21, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9006620; Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf.

likely shape future DRM deployments by injecting security considerations into their development and by influencing notice and consent practices.[189] These developments, as we discuss in Part VI, provide a solid foundation for broader interdisciplinary efforts to improve privacy and security in the online environment. But rather than analyze the sufficiency of the price paid by Sony BMG for its misdeeds, we seek to understand why existing law failed to prevent the deployment of DRM with known security and privacy risks. In hindsight, it is apparent that Sony BMG's decision to deploy its DRM was woefully misguided, and that the statements about its data collection were inaccurate and incomplete. Assuming Sony BMG had competent legal counsel, the question is why the law failed to clearly alert Sony BMG of the illegality of this strategy. Equally important is an understanding of the failure of the law to empower users with the information and control to avoid these security and privacy risks.

A complicated picture emerges. We contend in Section V.A that Sony BMG's likely reliance on the hidden nature of the DRM's functionality was buttressed in part by the Digital Millennium Copyright Act's anti-circumvention rules, which discourage experts from studying the security risks posed by technological protection measures. By exposing security researchers to liability for their research, the DMCA discourages the front-line of security defense in the online environment. The anti-trafficking rules similarly interfere with the distribution of information or tools that could assist users in disabling technological protection measures, like the Sony BMG DRM, in order to avoid risks to their privacy and security. Second, existing contract law has failed to set meaningful limits on the substance and formalities of click-wrap contracting. The unwillingness of courts to set substantive limits on EULAs and to critically consider the consent experience created an environment in which unreasonable material terms can be inserted into EULAs with impunity. And without a meaningful consent experience, users cannot even hope to have notice of the terms foisted upon them by these mass-market form contracts. Third and finally, the focus of U.S. privacy initiatives on a narrowly defined class of "personally identifiable information" created uncertainty about privacy rules for businesses using unique identifiers, such as IP addresses, to identify or monitor users. By discouraging security research on technological protection measures, failing to take a hard look at the terms and

189. Pamela Samuelson & Jason Schultz, *Regulating Digital Rights Management Technologies: Should Copyright Owners Have to Give Notice About DRM Restrictions?*, J. TELECOMM. & HIGH TECH. L. (forthcoming 2007) (manuscript at 17, available at http://www.ischool.berkeley.edu/~pam/papers/notice%20of%20DRM-701.pdf).

formalities of "click-wrap" agreements, and neglecting to provide guidance on privacy issues beyond those arising with "personal identifying information," courts and regulators failed to strike the appropriate balance between commercial convenience, on the one hand, and consumer protection and empowerment, on the other.

A. The DMCA's Veil of Secrecy

At present, federal law does not explicitly endorse invasive attacks by copyright holders against the computers of suspected infringers. Proposals like H.R. 5211, introduced by Representative Howard Berman in 2002, would have enabled such self-help hacking in the name of enforcing intellectual property rights.[190] Congress rightly rejected this approach.[191] But even in the absence of any official congressional imprimatur on invasive self-help, Congress has created a set of disincentives through the DMCA that, if not appropriately checked, could yield the same result—namely, unrestrained and overzealous copyright enforcement mechanisms that endanger the security of personal computers and the network generally.

This Section considers the implications of the DMCA on the security researchers who serve as the primary source of information regarding abusive protection measures for the public, law enforcement, and regulators. By imposing potential liability for discovery, disclosure, and deactivation of harmful protection measures, the DMCA was perhaps the primary component of the legal framework that failed to prevent the rootkit incident.

In the weeks and months prior to the public disclosure of the XCP rootkit, two prominent computer security and DRM researchers, Professor Ed Felten and J. Alex Halderman, were forced to divide their energy between researching and publicizing the dangerous implications of Sony BMG's protection measures, on the one hand, and engaging in protracted discussions of potential DMCA liability with both their outside legal team and the general counsel of their academic institution, on the other.[192] The

190. H.R. 5211, 107th Cong. (2d Sess. 2002), *available at* http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.5211:.

191. Legislative History of H.R. 5211, 107th Cong. (2002), http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR05211:@@@X.

192. Halderman and Felten were clients of the Samuelson Law, Technology & Public Policy Clinic directed by Mulligan. Perzanowski was the student most intimately and continuously involved in advising Halderman and Felten. Clinic Fellow Jack Lerner and clinic student interns Sara Adibisedeh, Azra Medjedovic, and Brian W. Carver all participated in the representation at various times. Joseph Lorenzo Hall, a Ph.D student at Berkeley's Information School and a long-standing participant in the Samuelson Clinic's

caution displayed by Halderman and Felten is hardly surprising given their personal histories with the DMCA. Both have been threatened with legal action in the past and are therefore acutely aware of the exacting toll of litigation threats, regardless of the merits of the claims.[193] But the necessary delay caused by legal uncertainty left millions at risk for weeks longer than necessary.

In broad terms, the DMCA undergirds the technological protection measures adopted by copyright holders with the force of law. The statute prohibits circumvention of any measure that effectively protects access to a copyrighted work.[194] In addition, the DMCA imposes liability on those who traffic in tools, devices, components, or services primarily designed, marketed, or commercially viable only for the purpose of circumventing protection measures that control access to or copying of copyrighted works.[195] Both the anti-circumvention and anti-trafficking provisions of the DMCA contribute to the ominous shadow that hangs over researchers examining the security of any product protected by a technological protection measure,[196] a pall most strongly felt by those examining the protection

---

research, provided technical advice and support to law students working on this project. As Felten and Halderman wrote, "Sadly, research of this type does seem to require support from a team of lawyers." As much as the lawyers enjoyed the privilege of working with and representing interesting people doing important work, they share their former clients' dismay at this particular state of affairs.

193. In 2000, Felten and a team of researchers, after accepting a challenge from the Secure Digital Music Initiative (SDMI), succeeded in breaking SDMI's digital audio watermark. After facing legal threats under the DMCA, Professor Felten filed for declaratory judgment seeking a determination that his research did not violate the DMCA. Only after the RIAA disavowed any intent to file suit was that action dismissed. *See Tinkerers' Champion*, THE ECONOMIST, June 22, 2002; First Amended Complaint, Felten v. Recording Indus. of Am., Inc., No. CV-01-2660 (D.N.J. June 26, 2001), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010626_eff_felten_amended_complaint.html.

In 2003, Halderman published an academic paper discussing his research on SunnComm's MediaMax protection measure. *See supra* note 4. Shortly thereafter, SunnComm threatened Halderman with legal action for his academic publication. Kevin Maney, *Debate Heats Up as Student Spots Hole in CD Protection*, USA TODAY, Oct. 27, 2003, at 1A. After scathing criticism of its attempt to silence legitimate research, SunnComm publicly retracted this threat. *See* Lisa Napoli, *Compressed Data; Shift Key Opens Door to CD and Criticism*, N.Y. TIMES, Oct. 13, 2003, at C3.

194. 17 U.S.C. § 1201(a)(1)(A) (2000).

195. 17 U.S.C. § 1201(a)(2), (b)(1) (2000).

196. *See generally* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004); Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

measures applied to creative works—music, movies, novels—that the DMCA was intended to protect.[197]

In their efforts to determine the security threats posed by DRM systems like XCP and MediaMax, researchers are likely to disable or remove some portion or the entirety of the protection measure, and thus potentially run afoul of the DMCA's prohibition against circumvention.[198] Assuming researchers—and their institutions—are willing to accept these risks, they could face further threats of litigation for publishing the results of their research. To the extent that publication of sufficiently detailed findings enabled others to circumvent the protection measure, it could lead to claims of trafficking. Although such claims are unlikely to succeed,[199] the

197. As discussed *supra*, the Digital Millennium Copyright Act (DMCA) has been used to threaten academic research. But the chilling effect of the DMCA has extended far beyond security research. It has impeded tinkering with online games and gadgets and interfered with online speech. *See supra* notes 151 and 152; ELECTRONIC FRONTIER FOUNDATION, UNINTENDED CONSEQUENCES: SEVEN YEARS UNDER THE DMCA (2006), http://www.eff.org/IP/DMCA/DMCA_unintended_v4.pdf.

Nor is the DMCA the only legal barrier to improving computer security. Bucking the call for growing scrutiny and improvement of electronic voting technology, dominant election system vendors have used the threat of legal action based on intellectual property violations to interfere with competition, impede the review of electronic systems by regulators, and chill public discourse about the lax security of their machines. For an overview of the issues faced by election officials see AARON BURSTEIN ET AL., SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC, LEGAL ISSUES FACING ELECTION OFFICIALS IN AN ELECTRONIC-VOTING WORLD (2007), http://www.law.berkeley.edu/clinics/samuelson/projects_papers/Legal_Issues_Elections_Officials_FINAL.pdf.

198. The great irony, of course, is that although during the exploration of the security risks posed by the DRM researchers are likely to disable or remove some portion or the entirety of the protection measure, and thus potentially run afoul of the DMCA, engaging in such research does not constitute copyright infringement. Indeed, security researchers are concerned with the manner in which protection measures function and the security threats they may pose; they have no interest in the copyrighted content those measures are meant to protect.

199. Statements made by the Department of Justice in *Felten v. RIAA* are instructive. In that case, the DOJ argued against an interpretation of "tools" that would include "normal scientific research" and publishing. Defendant John Ashcroft's Memorandum in Support of Motion to Dismiss, at 17, Felten v. Recording Indus. Ass'n of Am., No. 01-CV-2669 (D.N.J. Sept. 25, 2001) ("[t]he Plaintiffs are scientists attempting to study access control technologies. The DMCA simply does not apply to such conduct."). The DOJ did reserve the possibility that "making available a publication that describes in detail how to go about circumventing a particular technology, if written or marketed for the express purpose of actually circumventing that technology," could be prosecuted under the statute. *Id.* at 17 n.5. Some cases involving defendants who publicly distribute and advertise what effectively amount to step-by-step instruction guides on how to commit crimes have resulted in successful prosecutions in other areas. *See, e.g.*, Rice v. The Pala-

threat of litigation and the associated expense is sufficient to alter research agendas. Finally, assuming researchers discovered a security flaw that posed a significant threat to the public, as in the case of Sony BMG's DRM, and sought to provide a tool to enable the average computer user to quickly and safely avoid the harms posed by the protection measure, they almost certainly would raise the ire of the content industry to a fever pitch and draw a trafficking claim under the DMCA. Together the anti-circumvention and anti-trafficking provisions chill computer security research and create enormous disincentives to provide the information and tools necessary to enable computer users to avoid security and privacy risks once dangerous technologies have been deployed.

A detailed analysis of potential liability under the DMCA and the ways in which it complicates research, publication, and the dissemination of tools related to DRM is beyond the scope of this Article.[200] Nonetheless, there are good reasons to doubt that liability should attach in these circumstances. First, the more enlightened courts to analyze the DMCA recognize that liability requires some nexus between the act of circumvention and an act of copyright infringement.[201] Where circumvention and

---

din Enters., 128 F.3d 233, 266-67 (9th Cir. 1997); United States v. Barnett, 667 F.2d 835, 842 (9th Cir. 1982). However, sharing general information about how to commit criminal acts that is unlikely to incite others to imminently take lawless action typically fails to justify restricting its expression. McCoy v. Stewart, 282 F.3d 626, 632 (9th Cir. 2002). Given that security research is not marketed for the purpose of circumvention, it is unlikely to be found to incite others to imminently commit unlawful acts.

200. As counsel to Halderman and Felten, the authors have conducted an exhaustive analysis of this issue.

201. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004), succinctly sets forth the applicable law on this point:

> A plaintiff alleging a violation of § 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either: (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.

Chamberlain Group, Inc., 381 F.3d at 1203; *accord* Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (in order to prevail in a DMCA claim, the plaintiff must also be able to succeed on the merits in an underlying copyright infringement suit).

publication take place in the context of academic research, courts should be reluctant to find the requisite nexus.

Second, at least with respect to Sony BMG's DRM, it is far from clear that the technological protection measures at issue would have been found to "effectively control access" to the CDs.[202] Absent such a finding, research and subsequent publication, or even distribution of a tool, would not be actionable under the DMCA's anti-circumvention and anti-trafficking provisions.[203] In *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, the Sixth Circuit explained that section 1201(a)(2) does not extend to a technological measure that restricts one form of access but leaves another route wide open.[204] XCP and MediaMax both left audio content unprotected and accessible by other obvious means.[205] Purchasers could access the tracks without restriction on their CD players, any Apple computer, or any Windows machine on which AutoRun was disabled.[206] Under these circumstances, the availability of DMCA protection is an open question.

---

202. Per the statute, "controls access to a work" means that if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work. 17 U.S.C. § 1201(a)(3)(B) (2000).

203. 17 U.S.C. § 1201 (a), (b) (2000).

204. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

205. Some files, such as bonus video content or compressed audio files, are not accessible through these other means. But since removal of the protection measure does not grant access to these files, the fact that they remain protected cannot support a claim of circumvention.

206. DRM vendors and copyright holders would likely have argued that their controls are effective "in the ordinary course of its operation," i.e., in the environment in which they were intended to be used. This argument assumes that the DRM vendors have some authority to control the underlying configuration of a user's machine. Given that access to the audio files is not protected on some standard-configured Windows computers and on Macs, this argument would implicitly suggest that users with "normally configured" machines are engaged in illegal circumvention. To succeed on this argument, Sony BMG would have to convince the court to adopt the position that the licensor has the right to control the general computing environment in which the consumer makes personal use of the CD audio files. It is difficult to imagine this argument proving persuasive, given its rather radical and broad implications, and given that its adoption would run counter to the "no technology mandates" provision in the DMCA, which states: "Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure . . . ." 17 U.S.C. § 1201(c)(3) (2000).

An additional wrinkle in the analysis of potential liability facing researchers arises from the security testing exemption in section 1201(j), which applies to both the anti-circumvention provision and the anti-trafficking provision of 1201(a). It is the only statutory exemption that could potentially shield security researchers who disable protection measures like XCP and MediaMax and traffic in tools that enable others to avoid security risks. However, the scope of this exemption is, at best, uncertain,[207] and its applicability to the rootkit incident and similar potential circumstances is unsettled. First, section 1201(j)(1) limits the definition of "security testing" to "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing."[208] This definition may not apply to circumvention of technological measures that protect third party content stored on removable media, such as sound recordings on CDs, that are distinct from the computer, system, or network. The scant legislative history offers some support for this reading. Section 1201(j) was adopted to accommodate concerns raised by developers of firewalls who wanted to ensure that they, their customers, and their competitors could test the effectiveness of their products.[209] In addition, since the sole purpose of security research is not to "promote the security of the owner or operator," but rather to protect the security of the public broadly—a purpose that may require widespread publication of information regarding removing the protection measure at issue—this sort of research could run

207. Section 1201(j) has been given short shrift in judicial opinions addressing the DMCA. Aside from a passing and dismissive reference in *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294, 321 (S.D.N.Y. 2000), the exemption has been ignored by both courts and litigants. What attention the *Reimerdes* court did pay to 1201(j) was marred by a misreading of the statute. The court held that because "defendants sought, and plaintiffs granted, no authorization for defendants' activities" § 1201(j) did not apply. *Id.* The leading academic interpreting the statute also finds that the statute requires authorization. *See* Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1648 n.339 (2002) ("The computer security exception requires that the researcher actually get, and not just ask for, permission to defeat the technical protection measure."). However, the statute requires authorization not from the copyright holder, but from the owner or operator of the computer. This *Reimerdes* court's reading is therefore almost certainly a misapplication of the statute.

208. 17 U.S.C. § 1201(j) (2000).

209. The Conference Report on the DMCA offers further support for this narrow reading of the definition of security testing under 17 U.S.C. § 1201(j). That report explained, "It is not unlawful to test the effectiveness of a security measure before it is implemented to protect the work covered under title 17. Nor is it unlawful for a person who has implemented a security measure to test its effectiveness." H.R. REP. NO. 105-796, at 67 (1998) (Conf. Rep.).

afoul of the statute.[210] As discussed *infra*, the scope of the security research exemption was sufficiently unclear to justify the Copyright Office's decision to grant a temporary exemption to enable research on security-flawed CD-based protection measures.

Even assuming a competent legal team and success on the merits, defending against a DMCA suit consumes enormous resources. The threat of litigation understandably chills security research related to DRM. Suppressing research of this sort disables an important check on the safety and soundness of products in the consumer marketplace. Just as Consumers Union and other independent analysis and benchmarking entities act as independent checks on quality and safety for consumer products, computer security researchers play an important role in evaluating the security, privacy, usability, and other consumer-relevant effects of software. Preventing computer security researchers from evaluating products that contain technological protection measures removes an important player in the market ecosystem with respect to consumer protection.

Without the efforts of security researchers who discovered and publicized the risks created by Sony BMG's DRM,[211] consumers and policymakers would be nearly universally uninformed about security threats and other unknown consequences of DRM—a fact likely well understood by copyright holders who choose to deploy stealth protection measures with undisclosed functionalities. The vast majority of computer users lack the expertise to discover these threats independently. There is no government agency that is explicitly authorized to examine DRM or other technological protection measures to assess their policy implications or ramifications—security or other—on behalf of consumers. As a result, consumers must either rely on the research conducted by security experts[212] or blindly trust software developers and content owners to exercise restraint in designing protection measures that respect consumers' privacy and security interests.[213]

---

210. 17 U.S.C. § 1201(j)(3) (2000).

211. *See supra* Section I.A.

212. The DMCA harms consumers not only by denying them the expertise of researchers, but also by imposing liability for self-help. Once some information regarding the existence and functionality of a protection measure becomes available, many enterprising users could remove it on their own. However, the DMCA creates threats against users as well as researchers.

213. Posting of Ed Felten & J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=927 (Nov. 15, 2005, 07:07 EST). The rootkit incident and the historic use of monitoring in online content distribution systems suggests that such reliance would be misplaced. Deirdre K. Mulligan et al., *How DRM-based Content Delivery*

B. The Insufficiency of Consent

Aside from the force of law conferred by the DMCA, Sony BMG's DRM scheme benefited from some degree of legal protection offered by its software licenses. These licenses arguably enabled Sony BMG to maintain that users of XCP and MediaMax assented to the installation and functionality of Sony BMG's DRM. But the vast majority of Sony BMG customers lacked any meaningful understanding of the functionality of these protection measures, in part as a result of Sony BMG's misleading license terms and in part because of deficiencies in the consent experience associated with click-wrap licenses generally. Despite these barriers to meaningful consent, under contemporary contract doctrine, most of the terms of the XCP and MediaMax EULAs would be enforced against users, further emboldening Sony BMG.

XCP and MediaMax, like almost all consumer software, were distributed under the terms of EULAs. Typically EULAs disclose, among other things, the data collection, advertising, and other program functionalities of software, and require a "click" or other affirmative act to acknowledge the user's consent to the terms. In the case of the Sony BMG DRM protected CDs, the EULAs contained false statements claiming that no personal information would be collected about the user or their computer.[214] Indeed, the EULA governing DRM-protected Sony BMG CDs explicitly disavowed any collection or dissemination of data related to customers or their computers. The XCP EULA stated in part "the SOFTWARE will not be used at any time to collect any personal information from you, whether

---

Systems Disrupt Expectations of "Personal Use", in ASS'N FOR COMPUTING MACHINERY, PROCEEDINGS OF THE 3RD ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT 77 (2003).

214. The EULA stated, "[T]he SOFTWARE will not be used at any time to collect any *personal information* from you, whether stored on YOUR COMPUTER or otherwise." Sony BMG MediaMax EULA (emphasis added) (on file with authors). The use of the term "personal information", rather than "personally identifiable information", created exposure here for Sony BMG, as discussed *infra* in Section V.C. Information at the SunnComm Sony BMG customer care website further misleads consumers, stating, "*No information* is ever collected about you or your computer without you [sic] consenting" and also states: "Is any personal information collected from my computer during the digital key delivery process? No, during the digital key delivery process, no information is ever collected about you or your computer." Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST) (emphasis added). The lack of *any* modifiers with respect to "information" is startling. This statement would prohibit any connection to a remote server. The lack of consistency in terminology across the documents and the failure to use existing legally accepted definitions to describe the data they were claiming not to collect proved exceedingly problematic.

stored on YOUR COMPUTER or otherwise."[215] The MediaMax license agreement contained similar language.[216] In fact, both the XCP and MediaMax DRM collected and transmitted to Sony BMG the user's IP address, the time the CD was played, and a code corresponding to the particular CD title being played. Additionally, the EULA contained a host of overreaching terms.[217] The most significant was a provision permitting Sony BMG to install and use backdoors in the DRM and media player to enforce its rights at any time and without notice to the user.[218] Like the security threats introduced by XCP and MediaMax, the overreaching, false, and confusing statements found in the EULA were of the sort typically associated with spyware.

Since components of Sony BMG's DRM installed—sometimes permanently—before customers were confronted with the EULA terms, the CD packaging provided the only available means of pre-installation notice. But the information conveyed by the packaging left much to be desired. It too failed to provide adequate information about the installation and functionality of the software. XCP-protected discs contained the IFPI "Content Protected" logo on the front of the CD jewel case spine[219] and a small "content protection grid," illustrated below in Figure 1, on their back covers.[220] The majority of MediaMax discs included similar grids.[221] Others featured ambiguous disclosures in miniscule type, buried within system requirements.[222] Some neglected to inform customers that the CD

215. Sony BMG XCP EULA (Jan. 7, 2005) (on file with authors).

216. "At no time will any information provided by you in connection with the installation of the software system be collected about you or your computer." Sony BMG MediaMax EULA, *supra* note 214.

217. *See supra* note 27.

218. "As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program (the 'SOFTWARE') onto YOUR COMPUTER. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. Once installed, the SOFTWARE will reside on YOUR COMPUTER until removed or deleted." Sony BMG XCP EULA, *supra* note 215.

219. Electronic Frontier Foundation, *supra* note 57.

220. CD's Containing XCP Content Protection Technology, Sony BMG, http://cp.sonybmg.com/xcp/english/titles.html.

221. Electronic Frontier Foundation, *supra* note 57.

222. For a number of examples, see Gallery of Variations on SunnComm MediaMax CD Labeling, http://www.eff.org/IP/DRM/Sony-BMG/mediamaxpics.php (last visited Sept. 6, 2007).

would automatically install software on their systems,[223] while others failed to disclose any of the restrictions on copying or accessing content imposed by the MediaMax software.[224] These half-hearted disclosures failed to provide Sony BMG customers with fair warning of the security and privacy threats or the scope of the limitations on use imposed by its DRM.

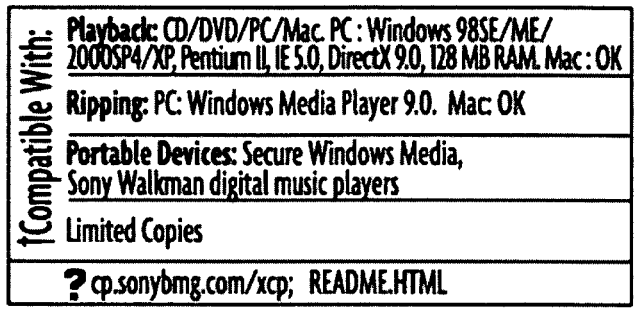

Figure 1

Users who took the time to sift through the nearly 3000-word XCP EULA[225] gleaned some additional detail beyond the cursory notice provided on the CD packaging. But the EULA failed to fully disclose the security and privacy risks imposed by Sony BMG's protection measures. Once customers purchased CDs and attempted to listen to them using their computers, the EULA—assuming they read it[226]—informed them:

> Before you can play the audio files on YOUR COMPUTER or create and/or transfer the DIGITAL CONTENT to YOUR COMPUTER, you will need to review and agree to be bound by

---

223. *See, e.g.*, http://www.eff.org/IP/DRM/Sony-BMG/img/cubanlink_close.jpg ("THIS CD IS ENHANCED WITH MEDIAMAX SOFTWARE AND PROTECTED AGAINST UNAUTHORIZED DUPLICATION.")

224. Some stated:

> This CD is enhanced with Media Max software . . . . Software will automatically install . . . . Usage of this CD on your computer requires acceptance of the End User License Agreement and installation of specific software contained on this CD . . . . Certain computers may not be able to access the enhanced portion of this disc. None of the manufacturer, developer, or distributor [sic] makes any representation or warranty, or assumes any responsibility, with respect to the enhanced portion of this disc.

See http://www.eff.org/IP/DRM/Sony-BMG/img/contraband_close2.jpg

225. Sony BMG XCP EULA, *supra* note 215.

226. Users frequently ignore or fail to read EULAs. Nathaniel Good et al., *User Choices and Regret: Understanding Users' Decision Process About Consensually Acquired Spyware*, 2 I/S: J.L. & POL'Y FOR THE INFO. SOC'Y. 283 (2006).

> an end user license agreement . . . . As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program (the "SOFTWARE") onto YOUR COMPUTER. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT.[227]

So while the EULA informed users that a small program would be installed on their machines, it provided no information about the specific restrictions that program placed on use of the CD or the manner in which it operated. Even customers who proactively sought information about the XCP software had no way, short of installing the software and running sophisticated diagnostic tests,[228] to discover the security vulnerabilities it introduced or that its explicit assurances regarding the collection of personal information were false. The same held true for the MediaMax EULA.[229] All but the most sophisticated users were left to blindly trust Sony BMG's incomplete and misleading disclosures. By doing so, they unwittingly opened their PCs to crippling attacks and their personal information to collection and transmission, both in exchange for restricted access to the music they believed they had purchased.

Because the EULA did disclose, albeit poorly, provisions that provided for Sony BMG's backdoor access and remote control over the user's computer—the provisions posing the greatest threats to security—courts would likely enforce those terms.[230] While EULA language is typically far from clear, even for those familiar with legal documents, courts are reluctant to excuse violations on the basis of unclear language. Nor do courts excuse consumers from license obligations on the basis of their failure to read EULA terms. As a matter of contract formation, courts typically find

---

227. Sony BMG XCP EULA, *supra* note 215.

228. Exceedingly few users possess the software and know-how necessary to conduct the sort of investigation engaged in by Mark Russinovich or Felten and Halderman. *See* Mark's Blog, *supra* note 6; Halderman & Felten, *supra* note 11.

229. "In order to properly utilize this CD on your computer, it is necessary to install a small software program on your computer hard drive." Sony BMG MediaMax EULA, *supra* note 214.

230. *See* Jane K. Winn, *Contracting Spyware by Contract,* 20 BERKELEY TECH. L.J. 1345 (2005). The doctrine of unconscionability, while unlikely to succeed, would provide the strongest basis for voiding this particular term. The form contracting of the EULA, the unexpected behavior of the software, and the general surprise of consumers that any software at all was being downloaded on to their computer, along with the potential harm the consumer is exposed to would lend support to a finding of unconscionability.

that installing or using the software is sufficient to establish acceptance of EULA terms even when users are not required to click "I Agree."[231] Whether consumers actually read the EULAs or whether they were designed to encourage reading or comprehension is generally not of interest to courts. When a document is reasonably understood to create legal obligations, courts impose a duty to read.[232] This obligation to read extends not just to EULAs, but to documents hyperlinked from EULAs as well.[233] If users read and understood the terms of software EULAs, many would be surprised by the number of legal obligations they create. As with the bizarre terms in the Sony BMG license that prohibited use of the CDs on office computers and terminated the licensee's rights in the CD if it was stolen or if the user filed for bankruptcy, the restrictions and obligations created in EULAs are often incongruous with consumer expectations about the contents of these documents.[234]

Unless squarely at odds with public policy or deemed unconscionable, EULA terms are generally enforced. Unconscionability requires both procedural defects in the contract formation process and substantive terms

---

231. *See* Tarra Zynda, Note, Ticketmaster Corp. v. Tickets.com, Inc.: *Preserving Minimum Requirements of Contract on the Internet*, 19 BERKELEY TECH. L.J. 495, 504-05 (2004).

232. Heller Fin., Inc. v. Midwhey Powder Co., 883 F.2d 1286, 1292 (7th Cir. 1989).

233. Hubbert v. Dell Corp., 835 N.E.2d 113 (Ill. App. Ct. 2005). *Hubbert* was followed twice in Nadler v. Merlin Int'l, Inc., 2007 U.S. Dist. LEXIS 19651 (S.D. Ill. Mar. 20, 2007) and Provencher v. Dell, Inc., 409 F. Supp. 2d 1196 (C.D. Cal. 2006).

234. Nathan Good et al., *Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements*, *in* 1 ASS'N FOR COMPUTING MACHINERY SPECIAL INTEREST GROUP ON COMPUTER-HUMAN INTERACTION, CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 607 (Bo Begole & Stephen Payne eds., 2007), *available at* http://www.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-CHI-noticing_notice.pdf; Deirdre Mulligan et al., *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, *in* 93 ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES: PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY 43 (2005). The overreaching and unexpected content of Sony BMG's EULA does not set it apart as an outlier. For example, after just a few clicks, a user installing a well-known and popular file-sharing program agrees to provisions that prohibit reverse engineering, disabling advertisements, and removing third party software; force them into mandatory arbitration; permit the sharing of the user's contact information and browsing history; and bind all subsequent users of the software to the EULA.

The iTunes EULA includes: "You also agree that you will not use these products for the development, design, manufacture, or production of missiles, or nuclear, chemical or biological weapons." Apple QuickTime 7.0.4 (free version for Windows) and iTunes EULA (on file with authors).

that unfairly oppress one party to the contract.[235] In the context of the Sony BMG EULA, many courts would not object to the formation process itself, given Sony BMG's use of current industry standard mechanisms like the scroll box and click through assent.[236] Nonetheless, research and experience show this process does not engage users in any meaningful way in the contracting process.[237] And, while the installation of software that can be remotely updated and can enforce Sony BMG's rights with respect to content sounds substantively problematic, it is consistent with the operation of other online content delivery systems for movies and music.[238] So embedding a term requiring users to consent to the installation of a backdoor allowing remote updates and ongoing access to the user's computer in a dense and lengthy EULA is not quite the aberration it seems to be, although we contend that it should be. This is, in fact, the direction in which content protection schemes in the PC environment are moving.[239] Although the security and privacy flaws created by the DRM could provide a basis for a substantive challenge to the EULA, unconscionability requires both substantive and procedural defects.

---

235. *See, e.g.*, Williams v. Walker-Thomas Furniture Co., 350 F.2d 445 (D.C. Cir. 1965).

236. *But see* Ting v. AT&T, 319 F.3d 1126, 1148 (9th Cir. 2002) ("[A] contract of adhesion, i.e., a standardized contract, drafted by the party of superior bargaining strength, that relegates to the subscribing party only the opportunity to adhere to the contract or reject it" is necessarily procedurally unconscionable).

237. Good et al., *supra* note 234.

238. *See* Mulligan et al., *supra* note 213 (discussing monitoring of user activities identified in EULAs and by monitoring program activities).

239. The general movement toward platforms and software that allow for remote attestation about software behavior is found in industry efforts around the creation of a trusted computing platform. This technology is designed to allow one party to verify the "state" and operations of another's machine. In the context of asset management, where a business wants to assure that all the machines remotely connecting to its network are configured in a manner that will protect business interests (personal information, intellectual property, etc.) remote attestation is a promising development. In the context of content owners seeking to monitor the state (what software is running) and activity of a home user's computer in order to protect digital content, the issue of remote attestation is far more problematic and has come, appropriately, under fire. In fact, one legislative effort to deputize this sort of private sector monitoring of private use of content and to privilege self-help by content companies was already vetted and rejected. Hopefully other systems that support remote access to consumers' computers will not introduce security holes, although developing systems that allow for remote access and control of networked PCs that cannot be exploited by a motivated attacker is likely a complicated task. Ross Anderson, 'Trusted Computing' Frequently Asked Questions, http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (last updated Aug. 2003); SCHOEN, *supra* note 158.

Existing law did not dissuade Sony BMG from introducing DRM-protected CDs that created security flaws. While it is almost certain that users had little to no idea that installing the XCP and MediaMax DRM would open security backdoors into their computers or allow remote monitoring of their activities and knowledge of their machine configuration, current EULA and contract law provides little hope for fixing the structure of either the consent process or the substantive terms of such contracts. As discussed *supra*, courts have shown little interest in examining all but the most egregious of contract terms and formation issues.

The need to consider the totality of the consumer contracting experience, rather than specific terms in isolation, suggests that successfully restructuring these interactions will require detailed fact finding about consumers' understandings and expectations, and the harms and risks to consumers and competition created by specific terms and consent procedures. Creating more nuanced and specific rules to govern consent with respect to software downloads is a task better undertaken by an administrative agency with deep expertise in consumer protection and the ability to provide guidance and forward-looking rules than by the courts. In the next Section, we consider the Federal Trade Commission's response to the flawed notice and consent provisions of Sony BMG's DRM and the privacy concerns to which they contributed.

C. Defining Deceptive and Unfair Acts: The Problem with Software Downloads and Privacy

At the time Sony BMG placed its DRM-protected CDs on the market, the FTC had already long demonstrated its authority to investigate and penalize parties making false statements about the collection, use, and disclosure of personal information.[240] In particular, successful enforcement

240. *See* Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf.

> [T]he disclosure shall be unavoidable and shall be presented prior to the consumer installing any content protection software or, if the disclosure is related to Internet connectivity, prior to causing any transmission to respondent about consumers, their computers, or their use of a covered product through Internet servers. The disclosure shall be of a size and shade, and shall appear on the screen for a duration, sufficient for an ordinary consumer to read and comprehend it. The disclosure shall be in understandable language and syntax.

Id. See FTC v. Seismic Entm't, Inc., No. 04-377, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004) (enjoining the unfair practice of exploiting a known vulnerability in the Internet Explorer web browser to download spyware to users' computers without their

actions were brought against companies, like Sony BMG, that offered public statements falsely disavowing the collection of information from users.[241] More recently, the FTC used its authority to bind companies to practices and procedures that provide a "reasonable" level of security for users' personal information.[242] Importantly, it successfully settled claims against companies for failing to implement practices to address commonly known and well-understood security vulnerabilities and for failing to identify and prevent security vulnerabilities that put customer information at risk.[243]

In light of these existing FTC actions, Sony BMG's inaccurate statements about data collection practices and software security, including vulnerabilities that could compromise personally identifiable information, appear inexplicable. However, a more careful consideration of the FTC's prior actions sheds some light on why Sony BMG may not have considered its practices objectionable as a matter of established FTC guidelines.

The centerpiece of the FTC's privacy enforcement actions has been the protection of individually identifiable personal information.[244] But, under

---

knowledge); *In re* Advertising.com, FTC File No. 042 3196 (Sept. 12, 2005). *See also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

241. *See* Microsoft Corp., 67 Fed. Reg. 52,723 (Fed. Trade Comm'n Aug. 13, 2002) (proposed consent order) (alleging that Passport misrepresented its data collection activities and obtaining consent order prohibiting such misrepresentations).

242. *See* MTS Inc., 69 Fed. Reg. 23,205 (Fed. Trade Comm'n Apr. 28, 2004) (proposed consent order) (failure to implement procedures that were reasonable and appropriate to detect and prevent "broken account and session management" vulnerabilities was unfair or deceptive given Tower Records's statements about attention to security and privacy); Eli Lilly & Co., 67 Fed. Reg. 4,963 (Fed. Trade Comm'n Feb. 1, 2002) (proposed consent order) (lack of proper controls to avoid disclosure of e-mail addresses was unfair or deceptive given statements to the contrary).

243. *See* Decision and Order, *In re* MTS, Inc., FTC File No. 032 3209 (May 28, 2004), *available at* http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf; Decision and Order, *In re* Guess?, Inc., FTC File No. 022 3260 (Aug. 5, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf; Decision and Order, *In re* Petco Animal Supplies, Inc., FTC File No. 032 3221 (Mar. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0323221/050308do0323221.pdf; Agreement Containing Consent Order, *In re* BJ's Wholesale Club, Inc., FTC File No. 042 3160 (May 17, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf.

244. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (2000).

> [Personal information means] individually identifiable information about an individual collected online including (a) a first and last name; (b) a home or other physical address including street name and name of a city or town; (c) an email address or other online contact information,

a literal reading of the FTC's application of that term, Sony BMG was not collecting "personal information." According to the FTC, the Sony BMG media player "establish[ed] a connection with Internet servers through which the user's or proxy server's Internet Protocol (IP) address and a numerical key identifying the album being played will be transmitted from the user's computer to the servers."[245] Such information was "used to display images and/or promotional messages on users' computers that are retrieved from those servers."[246] Under its only official statement on the issue, the FTC has said that "unless [IP addresses] are associated with other individually identifiable personal information, they would not fall within the . . . definition of 'personal information'" regulated by the Children's Online Privacy Protection Act.[247] Sony BMG's stance—that it collected no personal information that raised privacy concerns[248]—may seem counterintuitive, but viewed in light of the prevailing FTC definition of "personal information," Sony BMG's position becomes somewhat more coherent. While this in no way excuses the misleading statements found in

---

> including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's email address; (d) a telephone number; (e) a social security number; (f) a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or (g) information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Id.

See also FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (asking for legislation establishing rules, and providing the FTC with regulatory authority, to govern the commercial websites that collect "personal identifying information" from or about consumers).

245. Complaint, *In re* Sony BMG Music Enter., FTC File No. 062 3019, at para. 18 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130cmp0623019.pdf.

246. *Id.*

247. FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2006).

248. Carrie Kirby, *Sony Gets an Earful Over CD Software*, S.F. CHRON., Nov. 11, 2005, at A1; Jack Kapica, *CIPPIC Files Complaint Against SonyBMG Settlement*, GLOBEANDMAIL.COM, Sept. 21, 2006, http://www.theglobeandmail.com/servlet/story/RTGAM.20060921.gtsony0921/TPStory/Technology/columnists; Brian Garrity, *Sony BMG Agrees to DRM Settlement*, BILLBOARD, Jan. 7, 2006, at 5; Iain Thomson, *Sony BMG Settles Rootkit Lawsuit*, VNUNET.COM, Jan. 9, 2006, http://www.vnunet.com/vnunet/news/2148287/sony-settles-root-kit-fiasco.

Sony BMG's EULA, the narrow scope of the FTC's definition of personal information provides important context in which to consider Sony BMG's actions.

At the time Sony BMG put its DRM-protected CDs on the market, the FTC had already brought several actions—some pending and others successfully settled—against companies that had installed software without appropriate notice and consent procedures.[249] The majority of these cases involved "bundled software,"[250] where EULA disclosures were found insufficient to provide notice of the hidden software which typically served pop-up advertisements, collected click-stream data, or engaged in some other invasive data collection technique. Frequently the EULAs accompanying bundled software include multiple embedded or linked EULAs making the identification of the terms of the exchange complicated and time-consuming.

The software on the Sony BMG CDs, however, was not bundled in the traditional sense. Users did not intend to install some software but unknowingly install other software through the Sony BMG CD. Rather, most users likely did not intend to obtain any software at all during this interaction. Although the hidden and unexpected nature of the transactions at the root of the spyware-bundling cases provided a parallel to the Sony BMG CDs, Sony BMG may not have understood itself to be intentionally hiding the software in quite the same way as spyware companies.

---

249. FTC v. Seismic Entm't, Inc., No. 04-377, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004) (holding FTC was likely to succeed on the merits because it is an unfair practice to exploit a known vulnerability in the Internet Explorer web browser to download spyware to users' computers without their knowledge, and enjoining this method of software distribution); Analysis of Proposed Consent Order to Aid Public Comment, *In re* Advertising.com, FTC File No. 042 3196 (Aug. 3, 2005) (holding failure to clearly and conspicuously disclose bundled software that traced browsing deceptive); *see also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (alleging that failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

250. In "bundled" software offerings, the user understands that they are installing one program, but because they fail to read the EULA, and the software attempts to hide itself in other ways, they fail to understand that they are in fact installing several different software programs and often creating relationships with several different companies. Typically these programs engage in invasive activities (pop-up or other forms of push advertising) or extractive activities (monitoring and data collection) that users presumably would avoid if given appropriate notice. *In re* Advertising.com, FTC File No. 042 3196 (Sept. 12, 2005) (holding failure to clearly and conspicuously disclose bundled software that traced browsing deceptive); *see also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (holding that failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

In contrast to the bundled spyware cases, Sony BMG was installing only one piece of software and using a single EULA, which was, in form, consistent with the standard industry practice. The combination of standard disclosure through a EULA and the collection of no "personal information" may have led Sony BMG to conclude that their installation and data collection procedures were consistent with the law and industry norms. This may have been further buttressed by the failure of surveillance law generally to set limits on surreptitious monitoring and data collection in the context of advertising and commercial dealings as long as such monitoring is disclosed in the EULA.[251]

In the Sony BMG consent order, the FTC provided a new twist to the existing privacy landscape. The order stands for the propositions that: (i) clear and prominent notice and consent is required on CDs that condition access to content on the installation of software that monitors and reports on user activities; and (ii) clear and prominent notice and consent is required, again, before information about users, their computers, or their use of the CD's content is transmitted.[252] Through the Sony BMG order and bundled spyware orders, the FTC has established that software that collects and transmits information about users, their computers, or their use of the content—even if not "personal information" under the COPPA definition—raises privacy concerns.[253] The Sony BMG order also creates a requirement, at least with respect to Sony BMG, that the installation of software from a CD, and the transfer of information by such software, re-

---

251. Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1306-11 (2005) (discussing courts' general willingness to allow consent to interception to be given through "click-wrap" EULA provisions and therefore limiting the utility of Wire Tap Act and Computer Fraud and Abuse Act to provide remedies to a large set of spyware problems).

252. Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf

253. Where collection and transmission is part of the standard operation of internet protocols, clearly this cannot be the case. This line, which we are identifying, but is not clearly established in the settlements, may be a hard one to identify and maintain. In the context of traditional web-based interactions, IP addresses are routinely disclosed to the servers from which a user is requesting content (a web page, for example). In this context the requirement that notice and consent occur seems inappropriate. The Sony BMG phone-home feature is the opposite end of the spectrum, in that there is no need for users' machines to interact with Sony BMG's servers. There are many areas in between, and as technology changes, what is necessary and expected will likely change with it.

quires heightened "clear and prominent"[254] notice and consent.[255] Interestingly, the order does not create an obligation to analyze the security properties of products before release. Such obligations are found in earlier FTC orders and the absence here is noteworthy, particularly given that a provision of Sony BMG's settlement with the Attorney Generals requires that at least one qualified, independent third-party expert review future content protection software and conclude that it creates no "confirmed security vulnerabilities" prior to use by Sony BMG.[256]

Like the security vulnerability at issue in prior FTC actions, rootkits and privilege escalation are known, dangerous security vulnerabilities. However several factors make the Sony BMG system distinct, and distinctly troubling. As discussed *supra* in Part II, it seems likely that the choices to design and deploy software with these security vulnerabilities were deliberate and intentional design decisions, not failures of otherwise secure software or loopholes left unaddressed despite a security-conscious design process. Reflecting these distinctions, the FTC complaint against Sony BMG and, to some extent, the final order, included an unfairness claim based on the installation of the security vulnerabilities and the lack of adequate notice and consent during installation in addition to deception claims based on the affirmatively misleading omissions of material facts.

The unfairness claim is the most important element of the order because unfairness does not rely upon the content or sufficiency of statements made to the public, but rather evaluates the substantive impact of

---

254. *See* Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf

> [T]he disclosure shall be unavoidable and shall be presented prior to the consumer installing any content protection software or, if the disclosure is related to Internet connectivity, prior to causing any transmission to respondent about consumers, their computers, or their use of a covered product through Internet servers. The disclosure shall be of a size and shade, and shall appear on the screen for a duration, sufficient for an ordinary consumer to read and comprehend it. The disclosure shall be in understandable language and syntax.

Id.

255. *See id.* (prohibiting downloads unless a consumer "dictates his/her assent to install such software by clicking on a button or link that is clearly labeled or otherwise clearly represented to convey that it will activate the installation, or by taking a substantially similar action").

256. Settlement Agreement at 27, *In re* Sony BMG CD Techs. Litig., No. 1:05-CV-09575 (S.D.N.Y. Dec. 28. 2005), *available at* http://www.eff.org/IP/DRM/Sony-BMG/sony_settlement.pdf.

the businesses activity itself. In this way it is akin to substantive unconscionability in contract law. The FTC found that Sony BMG's installation practices and security vulnerabilities caused substantial injury that users could not reasonably avoid and were not outweighed by any countervailing interests.[257]

The Sony BMG order set two important new baselines. First, the complaint and ensuing order make clear that certain software may not be installed on a user's computer regardless of the consent experience.[258] In particular it prohibits the installation of content protection software that hides, cloaks or misnames files, folders, or directories, or misrepresents the purpose or effect of files, directory folders, formats, or registry entries.[259] This effectively prohibits the installation of content protection software that uses a rootkit like the one contained in XCP. While the order does not explicitly prohibit software that alters system, directory, or file privileges, such as MediaMax, it does require that such software be fairly represented to the consumer both through disclosures during installation and appropriate naming conventions.[260]

Second, where limits are placed on the expected functionality of a CD or information about the consumers' use of the CD is to be transferred, the user must receive clear and prominent notice and must communicate assent affirmatively.[261] This extends to information beyond the personally identifiable information traditionally at the heart of the FTC's privacy initiatives and enforcement actions. The first of these provisions is significant because it begins to establish an obligation to provide heightened notice aimed at truly informing consumers of material changes to functionality of media containing copyrighted works. The second is significant be-

257. *See* Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf.

258. *Id.* at 6.

259. *Id.*

> [Software] shall not install or cause to be installed on a consumer's computer any content protection software that prevents the consumer from readily locating or removing the software, including but not limited to by: (1) hiding or cloaking files, folders, or directories; (2) using random or misleading names for files, folders, or directories; or (3) misrepresenting the purpose or effect of files, directory folders, formats, or registry entries.

Id.

260. *Id.*

261. *Id.*

cause it recognizes a privacy interest in surveillance separate from the focus of prior FTC activity dealing with personally identifiable information.

The FTC and state Attorneys General settlements in the Sony BMG matter are a testament to the power of broad and flexible grants of authority that provide a basis for tailoring responses to new marketplace practices that mislead or injure consumers and materially disrupt settled consumer expectations. But at the same time, the fact that a large, reputable company of Sony BMG's stature was likely unaware that it was acting deceptively or unfairly highlights the problems the FTC and state Attorneys General face in attempting to endorse and enforce marketplace practices that promote meaningful contracting in the online environment. Given the judiciary's unwillingness to set limits or boundaries on the formalities or substance of contracting, this is a particularly daunting task.[262] A case-by-case approach, whether undertaken in agencies or courts, fails to provide clear guidance to companies seeking to engage fairly with consumers and allows ample room for companies to use EULAs to obtain "consent" to overreaching and egregious practices that are inconsistent with consumer expectations or that pose harm. The ongoing struggle within industry to define self-regulatory rules to distinguish legitimate software and business practices from spyware, as well as the ever-growing legislative efforts to address spyware, are a tribute to the yawning grey zone confronting both businesses and consumers and the inadequacy of current contract law to assist in their navigation.

VI. REALIGNING SKEWED INCENTIVES

Having traced the constraints and influences that encouraged and permitted Sony BMG to deploy its DRM strategy, this Part offers potential reforms, both legal and technical, aimed at reshaping the system of incentives that gave rise to the rootkit incident to guard against future harm to the public and the network. First, we build upon the Copyright Office's most recent DMCA rulemaking and suggest a permanent statutory exemption that enables researchers and lay users to proactively identify and remove dangerous protection measures from their systems. Second, we look to insights drawn from the field of HCI-Sec as an additional foundation for the development of more effective notice and consent guidelines and standards governing software downloads and online data collection practices. We argue that the FTC is the best situated institution for incorporating in-

262. Copyright Protection and Management Systems, 17 U.S.C. § 1201(a)(1)(C).

terdisciplinary insights, such as HCI-Sec, in developing such guidelines and standards.

But before outlining these recommendations, two antithetical but equally misguided reactions to the rootkit incident should be addressed. First, a superficial overview of the rootkit incident may suggest—and some will certainly argue—that no response is necessary. Sony BMG, the argument will go, miscalculated the tradeoff between preventing infringement and protecting user security, as a matter of both law and marketing. The investigations, lawsuits, and settlements that came in the wake of XCP and MediaMax simply demonstrate that the corrective mechanisms already in place served their function by holding Sony BMG accountable for its socially harmful behavior. The public flogging Sony BMG received from the press, consumer advocate groups, state Attorneys General, and the FTC will stand as a warning to other content owners and DRM vendors to behave more responsibly in the future.

Although it is undoubtedly true that no record label is likely to introduce protection measures that install rootkits on their customers' computers anytime soon, the ways in which privacy and security can be compromised by DRM are numerous. So long as the system of incentives that produced the rootkit incident remains in place, we can expect further abuses in the future. Although "rootkit" remains a watchword in the world of content protection, institutional memories—much like public awareness—will fade. Rather than relying solely on the content industry's insistence that it has learned its lesson, responsible public policy requires institutional reforms that recognize and counteract the lure of overzealous DRM implementation. Moreover, the anti-interventionist position fails to account for the importance of public interest advocates, the press, and public outcry in pressuring Sony BMG to settle the legal claims brought against it. Such a fortuitous feedback loop cannot be guaranteed in the future, and the protection of end user and network security should not hinge on something as rare and unpredictable as the perfect storm.

Second, standing in stark contrast to this hands-off approach is one that calls for prohibitions on particular technologies in the name of consumer protection. But the rootkit incident should not be understood to make a case for legislation that mandates or prohibits particular technological design decisions. In an extreme form, such legislation could ban the use of rootkits—or even DRM—altogether.[263] This response is mis-

263. Although the FTC's Sony BMG order prohibited Sony BMG from using any content protection software that incorporates a rootkit or similar technology, this is a far

guided for a number of reasons. Both rootkits and DRM can, in some instances, serve useful and legitimate purposes. DRM can enable new business models, such as digital video "rental," that as a matter of economics would prove impossible without some enforcement mechanism for use restrictions.[264] Likewise, legitimate software developers, such as anti-virus vendors, have used rootkits to protect their programs from attack.[265]

While not as pernicious as technological mandates, prohibitions against particular software tools could set dangerous legislative precedent. As a matter of institutional competence, legislators are poorly positioned to insert themselves into the design decisions of technology developers. Congress, in drafting the DMCA, recognized the bounds of its expertise as well as the risks to innovation posed by governmental interference in the minutiae of software and product design.[266] Rather than the immediate constraints on design alternatives that would result from a technological mandate, banning particular software or product components could give rise to a legislative incrementalism that in time will yield the same unfortunate result.

Aside from being dangerous, this tack would also prove ineffective. In all likelihood, rootkits will not prove the next serious threat to end user security and privacy. Legislative or regulatory efforts that narrowly target specific technologies will almost always come a day too late to provide meaningful protection for consumers and network resources.[267] Rather

---

cry from generally applicable legislation that constrains all technology developers and all potential products. *See* Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/ 070130agreement0623019.pdf.

264. Whether the enforcement mechanism requires or deserves the benefit of legislation like the DMCA to introduce the force of law as an additional layer of enforcement is analytically distinct from the technology's importance to new business models.

265. This decision stirred controversy. *See supra* note 2.

266. Copyright Protection and Management Systems, 17 U.S.C. § 1201(c)(3).

> (3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

Id.

267. Stefanie Olsen, *Nearly Undetectable Tracking Device Raises Concern*, CNET NEWS.COM, July 12, 2000, http://news.com.com/2100-1017-243077.html; Posting of Peter Fleisher to The Official Google Blog, http://googleblog.blogspot.com/2007/07/cookies-expiring-sooner-to-improve.html (July 16, 2007 09:52 PST); BRUCE H. KOBAYASHI & LARRY E. RIBSTEIN, A RECIPE FOR COOKIES: STATE REGULATION OF CONSUMER

than seeking to prevent a carbon copy of the most recent disaster, any useful response must attempt to reform the underlying factors that spur content owners to adopt dangerous DRM.

A. Enabling Security Research and Self-Help Through a Statutory Exemption to the DMCA

As described *supra*, the DMCA, by discouraging security research and criminalizing the distribution of software tools that enable users to protect themselves from harmful DRM, served as a key component of the legal landscape that permitted the rootkit debacle.[268] By establishing a permanent statutory exemption from DMCA liability, Congress could take a significant step towards preventing future threats to end user and network security.

In drafting the DMCA, Congress recognized the need to respond to changing circumstances given the fluidity of the nascent environment it sought to prospectively regulate and the otherwise lawful uses that might be adversely affected by the broad prohibition on circumvention. To retain some flexibility, Congress created a rulemaking proceeding that serves as a "fail-safe mechanism" intended to ensure that limits on the prohibition on circumvention keep pace with developments in the market for copyrighted works.[269] This proceeding requires the Librarian of Congress, acting on the recommendation of the Register of Copyrights, to conduct a rulemaking hearing to identify classes of copyrighted works the noninfringing uses of which are likely to be adversely affected by the prohibition on circumvention in the succeeding three year period.[270] Users of copyrighted works that fall within exempt classes are not subject to the prohibition against circumvention.[271]

MARKETING INFORMATION (2001), http://www.law.gmu.edu/faculty/papers/docs/ 01-04.pdf.

268. *See supra* Section V.A.

269. H.R. REP. NO. 105-551, pt. 2, at 35 (1998). As the Report explained, "The primary goal of the rulemaking proceeding is to assess whether the prevalence of these technological protections, with respect to particular categories of copyrighted materials, is diminishing the ability of individuals to use these works in ways that are otherwise lawful." *Id.* at 37.

270. *See* § 1201(a)(1)(C). For a detailed discussion and overview of the DMCA rulemaking process, the exemptions granted in 2006, and the limitations of this process in providing adequate protection to the public, *see generally* Aaron Perzanowski, *Evolving Standards and the Future of the DMCA Anticircumvention Rulemaking*, 10 J. OF INTERNET L., Apr. 2007, at 1.

271. 17 U.S.C. § 1201(a)(1)(B) (2000).

In 2006, the Copyright Office recommended, and the Librarian of Congress granted, an exemption requested by the Samuelson Law, Technology & Public Policy Clinic of the University of California, Berkeley School of Law, on behalf of Felten and Halderman[272] that permits the circumvention of technological protection measures distributed on audio CDs when those measures create or exploit vulnerabilities that compromise the security of personal computers.[273] This exemption, crafted to closely track the facts of the rootkit incident in light of the Copyright Office's traditionally conservative attitude toward the granting of exemption proposals,[274] offers meaningful protection to both lay users and researchers who seek to eliminate security vulnerabilities introduced by DRM on audio CDs. Prior to the exemption, genuine legal uncertainty existed as to whether a user who unknowingly installed XCP could be held liable under the DMCA for its removal or whether a researcher who bypassed the DRM in an effort to discern its operation violated section 1201.[275]

---

272. *See generally* Comment of Edward W. Felten & J. Alex Halderman to the United States Copyright Office, *supra* note 89.

273. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472 (Nov. 27, 2006) (to be codified at 37 C.F.R. § 201.40), *available at* http://www.copyright.gov/fedreg/2006/71fr68472.html; Memorandum from Marybeth Peters, Register of Copyrights, United States Copyright Office, to James H. Billington, Librarian of Congress, concerning Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Nov. 17, 2006), *available at* http://www.copyright.gov/1201/docs/1201_recommendation.pdf.

274. Somewhat surprisingly, the Copyright Office revisited the standards for the DMCA Rulemaking in 2006, potentially opening the door for an increase in narrowly tailored exemptions. *See* Perzanowski, *supra* note 270, at 19-20.

275. In something of an ironic turn, copyright industry representatives sought to defeat the exemption by claiming that: (i) the protection measures used on CDs were copy controls rather than access controls, and thus outside the scope of the anti-circumvention provisions; (ii) existing statutory exemptions, most notably the security testing exemption of section 1201(j), rendered an exemption unnecessary; and (iii) Sony BMG's voluntary release of a tool to uninstall the rootkit obviated the need for an exemption. *See generally* Testimony of Steven Metalitz, http://www.copyright.gov/1201/2006/hearings/transcript-mar31.pdf; Joint Reply Comment, http://www.copyright.gov/1201/2006/reply/11metalitz_AAP.pdf. Rejecting these arguments, the Register concluded that because particular software was required to play a CD on a computer, the technical protection measure used in the DRM at issue was an access control. Memorandum from Marybeth Peters, *supra* note 273, at 56. Because the scope of section 1201(j)—a provision not yet meaningfully interpreted by the courts—was ambiguous, the Register concluded that consideration of the exemption on its merits was appropriate. In light of the need for researchers to identify security vulnerabilities created by CD protection measures, the dangers posed by such measures to consumers, the unclear potential liability under the DMCA, and the

However, the new exemption and the rulemaking procedure itself are insufficient tools to address the security risks posed by technological protection measures. First, the exemption is temporary, with an expiration date of October 2009.[276] Second, the exemption applies only to the extent circumvention occurs for the sole purpose of good faith testing, investigating, or correcting security vulnerabilities, leaving some risk that those who also hope to place music on their iPods after eliminating the security threats could face liability.[277] Third, the exemption is limited to a particular medium—the Compact Disc—and a particular type of work—sound recordings. While these limitations were necessary as a practical matter to secure the endorsement of the Register of Copyrights, they are by no means ideal from a policy perspective. Protection measures that create security vulnerabilities could be introduced in a multitude of media in connection with any type of copyrighted work. As discussed *supra*, a solution tied to the specific facts of yesterday's disaster fails to account for variations on the theme.

But from a practical standpoint, by far the most fundamental inadequacy of the DMCA rulemaking is inherent in the Copyright Office's statutory authority. The rulemaking can exempt certain classes of works from the anti-circumvention provision, but Congress vested no authority in the Copyright Office or Librarian of Congress to grant corresponding exemptions from the anti-trafficking provisions.[278] This asymmetry gives rise to a rather perverse result: an act of circumvention is permitted by an exemption, but the tools necessary to take advantage of that privileged use

---

resulting adverse impact on the ability to engage in noninfringing uses, the Register recommended adoption of the exemption. *Id.*

276. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. at 68,472, *available at* http://www.copyright.gov/fedreg/2006/71fr68472.html. Maintaining the exemption will require proof of ongoing harm during the next rulemaking. Broadening it to cover additional technological protection measures found to present security risks will require separate showings of ongoing harm to a class of works. Given the fallout over the Sony BMG DRM, it is possible that no protection measures that create security risks will be released on CDs in the coming three years, making it impossible to renew the exemption. While this will mean that no security-flaw-riddled DRM is on the marketplace, it will also remove an important incentive for copyright holders to ensure the safety of their protection measures going forward. *See* Perzanowski, *supra* note 270.

277. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. at 68,472, *available at* http://www.copyright.gov/fedreg/2006/71fr68472.html.

278. Copyright Protection and Management Systems, 17 U.S.C. § 1201(a)(1)(C).

remain illegal.[279] Thus although both the public and security researchers may engage in circumvention under the new exemption, researchers like Felten and Halderman could still face potential liability for distributing tools to assist the public in exercising this exemption. Given that the average CD purchaser will possess neither the knowledge nor ability to eliminate the security risks of a protection measure without a software tool, the inability of the exemption process to free experts to develop tools renders this new right much less meaningful.

The solution to the shortcomings of the DMCA rulemaking must be a legislative one.[280] But rather than simply extend the authority of the Copyright Office to include the power to exempt classes of works from the DMCA's anti-trafficking provisions as well—a development the authors would welcome—Congress should simply expand the existing permanent statutory exemption found in section 1201(j) to permit both circumvention and trafficking to the extent undertaken to investigate or eliminate protection measures that "create or exploit security flaws or vulnerabilities that compromise the security of personal computers."[281]

B. Developing Meaningful Notice and Consent Mechanisms through Interdisciplinary Insight and Agency Action

As discussed *supra*, the security vulnerabilities in the DRM Sony BMG deployed are best viewed as intentional design choices. While Sony BMG is responsible for deploying dangerous software, the ease with which the software could be surreptitiously installed on consumers' ma-

279. The "reverse notice and takedown" process put forward by Reichman, Dinwoodie, and Samuelson in this volume proposes to address the limited technical ability of the general public by requiring copyright owners to take down technical protections to make tools for "public good" uses. Jerome H. Reichman, Graeme B. Dinwoodie, & Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981 (2007). This innovative approach would instill some needed balance back into the DMCA; however, it will not create room for research on protection measures themselves, nor create a safe harbor for those who create tools to enable users to make public good uses. *Id.*

280. Representatives Rick Boucher and John Doolittle's Freedom And Innovation Revitalizing U.S. Entrepreneurship Act would enshrine the current temporary exemptions and add additional valuable permanent exemptions; it does not, however, address the unnecessarily narrow scope of the "rootkit" exemption. H.R. 1201, 110th Cong. (2007). The authors humbly suggest that the bill would benefit from incorporation of the recommendations contained in this section.

281. Currently section 1201(j) applies only to (a)(1) and (a)(2). 17 U.S.C. § 1201(j) (2000). In light of the tortured distinction between copy controls and access controls, its scope should be expanded to include section 1201(b) as well.

chines causes us to reflect on the state of consumer control over the activities—software downloads and data collection and transmission—occurring on their desktops more generally. Consumer protection law has an important role to play in reforming the notice and consent process with respect to software installation and data collection practices.

But we believe that innovative reforms in this area will come about from a broader interdisciplinary approach. The FTC decisions discussed *supra*, in Section V.C, begin to chart a course in this direction. Incorporating insight from the field of HCI-Sec would enable the FTC and other consumer protection agencies to craft guidelines for language and mechanisms to facilitate effective notice and informed consent. Such guidelines would vest consumers with increased control of the software downloaded onto their machines and the information collected and transmitted about their activities.

A growing team of HCI-Sec researchers is exploring "usable privacy and security."[282] The Sony BMG disaster is one in a string of examples of the difficulties facing computer users in making good security and privacy choices about their computing environment.[283] It is imperative that users understand, value, and implement security. The question under exploration

---

282. See HCISec Bibliography, http://www.gaudior.net/alma/biblio.html, for an up-to-date list of contributions in this field. With respect to privacy, HCISec practitioners have studied a variety of fields. For research on browsers, see, for example, Batya Friedman, Daniel C. Howe, & Edward Felten, *Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design*, *in* PROCEEDINGS OF THE THIRTY-FIFTH ANNUAL HAWAI'I INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES; Umesh Shankar & Chris Karlof, *Doppelganger: Better Browser Privacy Without the Bother*, *in* THIRTEENTH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (2006); for peer-to-peer file-sharing research, see, for example, Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of Kazaa P2P File-Sharing*, *in* PROCEEDINGS OF THE ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI 2003); for notices and spyware acquisition, see, for example, Mulligan et al., *supra* note 234; for operating system research, see, for example, Alex J. DeWitt & Jasna Kuljis, *Aligning Usability And Security—A Usability Study Of Polaris*, *in* PROCEEDINGS OF THE 2006 SYMPOSIUM ON USABLE PRIVACY AND SECURITY 12-14 (2006); and for phishing, see, for example, Rachna Dhamija & J.D. Tygar, *The Battle Against Phishing: Dynamic Security Skins*, SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2005); Rachna Dhamija, J.D. Tygar, & Marti Hearst, *Why Phishing Works*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2006).

283. *See* A. Herzog et al., *User Help Techniques for Usable Security*, PROCEEDINGS OF THE 2007 SYMPOSIUM ON COMPUTER HUMAN INTERACTION FOR THE MANAGEMENT OF INFORMATION TECHNOLOGY, Article No. 11 (2007) (discussing research revealing that inadequate usability results in security failures in many contexts including firewalls, Internet Explorer, Word, Outlook Express, encrypting email clients, and login systems).

in the HCI-Sec community, and directly relevant to the consumer protection mandate of the FTC and related agencies, is how to make privacy and security compelling, usable, and routine to end-users.

One problem with current user interface design is that users do not play a central role in controlling their security and privacy choices. Anti-virus and anti-spyware vendors have stepped in to assist users in maintaining a safe computing environment, but reliance on third-party vendors for defense is insufficient due to the contextual, process-based nature of both privacy and security.[284] For example, the same program functionality can have radically different consequences depending upon the context—compare a parent's installation of a program to create a safe online experience for a child to a similar program installed by a third party on the machine of an unconsenting adult. Given that users' opinions about the desirability of particular functionalities may be dramatically altered by the context of its intended use, effective privacy and security management must allow users to play a central role in controlling their privacy and security profiles. Because of this contextual variation of the value of privacy and security tools, techniques that fail to account for user autonomy are unworkable, even if the current state of desktop security and privacy tools is beyond the grasp of the average user.[285]

The failure of consumers to appropriately respond to disclosures of the privacy and security features of their products poses another problem. Research in HCI-Sec and related fields finds that information about a product's functionality, even when fully and accurately disclosed, often fails to capture the attention of computer users or to aid them in acting in a man-

---

284. By "contextual", we mean that decisions about information flow and access, integral to utilizing both privacy and security, tend to be context-dependent rather than absolute, i.e., individuals' concerns may vary widely depending upon the nature of perceived risks, which is related to the information or activity to be protected and the parties involved. For an exploration of the contextual nature of privacy, see Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004). By "process-based", we mean that providing security and privacy requires an ongoing evaluation of emerging threats, changing resources of adversaries, and changes in technology. One cannot adopt a policy to protect either at a given point in time and consider protection complete.

285. The remainder of this section primarily explores mechanisms for engaging users in effective decision-making. Another common approach to security is to build it in and automate it to the extent possible. These techniques are not mutually exclusive, but reflect differences in orientation to system design, the first being user-centric, the second being security- and system-centric. *See* Ka-Ping Yee, *User Interaction Design for Secure Systems*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATIONS SECURITY (LECTURE NOTES IN COMPUTER SCIENCE 2513), 278-290 (2002); Herzog et al., *supra* note 283.

ner consistent with their stated interests.[286] If the legal framework is to actually aid consumers in marketplace transactions, a primary goal of consumer protection agencies should be making security and privacy "usable."

A number of barriers hinder efforts to engage users in privacy and security decision-making.[287] First, security is typically a secondary concern undertaken in support of some other objective.[288] Second, there is little time or tolerance for trial and error in security decision-making, as decisions must be correct the first time.[289] Third, experimental research demonstrates that users' stated privacy preferences do not always align with their behavior[290] and that during task completion users will put off privacy or security protective behaviors.[291] Fourth, cognitive biases lead individuals to discount future privacy or security losses if presented with an immediate benefit,[292] reinforcing all of the above. These barriers combine with more generic problems, identified in the context of notice design generally,[293] to create a very difficult problem and design space.

Building upon the usability metrics of effectiveness, efficiency, and satisfaction,[294] HCI-Sec researchers have developed guidelines for align-

---

286. Good et al., *supra* note 234; Mulligan et al., *supra* note 234 (concluding in part that users' failure to delve into documentation describing software functionality stems from the incomprehensible nature of the EULAs that typically house these disclosures).

287. Much of the discussion below draws on work on either security or privacy, and in a few instances both. For the points we are highlighting, we believe that the research on privacy and security can be generalized across the two topics.

288. Herzog et al., *supra* note 283; J. Hardee et al., *To Download or not to Download: An Examination of Computer Security Decision Making*, INTERACTIONS (May & June 2006), at 32.

289. Herzog et al., *supra* note 283.

290. Hardee et al., *supra* note 288.

291. *Id.*

292. Acquisti & Grossklags, *supra* note 103.

293. HCI researchers are studying the effects of notification systems in computing generally, in particular focusing on cognitive response to interruptions. Notification systems often use visualization or auditory techniques to simply convey information with minimal distraction from primary tasks. A broad range of research has examined the creation of effective notice systems that limit the chances of warnings being dismissed or ignored. *See* E. Cutrell, M. Czerwinski, & E. Horvitz, *Notification, Disruption and Memory: Effects of Messaging Interruptions on Memory and Performance, in* HUMAN-COMPUTER INTERACTION: INTERACT '01 263 (Michitaka Hirose ed. 2001), *available at* http://research.microsoft.com/~cutrell/interact2001messaging.pdf.

294. ISO standard 9241-11 defines usability as the "[e]xtent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." "Effectiveness is defined as the accuracy and

ing security and usability,[295] as well as an approach that recognizes the importance of user autonomy in framing security considerations.[296] Using the guidelines and methodologies of HCI-Sec to analyze the design of

---

completeness with which users achieve specified goals." "Efficiency is measured by relating the level of effectiveness achieved to the resources used." "Satisfaction (defined as freedom from discomfort and positive attitudes to the use of the product) is a response of users to interaction with the product." *See* Halderman & Felten, *supra* note 11.

295. Yee, *supra* note 285.

> *Path of Least Resistance.* The most natural way to do any task should also be the most secure way.
>
> *Appropriate Boundaries.* The interface should expose, and the system should enforce, distinctions between objects and between actions along boundaries that matter to the user.
>
> *Explicit Authorization.* A user's authorities must only be provided to other actors as a result of an explicit user action that is understood to imply granting.
>
> *Visibility.* The interface should allow the user to easily review any active actors and authority relationships that would affect security-relevant decisions.
>
> *Revocability.* The interface should allow the user to easily revoke authorities that the user has granted, wherever revocation is possible.
>
> *Expected Ability.* The interface must not give the user the impression that it is possible to do something that cannot actually be done.
>
> *Trusted Path.* The interface must provide an unspoofable and faithful communication channel between the user and any entity trusted to manipulate authorities on the user's behalf.
>
> *Identifiability.* The interface should enforce that distinct objects and distinct actions have unspoofably identifiable and distinguishable representations.
>
> *Expressiveness.* The interface should provide enough expressive power (a) to describe a safe security policy without undue difficulty; and (b) to allow users to express security policies in terms that fit their goals.
>
> *Clarity.* The effect of any security-relevant action must be clearly apparent to the user before the action is taken.

Id. Saltzer and Schroeder also suggest:

> [*Least privilege.*] Every program and every user of the system should operate using the least set of privileges necessary to complete the job.

J. H. Saltzer & M. D. Schroeder, *The Protection of Information in Computer Systems*, *in* 63-9 PROCEEDINGS OF THE IEEE, 1278, *available at* http://web.mit.edu/Saltzer/www/publications/protection/.

See also D. Balfanz, D.K. Smetters, & R. Grinter, *In Search of Usable Security: Five Lessons from the Field*, IEEE SECURITY & PRIVACY (Sept.-Oct. 2004), at 19; I. Flechais, A.M. Sasse, & S.M.V. Hailes, *Bringing Security Home: A Process For Developing Secure and Usable Systems*, *in* WORKSHOP ON NEW SECURITY PARADIGMS 49 (2003).

296. Yee, *supra* note 285.

AutoRun identifies core ways in which its design facilitated, or at least failed to prevent, Sony BMG's behavior.

The process of software installation under the default configurations of AutoRun violated several HCI-Sec usable security principles.[297] First, the principle of *explicit authorization* requires that delegations of authority require explicit user action that is actually understood by the user as an act of delegation. The decision of what software is on a machine is generally a decision for users.[298] By allowing others to install software without providing users with notice and the ability to affirmatively delegate or withhold the privilege of doing so, AutoRun ran afoul of this design principle. The failure of AutoRun to expose the action of downloading to the user in a meaningful manner ran afoul of the *visibility* principle as well. *Visibility* requires the interface to represent, in an easily understandable manner, all active actors and authority relationships (who can take what action amongst actors or on resources) that would affect security-relevant decisions.[299] The pop-up security notices produced by AutoRun did not achieve the level of *expressiveness* sufficient to describe a safe security policy and allow users to choose among security options.[300] In addition, the effect of installing the DRM software on the security of the users' system was not apparent to the users either before, during, or after installation. This violates the *clarity* principle.[301] Finally, the rootkit violated the principle of *revocability* by making it exceedingly difficult for the user to revoke her delegation.[302]

The HCI-Sec principles of explicit authorization, visibility, expressiveness, clarity, and revocability are reflected to some extent in the FTC Sony BMG order which directs more forthright communication with users and greater affirmative control over the installation of software and the collection and transmission of data. Through enforcement actions against spyware distributors, the Federal Trade Commission and state Attorneys

297. For the purpose of this analysis we use the principles set forth in Yee, *supra* note 285. They are more inclusive and detailed that those found in other discussions of this subject. For several case studies on usability and security and additional insight into integrating them into the design process, *see* HCISec Bibliography, *supra* note 282.

298. Yee, *supra* note 285. In the context of an employer-employee relationship, the employer often makes decisions about computer configuration and software.

299. *See id.*

300. *Id. See also* Herzog et al., *supra* note 283 (critiquing "security by pop-up windows" based on research that shows it leads users to click through to return to the first order task).

301. *Id.*

302. *Id.*

General have begun to establish what are likely to become de facto policies limiting the reliance on EULAs as a means of adequate disclosure with respect to spyware programs, and perhaps other downloadable software. The consent orders and judgments establish a new form of consent, "express consent," which must be obtained prior to the installation, separate and apart from the EULA.

The efforts of HCI-Sec researchers are buttressed by efforts in the private sector to establish best practices for the notice and consent experience mechanism in response to the growing problems with spyware.[303] The Antispyware Coalition, a group of anti-spyware software companies, academics, and consumer groups building consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies, similarly concluded that "EULAs alone are usually not enough to offset risk behaviors." Just as "express consent" as defined by the FTC and state Attorneys General requires "clear and prominent" disclosures, the Coalition's best practices require "clear and prominent" disclosures to be unavoidable and accessible (language, presentation, size) to "an ordinary consumer." They also establish heightened demands for communicating assent, requiring that software installations are clearly indicated on the button or other user interface that activates them.[304] In addition, these agreements begin to constrain the bundling of spyware and adware software with "free" programs to deceive consumers, and set procedural and substantive rules about uninstall procedures.[305]

---

303. ANTI-SPYWARE COALITION, *supra* note 185 ("For potentially unwanted technologies, EULAs alone are usually not enough to offset risk behaviors. Individual consent of risky behaviors may be appropriate."). The document addresses issues around remote control software, privacy, and other issues arising in the context of the Sony BMG DRM-protected CDs.

304. *Id.*

305. *Id.*

> Potentially unwanted software should ask for user consent before software technology is installed or uninstalled, or if any personal information about users will be collected during software technology installation or when the software application is running. After providing a prominent notice about what is about to occur, users should be presented with a clear, easy-to-understand choice. For the consent to be meaningful, the purposes for which the information is being collected and will be used should be stated in a matter reasonably understandable to the user. Nothing should happen unless users provide a clear, affirmative 'Yes' to whatever is proposed. If users choose not to agree, there should be no disruption or interference with the computing experience. There should not, as a condition to the supply of a product or

If we assume that courts will continue to treat EULAs and other notices as a proxy for a "meeting of the minds" sufficient to bind consumers to license terms, then HCI-Sec methods of improving feedback and control are useful tools to aid policy makers and the private sector in the creation of better notices and consent experiences. We believe the HCI-Sec principles should be a component of FTC action to develop security and privacy best practices and rules for software downloads based on the more stringent notice and consent procedures found in the Sony BMG and spyware decisions and orders.

The FTC is the natural place to build upon the work begun in the private sector, and to pull in additional expertise from disciplines including HCI-Sec, behavioral economics, and computer and information security to create best practices and potentially new rules to guide the interactions between consumers and businesses in the online environment. The FTC is far better suited to engage in the policy analysis and balancing required by this activity than the courts or even Congress. The need for flexible standards as opposed to hard and fast rules lends itself to the ongoing oversight of an agency, like the FTC, that can continue to revisit and alter standards as the market evolves.

Finally, improving the extent to which individuals understand that they are compromising security will not necessarily reduce the likelihood of such compromises if users acting in their own self interest nonetheless make poor security choices in a networked environment. Given the externalities posed by users' decisions to impair the security of their own machines—even those made knowingly, based on full and accurate information—the FTC must determine those terms to which users may not consent due to public policy concerns about the overall security of the information infrastructure.

VII. CONCLUSION

This Article set out to explain the market, technological, and legal factors that led Sony BMG toward a DRM strategy that, in retrospect, appears obviously and fundamentally misguided. Examining Sony BMG's long and unfortunate series of missteps offers important insights into necessary reforms of market practices, policy interventions, and the technology it-

---

> service, be a requirement for a user to consent to the collection, use, or disclosure of information beyond what is required to provide the services or applications in question without clear choices for the user."

Id.

self. The confluence of factors that encouraged, enabled, and failed to prevent Sony BMG's actions are complicated and interdependent. Unsurprisingly, we conclude that preventing similar future incidents requires approaches that incorporate technology and law and respond to the relevant market conditions.

Until average users are better equipped with intuitive tools and concise, compelling information describing relevant risks and benefits, they will be unable to manage the security of their machines. And unless users can take control of their security, we will be forced to choose between an increasingly insecure networked environment and one with diminished adherence to the end-to-end principle[306] as security management migrates from the desktop towards the center of the network.

Genuine end user control over security decisions relies on a level of transparency regarding the functionality and risks posed by software that can be assured only through independent public-minded security research. Such research can proceed at the necessary pace only once the threat of DMCA liability is lifted.

But the availability of information exposing these threats alone is insufficient. Both technology and law have a role to play in shaping usable security and privacy solutions. Technology can help to inform users and enforce their preferences to the extent those preferences can be accurately expressed and their violation detected. Users need the law to force the honest disclosure of terms and risks, and to protect them against overreaching license terms. And, in some rare circumstances, the law must prohibit certain risks that we cannot afford for users to accept in highly networked environments, regardless of their willingness.

If DRM is to emerge as a tool that benefits consumers through the introduction of new business models and innovative pricing structures, the terms of these transactions must be clearly and meaningfully presented to consumers. Unless consumers understand the rights granted and costs imposed by these transactions—among them sacrificed privacy and security—DRM will remain a tool that exclusively benefits copyright holders, while presenting consumers with, at best, inconvenience and, at worst, violations of their security, privacy, and expectations.

---

306. The end-to-end principle holds that complexity should be concentrated at the edges of a network rather than at its center. This principle gives rise to complex end points and relatively simple networks connecting them. *See generally* J.H. Saltzer, D.P. Reed & D.D. Clark, *End-to-end Arguments in System Design*, http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf (1981).