Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts

June M. Besek*

TABLE OF CONTENTS

Executive Summary .................................................................................................................. 389
I. Introduction ......................................................................................................................... 391
   A. Background ..................................................................................................................... 391
   B. Concerns About Anti-Circumvention Legislation ....................................................... 393
   C. The Kernochan Center’s Study ..................................................................................... 394
II. U.S. Law ............................................................................................................................ 395
   A. Summary of Legislation ............................................................................................... 396
      1. Prohibition Against Circumventing a Technological Protection Measure ............ 396
      2. Prohibition Against Trafficking in Circumvention Devices and Services .......... 396
         a. No Trafficking in Devices that Circumvent Access Controls ............................ 396
         b. No Trafficking in Devices that Circumvent Rights Controls ............................ 397
      3. Exemptions ................................................................................................................. 397
      4. Responsibility of Equipment Manufacturers .......................................................... 398
      5. Obligations of Rightholders ..................................................................................... 398
      6. Ongoing Monitoring .................................................................................................. 399
         a. Section 1201(a) Rulemaking .................................................................................. 399
         b. Study Concerning Encryption Research and Technology ................................. 399
         c. Study Under Section 104 of the DMCA ................................................................. 399
   B. History of U.S. Anti-Circumvention Provisions ............................................................. 400
      1. Action Prior to 105th Congress .................................................................................. 400
      2. Action in the 105th Congress ..................................................................................... 402
      3. Route to Final Passage .............................................................................................. 406
   C. Section 1201 in the Courts ........................................................................................... 407
      1. Statutory Issues ........................................................................................................... 407
         a. What Technological Measures Are Protected? ..................................................... 407
         b. What Does it Mean to “Circumvent” a Technological Measure? ....................... 410

* Executive Director, Kernochan Center for Law, Media and the Arts, Columbia Law School. Special thanks to Jane C. Ginsburg, Morton L. Janklow Professor of Literary and Artistic Property Law, Columbia Law School, who acted as a consultant on this project and provided invaluable suggestions throughout. Research assistance from the following Columbia Law School graduates is gratefully acknowledged: Julie Anderson, Trace Cooper, Deborah Fine, Geoffrey Gordon, Christopher Hapka, Jeffrey Korn, Tucker McCrady, Jennifer Norman, Michael Rizzo, Brian Verminks, Bradley Weyland, Brian Wildstein and George Williamson III.
c. What Is a "Work Protected Under This Title?" .................................................. 411
d. Statutory Exemptions ............................................................................. 411
2. Constitutional Challenges ......................................................................... 412
   a. Distribution of Circumvention Devices .............................................. 412
   b. Fair Use ......................................................................................... 415
D. Copyright Office Proceedings ................................................................. 416
   1. Section 1201(a) Rulemaking ............................................................... 416
      a. Congressional Guidance on the Rulemaking Procedure ............... 417
      b. Initial Rulemaking Proceeding ....................................................... 418
      c. Second Rulemaking Proceeding ...................................................... 420
   2. Study Concerning Encryption Research and Technology ............... 423
   3. Study Under Section 104 of the DMCA ............................................. 423
E. Proposed Legislation and Regulations .................................................. 424
III. Legislation in Other Countries ............................................................. 426
A. European Union ...................................................................................... 426
   1. Prohibition Against Circumventing a Technological Protection
      Measure ............................................................................................ 426
   2. Prohibition Against Trafficking in Circumvention Devices and
      Services .............................................................................................. 426
   3. Exemptions ....................................................................................... 427
   4. Responsibility of Equipment Manufacturers ...................................... 428
   5. Obligations of Rightholders ............................................................... 428
   6. Ongoing Monitoring ......................................................................... 428
B. Australia .................................................................................................. 429
   1. Prohibition Against Circumventing a Technological Protection
      Measure ............................................................................................ 429
   2. Prohibition Against Trafficking in Circumvention Devices and
      Services .............................................................................................. 429
   3. Exemptions ....................................................................................... 430
   4. Responsibility of Equipment Manufacturers ...................................... 431
   5. Obligations of Rightholders ............................................................... 431
   6. Ongoing Monitoring ......................................................................... 431
C. Japan ....................................................................................................... 431
   1. Prohibition Against Circumventing a Technological Protection
      Measure ............................................................................................ 431
   2. Prohibition Against Trafficking in Circumvention Devices and
      Services .............................................................................................. 435
   3. Exemptions ....................................................................................... 435
   4. Responsibility of Equipment Manufacturers ...................................... 436
   5. Obligations of Rightholders ............................................................... 436
   6. Ongoing Monitoring ......................................................................... 436
IV. Legal Provisions that Prohibit Circumvention of Protective Measures in
Other Contexts .......................................................................................... 436
A. Introduction ............................................................................................. 436
B. Analogous Provisions ............................................................................ 437
   1. Provisions Cited as Analogous to the DMCA in Official Reports .... 437
      a. Audio Home Recording Act, 17 U.S.C. § 1002(a) & (c). .............. 437
b. “Cable Communications Policy Act,” 47 U.S.C. § 553(a), Addressing Cable Descramblers........................................ 437

2. Additional Provisions that Address Circumvention-Type Situations..... 439
c. The Stored Wire and Electronic Communications Act, 18 U.S.C. § 2701 ................................................................. 440
d. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ............. 440
e. Additional Federal “Access” Statutes .................................. 441

3. Analogous State Laws ....................................................... 441
   a. State Laws Prohibiting Theft of Communication Services ...... 441
   b. State Computer Trespass Laws ....................................... 442
c. State Provisions Concerning Burglars’s Tools, Lock Picks, Hot Wires ................................................................. 442
d. State Provisions Against Deactivating Inventory Control Devices ... 443

C. Analysis of Measures .................................................... 443
   1. Action Versus Device Prohibitions ................................ 443
   2. Circumvention Defined and Compared .............................. 444
      a. Circumvention ...................................................... 444
      b. Descrambling/Decryption ....................................... 444
c. Deactivation/Removal/Destruction .................................. 445
d. Breaking and Entering ................................................ 445
e. Unauthorized Access ............................................... 445
   f. Interception/Reception ............................................ 445

D. Summary ..................................................................... 446

V. Technological Protection Measures and Digital Rights Management Technologies ........................................ 446
   A. Common Technological Protection Devices ....................... 447
      1. Watermarks ...................................................... 447
      2. Encryption ..................................................... 448
   B. Functions of Technological Protection Measures .................. 449
      1. Access Controls ................................................... 450
      2. Use Controls .................................................... 450
      3. Protection for the Integrity and Authenticity of Information 450
      4. Tracking ......................................................... 451
   C. Digital Rights Management Systems ................................. 451
   D. Measures Employed ................................................. 453
      1. Music Industry ................................................... 453
         a. SCMS ......................................................... 453
         b. SDMI ......................................................... 453
c. Copy-Protected CDs .................................................. 454
2. Motion Picture Industry ................................................................. 457
   a. Macrovision ............................................................. 457
   b. CSS ................................................................. 457
   c. DTCP ................................................................. 458
   d. Protection for Internet Distribution ........................................ 459
3. Book Publishing .................................................................. 459
E. TPMs and Technology Companies ................................................ 460
VI. Discussion ........................................................................ 466
A. Criticisms of the DMCA ......................................................... 467
   1. The DMCA Will Promote Digital Lockup and Lead to a “Pay-Per-
      Use” Society ................................................................. 467
   2. The DMCA Inhibits Fair Use and Other Copyright Privileges ...... 467
   3. The DMCA Inhibits Free Speech and Violates the First Amendment ... 467
   4. The DMCA Will Limit Access to Public Domain Works .......... 468
   5. The DMCA’s Anti-Trafficking Provisions Eliminate the Practical
      Ability to Enjoy Copyright Privileges ...................................... 468
   6. The DMCA Lets Copyright Owners Defeat Privileges Under the
      First Sale Doctrine by Supporting Access Restrictions that “Tether”
      Works to Particular Playback Devices .................................... 468
   7. The DMCA Prevents Legitimate Research Activities Involving
      Reverse Engineering and Investigation of Improved Encryption
      Methods ........................................................................ 469
   8. The DMCA Restricts Competition in the Replacement Parts
      Market ........................................................................ 469
   9. The Anti-Circumvention Approach of the DMCA Is Futile .......... 469
B. Factors Underlying the Debate About § 1201 .................................. 469
   1. The Access Right in § 1201 ................................................ 469
   2. Section 1201 Is a “Lightning Rod” ....................................... 469
   3. Polarization .................................................................... 470
   4. Exaggerated Perceptions of User Privileges .............................. 471
      a. Fair Use ..................................................................... 471
      b. The First Sale Doctrine ................................................ 473
   5. The Meaning of “Access” .................................................. 474
   6. Other Benefits of Technological Controls ............................... 475
C. Alternatives to Section 1201 ...................................................... 475
   1. Exempt Circumvention for Any “Legitimate Purpose” or
      “Non-infringing Use” .......................................................... 476
      a. Background .................................................................. 476
      b. Fair Use and Access Controls ------------------------------- 478
      c. The Effect of § 1201 on Fair Use .................................. 480
      d. Accommodating Fair Use .............................................. 481
      e. Constitutional Concerns ................................................. 484
   2. Audio Home Recording Act Model/Levies .................................. 485
   3. Regulated Circumvention Devices .......................................... 489
   4. “Fair Use by Design”/“Fair Use by Mandate” ............................ 491
EXECUTIVE SUMMARY

Digital media offer vastly increased opportunities to reach audiences of readers, listeners and viewers of works of authorship. But the ease with which digital works can be copied and widely disseminated also creates significant challenges for authors and copyright owners. In the long run, society as a whole stands to lose, should widespread unauthorized activities undermine the incentives to create or invest in the development of works of authorship. Technological mechanisms such as encryption, password protection and copy controls provide some protection against unauthorized use, but most of those mechanisms can easily be circumvented. Many countries have enacted laws to protect authors and copyright owners against the circumvention or bypassing of the technological controls they use to protect their works.

The United States, in 17 U.S.C. § 1201, prohibits circumvention of technological access controls that protect a copyrighted work. That law also prohibits trafficking in devices to circumvent technological controls that protect access to a copyrighted work or that protect works from being copied, redistributed or otherwise further communicated to the public. The European Union has enacted a Directive similar in many respects to U.S. law. Other countries have taken different approaches.

Anti-circumvention laws are designed to encourage authors and copyright owners to explore new business models and methods of distribution, and to provide consumers with a range of choices for experiencing copyrighted works, at different price and convenience levels. Section 1201 has fostered a variety of new distribution models, including DVDs, motion picture downloads, iTunes and various other online music services, and e-books.

On the other hand, anti-circumvention legislation has been criticized as
promoting digital lockup and ultimately, a “pay-per-use” society. Critics also claim that such laws “eliminate” fair use and other user privileges, inhibit free speech, hinder scientific research and restrict competition.

This study, undertaken by the Kernochan Center for Law, Media and the Arts at Columbia Law School, sought to review and evaluate the ways in which the United States and other countries protect technological controls against circumvention, the extent to which access to or use of copyrighted works is promoted or restricted by such controls and whether major changes to U.S. law are warranted. Our study found, among other things, that several factors have tended to skew public debate about the issues. They include the often highly polarized nature of the discussions, an exaggerated perception of the scope of user privileges, and fundamental differences over what it means to have “access” to a copyrighted work.

In light of the concerns expressed about anti-circumvention protections, we identified several potential alternatives to the regime set out in § 1201. They include, for example, (1) creating a broad new exemption to permit circumvention for any “legitimate purpose” or “non-infringing use”; (2) substituting the Audio Home Recording Act model, in which a particular form of technological protection would be mandatory, users would be granted statutory use privileges and authors would be compensated by means of a levy on copying mechanisms and media; (3) regulating the distribution of circumvention devices; (4) requiring copyright owners to make privileged uses available, possibly by making accommodations in the design of the technological controls; or (5) expanding the possible role of a “circumvention service provider” who could facilitate circumvention under defined conditions.

However, our study also found that pursuing these alternatives may be premature, because technological protections are not yet as pervasive or as intrusive as critics have feared. A host of legal, technological and market factors work together to counter digital lockup and provide a safety valve to accommodate legitimate uses. For example, many works are and will continue to remain available; and many privileged uses do not require digital, or even mechanical copying. In addition, user preferences influence protection mechanisms, and marketing models often permit and even encourage some copying and distribution of copyrighted works. The means of making privileged uses remain largely available, though in some circumstances, copying may not be as convenient as some users might wish. Finally, the current law already includes a “safety valve”—in addition to several exemptions set out in the law, the Copyright Office can create new exemptions through its rulemaking proceeding.

Nonetheless, some potential problems in the application of § 1201 have emerged, and others will undoubtedly emerge in the future. In some cases, the problems will likely be resolved satisfactorily by the courts or by the market. In others, statutory amendment may be warranted, but such amendments should be tailored to address the specific problems identified. Potential areas of concern include:

- Access to public domain works
- Archiving and preservation
Defects and malfunctions
- Combined access and rights controls
- The replacement parts market
- Reverse engineering and encryption research
- Enabling fair use without circulation of circumvention devices.

While existing evidence does not support new statutory exemptions at this time, these are areas that require closer scrutiny, and all of them should be carefully monitored to ensure that the means of making privileged uses are not foreclosed.

Section 1201 involves genuine tradeoffs: Congress, recognizing that technological controls might diminish the convenience of making privileged uses, nonetheless made a judgment that technological protection would foster innovation in new content delivery mechanisms and provide consumers with a range of new options for experiencing copyrighted works. The balance that Congress struck appears justified, based on the track record so far. Section 1201 appears to be performing largely as Congress had envisioned and should not be overhauled or replaced at this time. The benefits—development of new business models for delivering sound recordings, motion pictures, books and other copyrighted works to consumers at a variety of price and convenience points—are real, and so far privileged uses of copyrighted works have neither been foreclosed nor significantly compromised. It is important to continue to monitor § 1201’s effects and, where problems become apparent, to develop specific, focused solutions. Our study concludes that at the present time, however, we should allow the new types of digital deliveries that are promoted by § 1201 the opportunity to continue to flourish.

I. INTRODUCTION

A. BACKGROUND

Digital technology and the internet have made it possible to reproduce copyrighted works and disseminate them around the world with ever greater speed and efficiency. For example, the widely available MP3 format, faster communications channels and peer-to-peer file-sharing programs enable users to compress, upload and distribute sound recordings over the internet very quickly; as a result, millions of unauthorized copies of sound recordings are made each day. This is increasingly true of motion pictures as well, as compression techniques become more sophisticated and bandwidth increases. Nor is this phenomenon limited to sound recordings and motion pictures: novels, videogames, television programs, photographs and many other works are copied and disseminated through the internet daily, without authorization from the copyright owners.

One way copyright owners are responding to this phenomenon is by developing technological tools to protect their works. Technological protection measures (TPMs) range from the basic to the sophisticated and provide varying degrees of protection against unauthorized access and use of the works. They include such things as password protection, copy protection, encryption, digital "watermarking"
and, increasingly, rights management systems incorporating one or more of the foregoing. Many different technological protection methods are already in use, and many others are in development (discussed further in Part V).

However, it is widely recognized that TPMs can be broken quickly by the technologically able; these individuals can then create and distribute tools to those with less technological sophistication, allowing them to circumvent protection measures. Many policy makers believed that TPMs could not be effective without legal sanctions against circumventing them or circulating circumvention tools. Accordingly, national and international bodies have supported laws that prohibit circumventing TPMs. Their goal is to facilitate electronic commerce in copyrighted works by reducing the risk to rightholders of transmitting their works over the internet.

The World Intellectual Property Organization (WIPO) in its 1996 WIPO Copyright Treaty (WCT)\(^1\) included a requirement that countries that join the treaty 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 the treaty or under the Berne Convention and that restrict acts “not authorized by the authors concerned or permitted by law.”\(^2\)

The WCT provisions appear to give substantial latitude to adhering countries in deciding how to implement the treaty. For example, the provisions do not provide specific direction on the form the protection should take: a restriction on the act of circumventing, or on the manufacture or making available of circumvention devices, or both, or a different approach such as enhancing penalties for infringement enabled by circumvention of technological measures. Copyright owners believe strong protection—against both the distribution of devices and the act of circumvention—is essential. But strong protection for technological measures comes at a cost. Users argue that such protection allows copyright owners to control all uses of their works and makes it difficult, if not impossible, to benefit from copyright exemptions and privileges. The WCT sheds little light on how to achieve “adequate protection” while accommodating users’ privileges. This has proven to be the most difficult and controversial aspect of anti-circumvention legislation. Countries have taken different approaches.

More than forty countries have already ratified the WCT and implemented it in their domestic laws.\(^3\) The United States implemented its anti-circumvention

---

3. The WIPO Copyright Treaty required ratification by thirty countries to take effect. This occurred late in 2001. A list of all Contracting Parties is available at http://www.wipo.int/treaties/en/ip/wct/index.html. In some countries, the treaty is considered “self-executing” and becomes law merely by virtue of its adoption. Other countries, such as the United States, required specific implementing legislation to alter national law in order to make it consistent with the treaty. U.S. law and that of a representative sample of other countries is discussed in greater detail in infra Parts II and III.
requirement in § 1201 of the Digital Millennium Copyright Act (DMCA), passed in October 1998.\textsuperscript{4} Section 1201 contains three principal provisions. First, § 1201(a)(1) prohibits circumventing a technological protection measure that effectively controls access to a copyrighted work. In other words, this section bars the actual act of circumventing or bypassing an access control. Second, § 1201(a)(2) prohibits manufacturing or making available products or services for circumventing technological access controls. Products or services that have a commercially significant purpose or use other than to circumvent such controls and are designed and marketed for such other purposes, are permissible. Third, § 1201(b)(1) prohibits manufacturing or making available products or services for circumventing technological measures that protect a right of a copyright owner. This provision is largely identical to § 1201(a)(2) but is directed towards products and services that circumvent rights controls (such as copying restrictions) rather than access controls.

The law includes various exemptions, each with its own requirements. While the exemptions excuse the act of circumventing technological access controls, most permit only very limited distribution of circumvention devices and some permit none at all.

The European Union implemented the WCT in Directive 2001/29/EC, concerning the harmonization of certain aspects of copyright and related rights in the information society.\textsuperscript{5} The Directive requires EU member states to protect against the act of circumventing any effective technological measures (which apparently includes access control measures).\textsuperscript{6} Member states are also required to protect against the manufacture or distribution of circumvention products or services on terms similar in many respects to those in the U.S. legislation.\textsuperscript{7} In one significant respect, however, the EU legislation differs: it requires member states to take appropriate measures to ensure that users have the means to benefit from certain specified exemptions or limitations in the law, provided the beneficiary has legal access to the protected work.\textsuperscript{8}

**B. CONCERNS ABOUT ANTI-CIRCUMVENTION LEGISLATION**

There have been many criticisms about anti-circumvention legislation in the United States and elsewhere, but the overarching concern is that it prevents


\textsuperscript{5} Council Directive 2001/29/EC, 2001 O.J. (L167/10). The member states are now in the process of incorporating the Directive into their national laws. When that process is completed, it is anticipated that the European Union and its twenty-five member states will ratify the WIPO treaties.

\textsuperscript{6} Id. at art. 6(1).

\textsuperscript{7} Id. at art. 6(2).

\textsuperscript{8} Id. at art. 6(4). Article 6 also permits (but does not require) member states, absent voluntary measures by rightholders, to take "appropriate measures" in order to enable users to take advantage of "private use" exemptions contained in national laws. On demand services are exempt from this requirement. Id.
legitimate uses of copyrighted works. With respect to provisions that protect works against unauthorized access, critics argue that (1) they, in effect, create a new copyright right without the exemptions and limitations that attach to the other rights, and (2) the exemptions in the statute are inadequate. Indeed, some believe any scheme of specifically delineated exemptions is untenable, contending that what is needed is a broad, general purpose exemption that permits circumventing access controls for “legitimate purposes” (including, for example, “fair use” of the protected work). Critics also object to the breadth of the restrictions on the manufacture and circulation of circumvention devices. They contend that devices should be available to enable users to take advantage of the exemptions to the ban on circumventing technological access controls. Similarly, they maintain that the right to circumvent copy-control devices for noninfringing purposes should not be limited to the technologically proficient. In short, they claim the scheme is inherently troublesome since technological protection measures can never be as nuanced as the law and as a result, some appropriate uses of copyrighted works will be stifled. Supporters of the legislation, on the other hand, are concerned about any broadening of the exemptions. In particular, they fear that permitting manufacture and distribution of circumvention devices for some purposes will effectively make the anti-circumvention legislation meaningless.

The differing views concerning the appropriate scope of anti-circumvention laws are discussed in greater detail in infra Part VI.

C. THE KERNOCHAN CENTER’S STUDY

The Kernochan Center’s study focused on the issues raised by anti-circumvention legislation and the requirements of the WIPO treaties, among them: What kind of legislation can adequately and effectively protect against circumvention of technological protection measures? What is the significance of extending protection to access controls as well as rights controls? Is it essential to prohibit both the act of circumvention and trafficking in circumvention devices? How can users’ privileges be accommodated fairly, without substantially


10. See, e.g., Samuelson, supra note 9. This is the approach reflected in House Bill 1066, discussed infra Part II.E.


undermining the goals of the legislation? How effective are technological measures in protecting copyrighted works (and how effective are they likely to be in the future)? How are various countries implementing the anti-circumvention provisions of the treaties?

Specifically with reference to the DMCA, the study focused on the following issues: Should the exemptions in the DMCA be supplemented or replaced by a more general "legitimate purposes" exemption, or will this render the statute ineffective? Are there specific exemptions that should be narrowed or eliminated (or others that should be included)? Is there a sound rationale for permitting circumvention in some cases, yet restricting devices that enable that activity?

The Center's study focused on several areas: The U.S. anti-circumvention legislation, including its history and its application in judicial decisions and in the Copyright Office's rulemaking proceedings under § 1201; legislation in other countries; identification and review of legal provisions that prohibit circumvention of technological protection measures in other contexts; a review of existing technologies and those under development; and commentary on anti-circumvention legislation by academics, practitioners and others. In order to understand the perspectives of the various parties with an interest in the legislation, the Kernochan Center held a series of roundtable discussions. The goal was to evoke a frank exchange of views about the advantages and problems concerning anti-circumvention legislation.

We sought further input through a large international conference held at Columbia Law School in conjunction with Association Littéraire et Artistique Internationale (ALAI) from June 13-17, 2001. One of the principal topics of the conference, entitled "Adjuncts and Alternatives to Copyright," was legal protection for technological measures that protect copyrighted works. Almost three hundred copyright scholars and practitioners from thirty-two countries attended the conference.\(^\text{13}\)

Participants in the roundtables and the ALAI conference included individuals from the Copyright Office and other government personnel, copyright owners (including representatives of the motion picture and recording industries, publishers, authors and authors' collecting societies), legal scholars from the U.S. and abroad, educational and research users of copyrighted works, and representatives of the consumer electronics industry. A list of speakers at the ALAI conference and of participants at the roundtable discussions is included in Appendix A below.

II. U.S. LAW

This section begins with a detailed description of U.S. anti-circumvention provisions, as their terms are important to understanding the cases and commentary. A description of the legislative history follows, and subsequent

---

13. See also Adjuncts and Alternatives to Copyright: Proceedings of the ALAI Congress June 13-17, 2001 (Jane C. Ginsburg & June M. Besek eds., 2002).
sections discuss treatment of § 1201 by the courts and the Copyright Office.

A. SUMMARY OF LEGISLATION

Chapter 12 of Title 17 of the United States Code, created by the DMCA, addresses circumvention of technological protection measures.\textsuperscript{14}

1. Prohibition Against Circumventing a Technological Protection Measure

The law prohibits circumventing a technological measure that "effectively controls access to a work" protected under Title 17.\textsuperscript{15}

A technological measure "effectively controls access to a work" if, in the ordinary course of operation, it requires "the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."\textsuperscript{16}

In this context, to "circumvent a technological measure" means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."\textsuperscript{17}

However, U.S. law does not prohibit circumventing a technological measure that protects a right of a copyright owner (e.g., a copy control).

2. Prohibition Against Trafficking in Circumvention Devices and Services

There are two anti-trafficking provisions. One addresses devices and services that circumvent access controls. The other addresses devices and services that circumvent rights controls. They are detailed below.

a. No Trafficking in Devices that Circumvent Access Controls

U.S. law prohibits manufacturing, importing, offering to the public, providing or otherwise trafficking in technologies, products or services (1) that are primarily designed or produced to circumvent a technological measure that effectively controls access to a work protected under Title 17, or (2) that have only limited commercially significant purposes or uses other than to circumvent such controls, or (3) that are marketed for use in circumventing such controls.\textsuperscript{18}

In this provision, the terms "effectively controls access to a work" and "circumvent a technological measure" have the same definitions as set forth in Part II.A.1.

\textsuperscript{14} Section 1202 on "Integrity of Copyright Management Information" was passed to implement another provision of the WIPO treaties. A detailed discussion of § 1202 is beyond the scope of this report.

\textsuperscript{15} 17 U.S.C. § 1201(a)(1)(A).


\textsuperscript{17} § 1201(a)(3)(A). See discussion infra Part II.C.1.

\textsuperscript{18} § 1201(a)(2).
b. No Trafficking in Devices that Circumvent Rights Controls

There is also a prohibition against trafficking in devices or services to circumvent rights controls. Specifically, U.S. law prohibits manufacturing, importing, offering to the public, providing or otherwise trafficking in technologies, products or services (1) that are primarily designed or produced to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under Title 17, or (2) that have only limited commercially significant purposes or uses other than to circumvent such a measure, or (3) that are marketed for use in circumventing such a measure.19

A technological measure "effectively protects a right of a copyright owner" if, in the ordinary course of operation, it "prevents, restricts, or otherwise limits the exercise of a right of a copyright owner" under Title 17.20

In this context, "to circumvent protection afforded by a technological measure" means "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."21

3. Exemptions

Below is a list of exemptions, each of which excuses conduct that would otherwise be prohibited by § 1201(a)(1)'s prohibition on circumventing access controls. Where they also excuse conduct that would otherwise be prohibited by one or both of § 1201(a)(2)'s prohibition on trafficking in access control circumvention devices and § 1201(b)'s prohibition on trafficking in rights control circumvention devices, we have so noted. In most cases, specific and very detailed criteria must be met in order to take advantage of the exemptions, and where the statute permits transfer of circumvention technology, the permission is usually very limited.

Pursuant to the rulemaking process under § 1201(a)(1)(B)-(E), and at least until October 28, 2006, the Librarian of Congress has mandated four exemptions, discussed in Part II.D.

Additionally, there are exemptions for:

- Nonprofit libraries, archives and educational institutions so that they can determine whether they wish to acquire a work;22
- Law enforcement, intelligence and other government activities;23
- Reverse engineering of computer programs in order to identify and analyze elements necessary to achieve interoperability with other programs;24

19. § 1201(b)(1).
20. § 1201(b)(2)(B).
22. § 1201(d).
23. § 1201(e) (exemption from § 1201(a)(2) and § 1201(b), as well).
24. § 1201(f) (exemption from § 1201(a)(2) and § 1201(b), as well).
• Encryption research;\textsuperscript{25}
• Protection of minors;\textsuperscript{26}
• Circumvention that identifies and disables the capability of a technological measure to collect personally identifying information;\textsuperscript{27}
and
• Security testing.\textsuperscript{28}

See Part II.A.5 for further discussion.

Since there is no prohibition on circumventing rights controls, there are no corresponding exemptions. Legislators believed that if copies made as a consequence of circumventing rights controls were excused by copyright exemptions or privileges, there should be no liability for the circumvention. If, on the other hand, such copies were infringing, then the rightholder would have a claim under copyright law.

4. Responsibility of Equipment Manufacturers

Equipment manufacturers are not required to design their products to respond to any particular technological measure, so long as those products do not otherwise fall within the prohibitions of § 1201(a)(2) or § 1201(b)(1).\textsuperscript{29}

5. Obligations of Rightholders

With the exception of § 112(e)(8), under U.S. law there are no statutory obligations placed on rightholders to provide beneficiaries of copyright exemptions and privileges with the means of taking advantage of those exemptions and privileges, unlike in the EU directive discussed in Part III.\textsuperscript{30} However, if rightholders are unable to take advantage of statutory privileges, the Librarian of Congress may create an exemption to the ban on circumventing access controls under § 1201(a)(1)(B)-(E). That contingency may affect rightholders' choices of protective technology for their works and their decisions whether to continue to market unprotected versions.

Section 112(e) of the Copyright Act permits transmitting organizations to make "ephemeral" phonorecords (copies) of sound recordings in certain specified circumstances for purposes of transmission or archival preservation. Under

\textsuperscript{25} § 1201(g) (exemption from § 1201(a)(2), as well).
\textsuperscript{26} § 1201(h) (exemption from § 1201(a)(2), as well).
\textsuperscript{27} § 1201(i).
\textsuperscript{28} § 1201(j) (exemption from § 1201(a)(2), as well).
\textsuperscript{29} § 1201(c)(3). See infra note 68 (discussing differing views in Congressional reports). There is one exception to this "no mandate" rule. Section 1201(k) requires that within eighteen months of the legislation's effective date, analog videocassette recorders manufactured or sold in the United States must be designed to conform with certain defined copy protection technologies. Those technologies may not, however, be used to preclude consumers from copying free television or basic cable broadcasts. See also the discussion of the FCC's "broadcast flag" proceeding infra Part II.E.
\textsuperscript{30} But see supra note 29 (discussing certain mandated copy control technologies). Also, there are no statutory bans on circumventing rights controls, as noted in supra Part II.A.1.
§ 112(e)(8), copyright owners are required to make available to a transmitting organization "the necessary means for permitting the making of such phonorecord as permitted under this subsection, if it is technologically feasible and economically reasonable for the copyright owner to do so." If the copyright owner fails to meet this requirement in a timely manner, "the transmitting organization shall not be liable for a violation of § 1201(a)(1) of this title for engaging in such activities as are necessary to make such phonorecords as permitted under this subsection."

6. Ongoing Monitoring

There are three provisions in the DMCA that call for further study with respect to legal protection for technological protection measures. Copyright Office activities pursuant to these provisions are discussed in Part II.D.

a. Section 1201(a) Rulemaking

The prohibition against the act of circumventing technological access controls did not go into effect until October 28, 2000, two years after the date the DMCA was enacted. During that two-year period (and in each subsequent three-year period thereafter), the Librarian of Congress was directed to determine through a rulemaking proceeding whether users of any particular class of copyrighted works are, or are likely to be, adversely affected in their ability to make non-infringing uses of those works by the prohibition against circumventing technological access controls. If so, the Librarian of Congress was directed to lift the prohibition for that particular class of works for the ensuing three-year period. As a result of the most recent rulemaking proceeding, the Librarian exempted four classes of works. This determination provides an exemption only from § 1201(a)(1), which prohibits circumvention of access controls. It does not affect potential liability under the anti-trafficking provisions.

b. Study Concerning Encryption Research and Technology

Under § 1201(g)(5), the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce were required to report jointly to Congress, one year after the DMCA went into effect, on the effect of § 1201 on encryption research and encryption measures.

c. Study Under Section 104 of the DMCA

Section 104 directed the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce to evaluate the effect of the DMCA and of new technologies on the operation of § 109 (first sale

doctrine) and § 117 (copying of computer programs).

Other aspects of Chapter 12 deserve mention. Section 1201(c) contains two "savings clauses." One makes clear that "[n]othing in [§ 1201] shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." The other states that nothing in § 1201 "shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product or service." 33

The principal civil remedies available for violation of § 1201 are temporary and permanent injunctions and damages. In the case of repeat offenders, a court may award up to treble damages. 34 A court may decline to award damages against innocent violators. There are also criminal sanctions (fine and/or imprisonment) available if someone violates § 1201 "willfully and for purposes of commercial advantage or private financial gain." 35

B. HISTORY OF U.S. ANTI-CIRCUMVENTION PROVISIONS

1. Action Prior to 105th Congress

The U.S. anti-circumvention provisions originated in a 1995 report entitled Intellectual Property and the National Information Infrastructure (commonly referred to as the "White Paper"). 36 The White Paper was the product of the Working Group on Intellectual Property Rights of the Task Force on the National Information Infrastructure. The Working Group was created in 1993 during the first Clinton administration to review intellectual property aspects of the internet. It was chaired by Bruce Lehman, then Assistant Secretary of Commerce and Commissioner of Patents and Trademarks. 37

The White Paper proposed a legislative ban on circulation of circumvention devices:

Circumvention of Copyright Protection Systems. No person shall import, manufacture or distribute any device, product, or component incorporated into a device or product, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without the authority of the copyright owner or the law, any process, treatment, mechanism or system which prevents or inhibits the violation of any of the exclusive rights of the copyright owner under section 106. 38

---

33. § 1201(c).
34. § 1203(b).
35. § 1204(a).
37. The United States urged the adoption of anti-circumvention provisions in the international arena as well, proposing to WIPO the inclusion of such a provision in a treaty under consideration known at the time as "the Berne Protocol."
The White Paper did not recommend a prohibition on the act of circumventing itself. Nor did the proposed formulation explicitly address access or access controls, though to the extent that such controls "inhibit" the violation of exclusive rights they are embraced in this prohibition.

The premise of the Working Group's recommendation was that legal protection alone would not provide sufficient incentive to authors to create and distribute their works in the internet environment, where they could easily be copied and disseminated without permission. It concluded that while technological protection measures would provide additional security, they would likely not be effective without legal reinforcement. A law prohibiting circumvention of technological protection measures would be consistent with the constitutional goals of copyright, the White Paper asserted, since it would ultimately increase public access to copyrighted works online. 39

The White Paper emphasized that its proposal would prohibit only those devices or products whose primary purpose or effect was to circumvent technological protections without authority. Such authority, it explained, could come either from the copyright owner or from limitations on copyright rights in the Copyright Act. 40

In response to concerns that the proposed anti-circumvention provision would inhibit fair use of copyrighted works, 41 the Working Group asserted that fair use "does not require a copyright owner to allow or to facilitate unauthorized access or use of a work." 42 "Otherwise," the report reasoned, "copyright owners could not withhold works from publication; movie theaters could not charge admission or prevent audio or video recording; museums could not require entry fees or prohibit the taking of photographs. Indeed if the provision of access and the ability to make fair use of copyrighted works were required of copyright owners—or an affirmative right of the public—even passwords for access to computer databases would be considered illegal." 43

The White Paper stated that under its proposed formulation, if a circumvention device is primarily intended and used for legal purposes, such as fair use, its distribution would be permitted, because a device with such purposes and effects would fall under the "authorized by law" exemption. 44

The Report responded similarly to criticisms that the proposed provision would limit access to works in the public domain. It pointed out that a device whose primary purpose or effect is to defeat protection for such works would not violate the provision, since it was intended to be used for legal purposes, and also because it was not a device that prevents or inhibits the violation of exclusive rights under

39. Id. at 230.
40. Id. at 231.
41. A draft of the White Paper (known as the "Green Paper") was disseminated for comment in 1994. Some of the discussion in the White Paper attempts to respond to concerns raised in those comments.
42. WHITE PAPER, supra note 36, at 231 (emphasis added).
43. Id.
44. Id.
copyright. It also pointed out that a technological protection mechanism would affect only particular copies, not the underlying work, implicitly assuming that the work would be otherwise available.

Shortly after the White Paper was issued, bills incorporating its legislative recommendations were introduced in both houses of Congress. The anti-circumvention provisions in those bills tracked the Working Group's proposal. Although hearings were held in the Senate in late 1995 and early 1996, neither bill passed in the 104th Congress.

Meanwhile, at a diplomatic conference in Geneva in December 1996, nations from around the world, including the United States, agreed on two new treaties: the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). Both treaties required adhering countries to include anti-circumvention provisions in their national legislation, as discussed above in Part I.A.

2. Action in the 105th Congress

In July 1997, legislation to change U.S. law to implement the requirements of the WIPO treaties and enable the U.S. to ratify them was introduced in the House of Representatives. That bill, H.R. 2281, contained the following anti-circumvention provision:

Section 1201. Circumvention of copyright protection systems.

(a) VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL PROTECTION MEASURES.

(1) No person shall circumvent a technological protection measure that effectively controls access to a work protected under this title.

(2) No person shall manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof that—

(A) is primarily designed or produced for the purpose of circumventing a technological protection measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to

45. The White Paper did not grapple with the most vexing issue: What if the same type of protection measure is used to protect public domain and non-public domain works so that circumvention devices would be the same for both? If the "primary effect" of such a device is to enable circumvention of the measure on protected works, how can it be made available to those who want to use it to access public domain works without running afoul of the law? This issue is discussed infra Part VI.

46. WHITE PAPER, supra note 36, at 232.


48. Hearings were held in the Senate on S. 1284 on November 15, 1995 (government and WIPO witnesses), February 7-8, 1996 (private sector witnesses) and May 7, 1996 (private sector witnesses).

circumvent a technological protection measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person for use in circumventing a technological protection measure that effectively controls access to a work protected under this title.

It also included an analogous prohibition against distributing devices to circumvent rights controls, in language similar to the current § 1201(b).

The anti-circumvention provisions in H.R. 2281 were more stringent than those in the White Paper and the earlier bills. H.R. 2281 contained a specific prohibition on circumventing access controls, thus introducing the so-called "access right." It barred devices to circumvent either access or rights controls.\(^50\) The prohibition in H.R. 2281 extended not only to devices whose "primary purpose or effect" was to circumvent (as the White Paper had), but also to devices marketed for that purpose or that had no commercially significant purpose or use other than to circumvent.\(^51\) The anti-trafficking provision in H.R. 2281 differed from that in the White Paper in another significant way. The White Paper had barred only those devices whose primary purpose and effect was to circumvent "without the authority of the copyright owner or the law." That limitation—which presumably would have permitted circumvention of devices to facilitate fair use and other privileges—was not incorporated in H.R. 2281 or, ultimately, in § 1201. As introduced, H.R. 2281 contained a single exemption (the earlier versions had none) for law enforcement and intelligence activities.

The House Subcommittee on Courts and Intellectual Property of the House Judiciary Committee held hearings in fall 1997.\(^52\) The following spring, the House Committee on the Judiciary issued its report on H.R. 2281.\(^53\) As reported out of committee, the anti-circumvention provision was substantially unchanged, except that it included a second exemption (in addition to the one for law enforcement in the bill as introduced) for nonprofit libraries, archives and educational institutions to circumvent access controls solely to determine whether they wished to acquire a commercially exploited work.\(^54\)

After the House Judiciary Committee issued its report, H.R. 2281 was

---

50. In addition, it contained a provision barring importation of circumvention devices. H.R. 2281 § 103 (proposed § 1201(c)).

51. Both the White Paper and H.R. 2281 impose on devices a standard higher than the "merely capable" of non-infringing uses articulated in the *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), though H.R. 2281 and § 1201 as passed are considerably more restrictive of devices than the White Paper.

52. Hearings on H.R. 2281 and H.R. 2180, a related bill that addressed internet service providers' potential liability, were held on September 16-17, 1997 before the Subcommittee on Courts and Intellectual Property of the House Judiciary Committee. An alternate bill to implement the WIPO treaties was introduced in the House in fall 1997, H.R. 3048, 105th Cong. (1997). H.R. 3048 included not only WIPO treaty implementation legislation, but other provisions as well, as did S. 1146, discussed below. Its anti-circumvention provision closely resembled that of S. 1146, which had been introduced in the Senate a couple of months earlier.


54. *Id.* at 20.
sequentially referred to the House Committee on Commerce.

While H.R. 2281 was under consideration in the House, a different version of WCT implementing legislation moved rapidly through the Senate. S. 2037\textsuperscript{55} was introduced on May 6, 1998, reported out of the Senate Judiciary Committee on May 11, 1998 and passed by the Senate on May 14, 1998. S. 2037's rapid passage was the apparent result of behind-the-scenes work in the Senate to reconcile supporters of two versions of WIPO-implementing legislation introduced in the Senate earlier in the 105th Congress that failed to advance.\textsuperscript{56}

In addition to the provisions strictly necessary for treaty implementation, S. 2037 included provisions limiting copyright liability for internet service providers relating to online material, an amendment to § 117 of the Copyright Act in connection with computer repair and maintenance and a fourth title that addressed a number of issues including ephemeral recordings (a proposed amendment to § 112 of the Copyright Act), a report in connection with distance education and a modest expansion of the privileges of libraries and archives to make reproductions for preservation, security and replacement purposes.

The anti-circumvention provision in S. 2037 was similar in its basic thrust to that of H.R. 2281. The bill contained four exemptions from the ban on circumventing access controls: for law enforcement, § 1201(e); for nonprofit libraries and archives to examine a work to determine whether to acquire it, § 1201(d); for reverse engineering to achieve interoperability, § 1201(f)-(i); and an exemption concerning minors and inappropriate material on the internet, § 1201(j).

The reverse engineering exemption, according to the Senate Judiciary Committee Report, was intended “to allow legitimate software developers to continue engaging in certain activities for the purpose of achieving interoperability to the extent permitted by law prior to the enactment of this chapter.”\textsuperscript{57} According to the report, the exemption concerning minors was adopted to ensure that the prohibitions in § 1201(a) did not inadvertently make it unlawful for parents to protect their children from pornography or other inappropriate material on the internet.\textsuperscript{58}

The Senate report did not advocate a specific exemption for encryption research. However, it stated the Committee's view that generally available encryption testing tools would be permissible under the act.\textsuperscript{59}

Meanwhile, WIPO treaty implementing legislation continued to move forward

\textsuperscript{55} S. 2037, 105th Cong. (1998).
\textsuperscript{56} S. 1121, 105th Cong. (1997), contained an anti-circumvention provision similar to that in H.R. 2281 as introduced. The second bill, S. 1146, 105th Cong. (1997), contained not only treaty implementation language but a host of other provisions as well (for example, a limitation on copyright liability for internet service providers, an expansion of the library photocopying privileges in § 108, and an expansion of the exemptions in § 110 to facilitate distance education). Its anti-circumvention provision was more limited than those in the other pending bills, containing only a ban on the act of circumventing for the purpose of infringement, and no restriction on the circulation of circumvention devices. S. 1146, § 301.
\textsuperscript{57} S. REP. NO. 105-190, at 13 (1998).
\textsuperscript{58} Id. at 14.
\textsuperscript{59} Id. at 15.
in the House of Representatives. The Commerce Committee’s Subcommittee on Telecommunications, Trade and Consumer Protection held hearings on H.R. 2281 on June 5, 1998, and the full Commerce Committee reported the bill out on July 22, 1998 with some significant modifications.\textsuperscript{60}

The Commerce Committee Report reflects that Committee’s concern about the possible effects of § 1201 on the ability to make fair use of copyrighted works.\textsuperscript{61} Specifically, it recommended:

- Turning § 1201(a)(1) into a requirement that the Secretary of Commerce issue regulations prohibiting circumvention of technological access controls, rather than making it an outright statutory prohibition.\textsuperscript{62}
- Delaying the effect of the prohibition for two years to give the Secretary of Commerce the opportunity to conduct a rulemaking to determine whether there are classes of works whose users are, or over the next two years are likely to be, adversely effect in their ability to make non-infringing uses of copyrighted works by the implementation of technological access controls, and if so, to exempt each such class of work from the operation of the regulation prohibiting circumvention of access controls. That rulemaking, to be done in consultation with the Assistant Secretary of Commerce for Communications and Information, the Commissioner of Patents and Trademarks and the Register of Copyrights, was to be repeated every two years.\textsuperscript{63}
- Including not only the two exemptions supported by the House Judiciary Committee, but also four more. Two of them—for reverse engineering and for preventing access by minors to inappropriate materials on the internet—had been included in S. 2037 as passed by the Senate. The other two were for encryption research and to facilitate protection of personally identifying information.\textsuperscript{64}

With regard to the exemption for encryption research, the Committee emphasized the need for “rapid and dynamic development” of better encryption technology.\textsuperscript{65} The exemption was designed to permit “legitimate encryption research” into flaws in existing encryption systems.\textsuperscript{66}

The “personal information” exemption sprang from the Committee’s concern about digital technology that could surreptitiously gather consumers’ personal information by means of software that is protected, or “cloaked,” by a technological measure.\textsuperscript{67} It permits the user to discover and disable such programs, creating an incentive for copyright owners to disclose fully personal data-gathering practices.

The version of H.R. 2281 ultimately placed on the calendar and passed by the

\textsuperscript{60} H.R. REP. NO. 105-551, pt. 2 (1998).
\textsuperscript{61} See, e.g., id. at 25.
\textsuperscript{62} Id. at 2, 36.
\textsuperscript{63} Id. at 2-3, 35-38.
\textsuperscript{64} Id. at 4-6, 41-45.
\textsuperscript{65} Id. at 27.
\textsuperscript{66} Id. It also added a study in respect of encryption research. Id. at 5.
\textsuperscript{67} Id. at 27.
House of Representatives on August 4, 1998 reflected a compromise between the House Judiciary Committee and the House Commerce Committee. The basic provision governing the act of circumvention, § 1201(a)(1), was once again a statutory prohibition rather than a direction to the Secretary of Commerce to issue regulations. The rulemaking structure, however, remained substantially intact, with the determination the ultimate responsibility of the Secretary of Commerce.

3. Route to Final Passage

Since the versions of WIPO treaty implementing legislation passed by the House and Senate differed, a Conference Committee was established. As reported out of the Conference Committee, H.R. 2281 contained all of the exemptions in the House version of the bill, as well as one for system testing. This exemption was designed to cover persons who access computers and computer systems, with the owner's authorization, for good faith testing for security flaws. It is not a violation to circumvent access controls to engage in such testing, provided it does not

---

68. Since the House Judiciary Committee Report was issued before most of the exemptions to § 1201 were introduced into the legislation, it did not address their scope. After the bill was passed in the House, a report analyzing its provisions was issued by the House Judiciary Committee staff. See STAFF OF HOUSE COMM. ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998 (Comm. Print 1998) (Rep. Coble) [hereinafter HOUSE MANAGER'S REPORT]. The weight to be accorded this document has been debated. See infra note 141. There are marked differences between the House Commerce Committee Report and the House Manager's Report in some areas. For example, the Commerce Committee Report expresses the view that the legislation does not prevent equipment manufacturers from designing or modifying their products to mitigate "playability" problems, that is, measures causing "noticeable and recurring adverse effects on the authorized display or performance of works." According to the Report, such measures cannot be deemed "effective." HOUSE MANAGER'S REPORT at 40-41. The House Manager's Report disagreed, expressing concern that these statements would cause manufacturers to circumvent whenever they believed their equipment would function better without the protective measures. Id. at 11-12. The Conference Committee attempted to resolve the differences by stating that a manufacturer would not be liable for violating circumvention prohibitions "solely to mitigate . . . adverse effects on product performance." H.R. REP. NO. 105-796, at 65 (1998). However, the Report echoed the concern expressed in the House Manager's Report and clarified:

[T]his construction is not meant to afford manufacturers or servicers an opportunity to give persons unauthorized access to protected content, or to exercise rights under the Copyright Act of copyright owners in such works, under the guise of "correcting" a performance problem that results from the implementation of a particular technical measure.

Id.

69. Between its introduction and passage in the House, H.R. 2281 acquired many provisions beyond those strictly necessary for WIPO Treaty implementation, including a title limiting liability for internet service providers (originally introduced as a separate bill, see supra note 52), an amendment to § 117 addressing computer maintenance and repair, a host of miscellaneous amendments to the copyright law for matters such as distance education, copying by libraries and archives, and so on. It had also acquired three additional titles dealing with protection for collections of information, vessel hull protection, and the assumption of certain contractual obligations related to the transfer of rights in motion pictures.

70. The House bill, H.R. 2281, had been placed on the Senate calendar. The Senate amended the bill by substituting the text of S. 2037, and passed H.R. 2281 as amended.

constitute infringement or any other legal violation.\footnote{Id. at 66-67.}

The Conference Committee retained most aspects of the rulemaking procedure in the House version of the bill but transferred authority in respect of the rulemaking from the Secretary of Commerce to the Librarian of Congress, on the recommendation of the Register of Copyrights.\footnote{The Department of Commerce retained a role in the determination, however, as the final version of the bill required the Register of Copyrights to consult with the Assistant Secretary for Communications and Information and report or comment on his or her views in making the recommendation to the Librarian. § 1201(a)(1)(C). The rulemaking is discussed further infra Part II.D.}

The final version of H.R. 2281 was passed by the Senate on October 8 and by the House on October 12. It was signed by the president and became effective October 28, 1998.

C. SECTION 1201 IN THE COURTS

It did not take long from the passage of the DMCA for the first cases to reach the courts. The earliest cases addressed only the device distribution prohibitions, since the law against circumventing access controls did not take effect until 2000.

1. Statutory Issues

   a. What Technological Measures Are Protected?

In RealNetworks, Inc. v. Streambox, Inc.,\footnote{No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).} the court granted a preliminary injunction against the distribution of defendant's "Streambox VCR." RealNetworks' content delivery system allowed copyright owners to encode and communicate their works via a "RealServer" to consumers who could access them using a "RealPlayer." The RealPlayer and the RealServer worked together to allow content owners to make their works available for streaming, but not for copying, by consumers. This was done through the use of two security mechanisms: (i) the "secret handshake," an authentication sequence that ensured that content from a RealServer is streamed only to a RealPlayer; and (ii) a copy switch that allowed the copyright owner to determine whether or not to permit consumer copying. The Streambox VCR used the RealPlayer's "secret handshake" essentially to disguise itself as a RealPlayer and trick the RealServer into sending files, but it ignored the copy switch. Thus, consumers who purchased the Streambox VCR could access the content licensed for the RealPlayer without the hindrance of copy restrictions.

The court concluded that the secret handshake and the copy switch were protected technological measures and that the Streambox VCR, which bypassed them to allow consumers to copy the streamed content, was a circumvention device within the meaning of § 1201. The court ruled that the Streambox VCR was designed primarily, if not exclusively, to circumvent the access control and copy
protection measures provided by RealNetworks’ system and that it had no other significant commercial purpose.

Streambox argued that its VCR did not violate § 1201 because it allowed consumers to make fair use copies of files distributed via the RealServer, citing the Supreme Court’s decision in *Sony Corp. of America v. Universal City Studios*. In *Sony*, the Court held that time-shifting broadcast television programs by consumers was a fair use and, consequently, a "substantial non-infringing use" that justified distribution of Sony's Betamax video tape recorder. The RealNetworks court rejected Streambox's claim, concluding that the DMCA did not employ Sony's "substantial non-infringing use" standard.

The court entered a preliminary injunction against further distribution of the Streambox VCR, citing the potential harm to RealNetworks and the public if lack of confidence in RealNetwork's security measures made copyright owners less willing to make their audio and video works available over the internet.

In *Universal City Studios v. Reimerdes*, defendants, who operated a website geared toward hackers, were sued under § 1201 for posting and linking to a software utility known as DeCSS. DeCSS unlocks the encryption mechanism known as the Content Scramble System, or CSS, that protects motion pictures on digital versatile disks (DVDs) from being copied or played on non-compliant DVD players or computer drives.

The district court concluded that CSS "effectively controls access" to the motion pictures on DVDs, since keys are required to access the motion pictures, and the keys cannot be obtained without a license or the purchase of an authorized DVD player or a drive. The court rejected defendants' argument that CSS does not control access because it is "weak" encryption, pointing out that the statute would be meaningless if it protected only successful technological measures. It held DeCSS was a circumvention device under § 1201(a)(2) since it was designed primarily to decrypt CSS.

The court rejected the defense that DeCSS was created not to pirate motion pictures but to further the development of a DVD player that runs under the Linux operating system. According to the court, since these defendants did not create DeCSS, the reason for its development was immaterial to them. Offering it on their website to circumvent CSS was prohibited conduct, regardless of why it was

76. Id. at 442.
78. Another authentication sequence was at issue in *Lexmark Int'l v. Static Control Components*, 253 F. Supp. 2d 943 (E.D. Ky. 2003), appeal docketed, No. 03-5400 (6th Cir. argued Jan. 31, 2004). The court held that the authentication sequence, which controlled access to a computer program in Lexmark's toner cartridges, was a protected technological measure. Lexmark sought through the authentication sequence to prevent customers from using toner cartridges from other manufacturers. The case is discussed further below.
80. Id. at 317-18.
written. 81

321 Studios v. Metro-Goldwyn-Mayer Studios 82 was another challenge to the application of § 1201 in the context of DVD encryption. 321 Studios developed and marketed “DVD Copy Plus” and “DVD–X COPY” software and documentation, which enable consumers to make copies of the contents of DVDs and store them on CDs or recordable DVDs, respectively, notwithstanding the copy protection provided by CSS. 321 Studios sought a declaratory judgment that distribution of its software does not violate § 1201, since it merely enabled legitimate uses by consumers, such as copying public domain materials, making back-up copies or fair use. In the alternative, 321 Studios sought a judgment that § 1201 is invalid on constitutional grounds.

The court granted summary judgment to defendants. It held, like Reimerdes, that CSS is an effective technological measure protected under § 1201. 83 Concerning 321’s claim that the primary intended purpose of its software is to enable legitimate uses by consumers, the court concluded that “legal downstream use of copyrighted materials by customers is not a defense” to 321’s violation of § 1201(b). 84 It went on to rule that 321’s software (or a component thereof) was primarily designed to circumvent CSS and marketed for that purpose. 85 The court entered a preliminary injunction against 321, ordering it to cease distribution of its DVD copying software. 321 immediately announced its intention to seek an emergency stay of the injunction and appeal the court’s order. 86

Paramount Pictures Corp. v. 321 Studios, 87 was another case involving 321 Studios’ “DVD Copy Plus” and DVD-X COPY” software. Relying on Reimerdes and 321 Studios, the court dismissed 321’s argument that its software was not primarily designed and produced for circumvention. The court granted a preliminary injunction against further distribution of 321 Studios’ software.

IMS Inquiry Management Systems v. Berkshire Information Systems 88 involved a different type of access control, password protection. The court held that password protection on plaintiff’s website qualified as a protected technological measure that effectively controls access to a copyrighted work. Entering the password, according to the court, constitutes the “application of information” in order to gain access to the work. The case will be discussed further below.

In Sony Computer Entertainment America v. GameMasters, 89 the court entered a preliminary injunction against defendants’ distribution of “Game Enhancer,” a device that permits users in the United States to play videogames licensed by Sony

81. Id. at 319.
83. Id. at *22.
84. Id. at *30.
85. Id. at *34. The court declined to decide on summary judgment whether 321’s product has only limited commercially significant purpose or use other than circumvention.
89. 87 F. Supp. 2d. 976 (N.D. Cal. 1999).
exclusively for use on Japanese or European Playstation consoles. Sony’s Playstation game console allows consumers to play videogames in CD-ROM format on a television set and is designed to operate only after it confirms, by reading encrypted data on the Sony CD-ROMs, that the videogame is authorized for use in the same geographic territory as the game console. The court concluded, with little discussion, that the Game Enhancer appeared to be a device whose “primary function” was to circumvent a technological measure that controls access to a work protected by copyright.

b. What Does it Mean to “Circumvent” a Technological Measure?

321 Studios claimed that its software does not “circumvent” CSS because purchasers of DVDs—on which 321’s products operate—have the authority of the copyright owner to bypass CSS. It also argued that its software did not violate § 1201 any more than DVD players do, since they also decrypt CSS. The court, however, held that purchasing a DVD does not give the purchaser authority to decrypt CSS. It also distinguished 321’s software from DVD players that decrypt CSS with the authorization of copyright owners pursuant to stringent license conditions.

Plaintiff in Chamberlain Group v. Skylink Technologies was more successful in its claim that circumvention was authorized and therefore not a violation of § 1201. Chamberlain claimed that Skylink’s universal remote transmitter violates § 1201 by circumventing the access control on the computer program in the receiver of Chamberlain’s garage door opener. Chamberlain’s computer program has two functions: It verifies the code received from the transmitter, and it activates the motor on the garage door. The court granted summary judgment to Skylink, concluding that Chamberlain had tacitly authorized the circumvention by failing to notify consumers that they were limited to Chamberlain-manufactured replacement transmitters in a market in which universal transmitters are commonly sold (including by Chamberlain).

In IMS Inquiry Management Systems v. Berkshire Information Systems, IMS operated a web-based service known as “eBasket,” which it licensed to clients (each of whom received a unique user ID) to track magazine advertising. Berkshire allegedly obtained a user ID and password issued to a third party and used it to access and copy the eBasket web pages. The court held that although IMS’s password protection system was an “effective technological measure,” Berkshire’s actions did not qualify as circumvention under § 1201. Berkshire did not “descramble, decrypt, avoid, bypass, deactivate or impair” a technological measure, according to the court. The court distinguished *Reimerdes* because defendants in

---

90. Sony also alleged that Game Enhancer 5.0 permits users to play counterfeit copies of Sony videogames, but there was no evidence that defendants distributed Game Enhancer 5.0.
93. 292 F. Supp. 2d 1040 (N. D. Ill. 2003), *appeal pending* (Fed. Cir.).
that case used a circumvention device, DeCSS, which was similar to a skeleton key or a neutralizing device. Berkshire, in contrast, merely used a valid user ID and password issued to an IMS client to gain access.

c. What Is a "Work Protected Under This Title?"

In *Lexmark International v. Static Control Components*, 95 Lexmark, a manufacturer of computer printers and toner cartridges, sued Static Control, a rival manufacturer of replacement toner cartridges. Lexmark’s printer and toner cartridge operations are controlled by computer programs. Lexmark printers function only with authorized Lexmark cartridges, identified through an authentication sequence. Static Control’s “Smartek” replacement microchips enable unauthorized toner cartridges to function with Lexmark’s printers. Lexmark alleged, among other things, that Smartek chips violated the DMCA by circumventing the authentication sequence that controls access to both of Lexmark’s programs.

The court found Static Control liable under § 1201 for circulating a device designed and marketed to circumvent a technological measure that controls access to a copyrighted work—specifically, to Lexmark’s computer programs. Static Control argued that the DMCA was intended to protect copyrighted works that have independent market value. The court, however, refused to read such a limitation into § 1201(a)(2), which by its literal terms applies to technical measures that protect access to “a work protected under this title,” and a computer program is such a work.

d. Statutory Exemptions

Defendants in *Reimerdes* argued they were exempt from liability under the reverse engineering exemption in § 1201(f), because DeCSS was necessary to achieve interoperability between the Linux operating system and DVDs. The court ruled that defendants could not avail themselves of the exemption: first, because information acquired through reverse engineering may be made available only by the party who undertook the reverse engineering (defendants merely took DeCSS from another website) and second, because defendants did not post DeCSS solely to achieve interoperability with Linux. According to the court, even the creators of DeCSS could not credibly claim that their sole purpose was to create a Linux DVD player. 96 The court also rejected defendants’ attempts to invoke two other statutory exemptions, for encryption research under § 1201(g) (because there was no evidence that defendants were engaged in good faith encryption research) and security testing under § 1201(j) (because there was no evidence DeCSS had anything to do with security testing or that defendants’ activities were

authorized).97

The Reimerdes court declined to read a fair use exemption into § 1201. It concluded that the anti-trafficking provisions of § 1201 are subject only to the exemptions in the statute (which do not include a general fair use exemption).98

Defendant in the Lexmark case similarly failed to qualify for the exemption under § 1201(f) for reverse engineering for compatibility purposes. Static Control’s Smartek microchips did not contain independently created computer programs; instead, they included identical copies of Lexmark’s program, more than what was essential for compatibility.99 The court entered a preliminary injunction in Lexmark’s favor.

2. Constitutional Challenges

a. Distribution of Circumvention Devices

In the portion of its opinion that became the principal basis of defendants’ appeal (discussed below), the Reimerdes court dismissed defendants’ argument that prohibiting dissemination of DeCSS violated their First Amendment rights. The court held that the anti-trafficking provisions of the DMCA were content-neutral, a valid exercise of Congressional authority and not unduly restrictive of expression.100 The court also examined the constitutionality of the DMCA as applied to linking. It concluded that while plaintiffs could readily take action against other sites based in the U.S. that post DeCSS, the real significance of an injunction against linking is to prohibit links to foreign sites less amenable to suit in the U.S. But the court conceded that a ban on linking to web sites with content other than DeCSS could have a chilling effect. Therefore, it concluded there should be no liability for such a link without clear and convincing evidence that those responsible for the link “(a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not lawfully be offered, and (c) create or maintain the link for the purpose of disseminating that technology.”101 Plaintiffs had made the requisite showing, according to the court.

On appeal, defendants focused on their constitutional challenge to § 1201 of the DMCA.102 They argued that DeCSS is speech entitled to full First Amendment protection and that § 1201 fails to meet the strict scrutiny applied to content-based regulation of speech. They also claimed that § 1201 restricts “fair use” of copyrighted works, in violation of the First Amendment.103

97. Id. at 320-21.
98. Id. at 322-24.
100. Reimerdes, 111 F. Supp. 2d at 332.
101. Id. at 341.
103. Id. at 436. The Second Circuit ruled that defendants’ third argument that § 1201 violates the “limited times” requirement of the Constitution was not properly before the court, and in any case was “premature and speculative.” Id. at 444-45.
At the outset, the Second Circuit refused defendants' invitation to avoid the constitutional issues by interpreting § 1201 to allow circumvention of encryption technology protecting copyrighted material (and presumably distribution of that technology) as long as the material is used for fair use purposes. The court viewed defendants' proposed reading of the statute as implausible and contrary to the legislative history.\textsuperscript{104}

The Second Circuit concluded that computer code can merit First Amendment protection. However, like the district court, it ruled that code is not pure speech but also has a functional aspect which affects the scope of its First Amendment protection.\textsuperscript{105} It found that the prohibition on posting DeCSS was aimed at its functional, nonspeech component and was content-neutral (and, consequently, not subject to the strictest form of First Amendment scrutiny).\textsuperscript{106}

Accordingly, the statute must have a "substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest."\textsuperscript{107} The court concluded that the government's interest in preventing unauthorized access to encrypted copyrighted works is "unquestionably substantial" and that regulating DeCSS by prohibiting its posting "plainly serves that interest" which is unrelated to the suppression of free expression.\textsuperscript{108}

In determining that the incidental regulation of speech did not burden speech more than necessary to further the government's interest in preventing unauthorized access to copyrighted materials, the court observed that posting DeCSS to a website makes it "instantly available at the click of a mouse" to anyone around the world and that defendants had not shown any means of preventing this worldwide distribution that would have a lesser burden on the code's communicative aspect. It rejected the attempt by defendants (and amici) to use the Audio Home Recording Act as the model for a less burdensome solution.\textsuperscript{109}

The court also affirmed the district court's three-part test for enjoining linking. Defendants urged the addition of a requirement of proof of intent to cause harm, which the court rejected. Defendants also claimed that a linking prohibition could be valid only if the same prohibition could be applied to the publication in a print medium of an address for a bookstore at which prohibited material could be obtained. The court said that defendants' arguments ignored the reality that hyperlinks can facilitate instantaneous unauthorized access to copyrighted materials in a manner that publishing a bookstore address in print cannot. The court observed that the case raised difficult issues concerning how much impairment of

\begin{flushright}
104. \textit{Id.} at 443.
105. \textit{Id.} at 452-53.
108. \textit{Id.}
109. \textit{Id.} at 454-55 n.28.
\end{flushright}
communication should be tolerated to prohibit unauthorized decryption of copyrighted works, but how the balance is struck is an issue for Congress. And, according to the court, the legislative solution adopted by Congress and applied by the district court is consistent with the First Amendment.  

In United States v. Elcom Ltd., defendant was a software company, doing business as Elcomsoft, charged with distributing a device called “the Advanced eBook Processor” that enabled consumers to strip copy protection and other restrictions from works distributed in the Adobe eBook Reader format. Elcom was indicted for alleged violations of § 1201(b) of the DMCA. Defendant moved to dismiss the indictment, challenging the statute as unconstitutional. Specifically, it claimed § 1201(b): (i) is unconstitutionally vague, and therefore violates due process; (ii) violates the First Amendment since it is an impermissible content-based restriction on speech and restricts the ability of users to engage in fair use; and (iii) exceeds Congress’s constitutional power.  

The court rejected the premise of defendant’s due process argument—that Congress meant to ban trafficking only in tools to circumvent copy restrictions in order to enable infringement but not in devices designed to circumvent restrictions to enable fair use. It concluded instead that “all tools that enable circumvention of use restrictions are banned, not merely those that prohibit infringement.” Accordingly, the court found no ambiguity in the statute.  

The court relied on Corley, concluding that the DMCA targets the functional aspect of DeCSS and passes muster under the First Amendment, because it furthers an important governmental objective to reduce copyright piracy and does not burden substantially more speech than necessary.  

Edelman v. N2H2, Inc. involved a challenge to § 1201 in another context. Benjamin Edelman filed this declaratory judgment action against N2H2, a company that markets a computer program to block certain internet content. Edelman, a computer consultant (and law student), claimed N2H2’s program is over- and under-inclusive, and therefore its use by schools and libraries to block objectionable material violates the First Amendment. Despite restrictions in N2H2’s license, Edelman proposed to (i) reverse engineer N2H2’s program to identify technical measures that protect the list of websites it blocks (“the block

110. Id. at 458.
111. 203 F. Supp. 2d 1111 (N.D. Cal. 2002).
112. This case became a lightning rod for criticism of the DMCA’s anti-circumvention provisions when Russian programmer Dmitry Sklyarov was detained while in the United States to speak at a conference, on the ground that he had helped to develop the Advanced eBook Processor that was distributed by his employer, Elcomsoft. The Justice Department eventually allowed Sklyarov to return home and elected to proceed against Elcomsoft. See Electronic Frontier Foundation, UNINTENDED CONSEQUENCES: FIVE YEARS UNDER THE DMCA 6, available at http://www.eff.org/unintended_consequences; Lawrence Lessig, Jail Time in the Digital Age, N.Y. TIMES, July 30, 2001, at A7.
113. Elcom, 203 F. Supp. 2d at 1122.
114. Id. at 1124.
115. Id. at 1128, 1130-32.
list”), (ii) design a tool to circumvent those measures and access the list, (iii) analyze the list for accuracy and publish the results of his research, including the block list and (iv) distribute his circumvention tool so that others can use it to access the block list, since the list changes periodically.117

Edelman sought, inter alia, a declaration that his activities were protected under exemptions to § 1201. Alternatively, he claimed that § 1201 as applied to him is a content-based restriction on his research that violates the First Amendment. The court gave Edelman’s complaint short shrift. It concluded that the alleged injury was too speculative to meet the “case or controversy” requirement of Article III of the Constitution. The court observed that since it had “no inkling” of the exact dimensions of Edelman’s proposed research and no idea of the full content of what he proposed to publish, an advisory opinion would provide Edelman with little guidance.118

b. Fair Use

The Corley court rejected what it called defendants’ “extravagant” claim that § 1201 as applied by the district court unconstitutionally “eliminates” fair use.119 According to the Second Circuit, the Supreme Court has never said fair use is constitutionally required. The court declined to explore the extent to which fair use might have constitutional protection, saying that defendants did not claim to be making fair use and are not prevented from doing so by the injunction.120 The court concluded, however, that there is no authority to support a claim that the Copyright Act or the Constitution guarantees fair use by the optimal means or in the identical format as the original. It observed that the DMCA imposed no limitation on many traditional fair uses (e.g., commentary, quotation of excerpts), nor did it prevent someone from rerecording the movie with a camcorder, even though the resulting copy may not be as good. According to the court, “[f]air use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user’s preferred technique or in the format of the original.”121

The Elcom court was similarly unpersuaded by defendants’ claim that the DMCA eliminates fair use, observing that fair use is still available, though perhaps less convenient. According to the court, “quoting may have to occur the old-fashioned way, by hand or by re-typing, rather than by ‘cutting and pasting’ from existing digital media.” Like Corley, it rejected the argument that users have a right to “the most technically convenient way to engage in fair use.”122 It was also unreceptive to defendant’s argument that the DMCA grants rights in public domain

117. Id. at 138.
118. Id. at 139. In any event, it is doubtful that Edelman’s proposed circumvention of the access controls on N2H2’s block list would have violated § 1201(a)(1), as there was a relevant exemption pursuant to the rulemaking proceeding. See infra Part II.D.1.b.
120. Id. at 458-59.
121. Id. at 459.
works, observing that defendant’s “lock up” argument presupposes that the only available version is an electronic, technically protected one. The court rejected defendant’s proposed less onerous alternative, heightening penalties for infringement, as potentially less effective than outlawing circumvention tools.123

In response to defendant’s argument that the DMCA eliminates the right to make a copy of works in electronic media for personal noncommercial use, the Elcom court disputed the claim that the Ninth Circuit in Recording Industry Association of America v. Diamond Multimedia Systems, Inc.124 had recognized a fair use “right” to make a copy for personal use. The Elcom court suggested that making such copies could be deemed fair use but pointed out that “there is as yet no generally recognized right to make a copy of a protected work, regardless of its format, for personal noncommercial use” and no generally recognized First Amendment right to make backup copies. It ruled that precluding users from making backup copies, or “space shifting,” does not significantly impair their First Amendment rights so as to make the DMCA unconstitutionally overbroad.125

The court concluded that Congress had the authority to enact the DMCA under the Commerce Clause. Citing United States v. Moghadam,126 the court ruled that the Copyright Clause does not limit Congress’s ability to legislate pursuant to other grants of power, provided such legislation is not fundamentally inconsistent with the Copyright Clause.127 The Elcom case went to trial, but the defendant was ultimately acquitted, apparently because the jury found that its violation of the law was not willful.128

Finally, the court in 321 Studios relied on the reasoning in Corley and Elcom to conclude that the DMCA does not unconstitutionally burden fair use. According to the court: “Fair use is still permissible under the DMCA, although such copying will not be as easy, as exact, or as digitally manipulable as plaintiff desires.”129

**D. COPYRIGHT OFFICE PROCEEDINGS**

1. Section 1201(a) Rulemaking

The DMCA contains an administrative mechanism that empowers the Librarian of Congress to create additional exemptions from the ban on circumventing access controls. The Librarian’s decision is to be based on the recommendation of the

123. Id. at 1131-32.
124. 180 F.3d 1072 (9th Cir. 1999).
125. Elcom, 203 F. Supp. 2d at 1135.
126. 175 F.3d 1269, 1279-80 (11th Cir. 1999).
Register of Copyrights\(^\text{130}\) and made though a rulemaking proceeding. The Librarian is to exempt those particular classes of copyrighted works whose users are, or are likely to be, adversely affected in their ability to make non-infringing uses by the prohibition against circumventing technological access controls.\(^\text{131}\) Such an exemption is not permanent; a *de novo* determination must be made every three years so that the exemptions reflect changes in the marketplace for copyrighted materials. The exemptions are only from the ban on circumventing access controls; the Librarian has no authority to permit the creation or distribution of circumvention devices.

Section 1201(a)(1)(C) delineates factors that should guide the inquiry:
(i) The availability for use of copyrighted works;
(ii) The availability for use of works for nonprofit, archival, preservation, and educational purposes;
(iii) The impact that the prohibition on circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
(iv) The effect of circumvention of technological measures on the market for or value of copyrighted works; and
(v) Such other factors as the Librarian considers appropriate.

\(\textit{a. Congressional Guidance on the Rulemaking Procedure}\)

What guidance has Congress provided with respect to the rulemaking proceeding, in addition to the factors expressly included in the statute, cited above? According to the House Commerce Committee Report, the rulemaking proceeding should focus on "distinct, verifiable and measurable impacts; should not be based on *de minimis* impacts; and will solicit input to consider a broad range of evidence of past or likely impacts."\(^\text{132}\) According to the Report, the criteria in the statute should serve as guidelines for the types of questions the rulemaking proceeding should address; adverse impacts from other sources should not be considered. The Report stated that a class of works should be exempted only if there is sufficient evidence that adverse impacts have occurred or are likely to occur with regard to the class. According to the Report, the "particular class of copyrighted works" must be a "narrow and focused subset of the broad categories of works of authorship . . . identified in § 102 of the Copyright Act."\(^\text{133}\)

The House Manager's Report states that the main focus of the proceeding is "whether a substantial diminution of [the availability of works in the marketplace for non-infringing uses] is *actually occurring* in the market for particular classes of works."\(^\text{134}\) The rulemaking proceeding should also consider whether an adverse

---

130. The Register of Copyrights, in turn, is directed to consult with the Assistant Secretary for Communications and Information of the Department of Commerce. 17 U.S.C. § 1201(a)(1)(C).
131. *Id.*
133. *Id.* at 38.
134. HOUSE MANAGER'S REPORT, supra note 68, at 6.
impact is likely to occur over the next three-year period. However, with regard to perceived future harm, the Report explains that, in order to avoid undermining the prohibitions, "the determination should be based upon anticipated, rather than actual, adverse impacts only in extraordinary circumstances in which the evidence of likelihood of future adverse impact during that time period is highly specific, strong and persuasive." Adverse impact from other sources, questions of mere inconvenience and individual cases that do not rise to the level of "substantial adverse impact" must not be considered in making the determination.

The House Manager's Report also instructs the Secretary to consider the positive effects new technological protection measures have on the availability of copyrighted works in the rulemaking proceeding. For example, certain protection measures are essential in digital distribution strategies. Therefore, the positive effects of TPMs should be given weight in determining whether a measure adversely impacts non-infringing uses of a class of works. The availability of the work in alternative formats not subject to TPMs should also be considered. Regarding the scope of what constitutes a "particular class" of works, the Report explains that the § 102 categories are only a "starting point" that could be further refined as needed. However, the classes should not be defined too narrowly; for example, it would be inappropriate to subdivide the § 102 category "motion pictures and other audiovisual works" into "particular genres of motion pictures, such as Westerns, comedies, or live action dramas." According to the Report, any exemption will apply to the particular class of works, not to the measures that protect them. Therefore, a user could not circumvent a TPM that is used to protect a class of exempted works in order to access a different class of works that remains subject to the prohibition.

b. Initial Rulemaking Proceeding

In the initial rulemaking, the Librarian exempted two classes of works: "compilations consisting of lists of websites blocked by filtering software applications" and "literary works, including software and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence."

In the discussion accompanying the rule, the Copyright Office articulated certain principles that guided its determination. It concluded that the burden was on the proponent of an exemption to establish a "substantial adverse effect" on lawful use

---

135. id.

136. id.

137. id. at 7.

138. id.

139. The prohibition against circumventing access controls did not go into effect until two years after the DMCA became law, to provide time for the initial rulemaking proceeding. The rulemaking was published October 27, 2000, the day before the prohibition took effect.

of a particular class of works.\textsuperscript{141} It indicated that adverse effects that flow from factors other than the access control circumvention prohibition should not be considered in determining exemptions. The availability of works in other unprotected formats was relevant, however, in determining whether users were adversely affected by technological access controls.

The discussion considered at length how the term “class of works” should be defined. It ultimately rejected suggestions that a class could be defined with reference to particular users or the uses to which the works were put. It concluded that the statutory language and legislative history required it to define “class of works” based on attributes of the works themselves.\textsuperscript{142}

The Copyright Office explained in some detail the reasons for the exemptions. Parents, schools and libraries use filtering software programs to restrict children’s access to explicit or inappropriate websites. However, such programs allegedly have a high error rate and erroneously block sites that do not contain offensive material. Particularly in a library context, their use may implicate patrons’ First Amendment rights. Proponents of the exemption argued that they should be able to circumvent technological controls to get access to the list of blocked sites compiled within the program. Evidence showed that persons had already decrypted the lists for the purposes of criticism and commentary prior to the effective date of § 1201(a)(1). Without an exemption, decrypting the lists would violate the new law. After determining that there was no other way to obtain the lists of blocked sites, the Librarian exempted this class of works.

The second exempted class comprises literary works, software and databases that are protected by malfunctioning, damaged or obsolete access controls; these faulty controls potentially deny authorized users access to works.\textsuperscript{143} The Librarian concluded that even with the exemption, copyright owners’ interests would be adequately protected since the user has already compensated the copyright owner for access to the work. Moreover, since circumvention can be time-consuming, users are unlikely to take that route unless the copyright owner is unwilling or unable to assist them. If an exemption were not allowed, legitimate users might be required either to purchase the work again or lose access entirely. In exempting this class, the Librarian noted that the exemption likely reached the “outer limits” of the term “class of works” as described by Congress, for the class is defined in part by the particular access controls applied. If it were shown in the next rulemaking procedure that all types of works suffered from malfunctioning, damaged or obsolete access controls, the exemption might be beyond the

\textsuperscript{141} The Office noted that some commentators suggested that the House Manager’s Report—which used the term “substantial adverse impact”—was entitled to little deference as legislative history as it is not a Congressional committee report. However, the Office found that the House Manager’s report was consistent with the House Commerce Committee Report on this point, and relied on both. \textit{Id.} at 64558.

\textsuperscript{142} \textit{Id.} at 64559-61.

\textsuperscript{143} Due to issues of proof, this exemption does not apply to problems that occur when “dongles” (hardware locks attached to a computer that interact with software programs to prevent unauthorized access to that software) are lost or stolen.
Librarian's authority. Therefore, the Register and Librarian recommended that Congress consider amending § 1201 to provide a statutory exemption for all works that suffer from faulty protection measures.\textsuperscript{144}

The Register considered, but ultimately did not recommend, exempting ten additional classes of works.\textsuperscript{145} As a general matter, the proposed exemptions were rejected either because the proposed class could not be properly characterized as a "class of works," or there was insufficient evidence of the adverse effects of the prohibition on non-infringing uses (or both).\textsuperscript{146} In some cases, the Librarian indicated willingness to provide an exemption for appropriately defined classes if provided with evidence that access controls significantly restrict legitimate uses. In other cases, however, the Office indicated that the exemptions sought were beyond its mandate and that proponents would have to seek their proposed exemptions through legislation.\textsuperscript{147}

In two particular instances the Copyright Office seemed to welcome possible Congressional intervention: first, to create a statutory exemption to circumvent malfunctioning and obsolete access controls for all categories of works, discussed above; and second, to clarify the law regarding circumvention when access and use controls are combined, an issue raised in connection with DVDs.\textsuperscript{148}

\textit{c. Second Rulemaking Proceeding}

In its second rulemaking proceeding, the Librarian of Congress, on the recommendation of the Copyright Office, created exemptions for four classes of works:\textsuperscript{149}

1. Compilations consisting of lists of internet locations blocked by commercially marketed filtering software applications that are intended to prevent access to domains, websites or portions of websites, but not including lists of internet locations

\begin{itemize}
\item \textsuperscript{144} 65 Fed. Reg. at 64565.
\item \textsuperscript{145} These were: (1) "thin copyright" works; (2) "sole source" works; (3) audiovisual works on DVDs; (4) videogames in formats playable only on dedicated platforms; (5) computer programs and other digital works for purposes of reverse engineering; (6) encryption research purposes; (7) "fair use" works; (8) material that cannot be archived or preserved; (9) works embodied in copies lawfully acquired by users who seek to make non-infringing uses thereof; and (10) an exemption for public broadcasting entities. \textit{Id.} at 64566-74.
\item \textsuperscript{146} The discussion also noted that many complaints raised in the rulemaking actually related to licensing practices, rather than grievances with technological protection measures that control access to works. While licensing practices are relevant to the inquiry, a showing that such practices substantially and adversely affected non-infringing uses was not made. \textit{Id.} at 64563.
\item \textsuperscript{147} In the case of proposed exemptions for reverse engineering and encryption research, the Office also cited the exemptions already in §§ 1201(f) and 1201(g) of the statute. \textit{See id.} at 64570-71.
\item \textsuperscript{148} \textit{Id.} at 64568.
blocked by software applications that operate exclusively to protect against damage to a computer or computer network or of internet locations blocked by software applications that operate exclusively to prevent receipt of email. For purposes of this exemption, "internet locations" are defined to include "domains, uniform resource locators (URLs), numeric IP addresses or any combination thereof.

Although similar to the previous exemption for filtering software programs, the new exemption substitutes "internet locations"—which includes URLs, IP addresses and domains—for the narrower "websites," in order to include filtering programs or "net nannies" with different blocking systems. The Office also substituted "commercially marketed filtering software" for "filtering" to avoid touching upon spam, firewalls and other types of filters. The opponents to the exemption argued that other sources of the lists are available, including the querying of the programs' databases. The Office found that the limited nature of these queries "foreclosed comprehensive or meaningful results."  

2. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete.

As a result of the first rulemaking proceeding, the Copyright Office had granted an exemption for literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence. The only testimony the Office received in the second rulemaking related to problems that continue to arise with dongles, or hardware locks, so the Office limited its recommended exemption accordingly. The Office clarified that the exemption applies only to dongles which are actually malfunctioning and not to those that may malfunction in the future. As long as the dongle continues to provide access to the work, the exemption is not applicable.

3. Computer programs and video games distributed in formats that have become obsolete and which require the original media or hardware as a condition of access. For purposes of this exemption, "formats that have become obsolete" may refer to particular media or operating systems and shall have the same meaning as in 17 U.S.C. § 108(c): a format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.

The Internet Archive, a nonprofit archive of works in digital formats, proposed a broader formulation of this exemption to assist the migration of works from obsolete, degrading formats to modern hard drives. Some of the protection mechanisms on formats such as floppy disks and CD-ROMs allowed copies to be made but prevent them from functioning unless the original media is in the computer's disk drive.

The Office was persuaded of the merits of this exemption to facilitate

150. 68 Fed. Reg. at 62013.
151. Recommendation of the Register of Copyrights, supra note 149, at 27.
preservation but limited the Internet Archive's formulation in several respects. It restricted the exemption to computer programs and videogames, because the evidence did not support extending the exemption to literary and audiovisual works.\textsuperscript{153} Also, it was concerned a class as broad as the one proposed by the Internet Archive would come "dangerously close" to a use-based exemption for preservation activity, which is beyond the rulemaking authority.\textsuperscript{154}

The Office clarified that the exemption does not apply to formats that are becoming obsolete, but only to those that have already become so. It concluded that § 108(c), which authorizes preservation activities by libraries and archives, did not provide a basis for making preservation copies of works whose formats had not yet become obsolete, and that systematic migration of works to modern storage formats does not fall within the privilege in § 117 to make archival copies in case of software malfunction, nor is it likely to be deemed fair use.\textsuperscript{155}

4. Literary works distributed in e-book format when all existing e-book editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the e-book's read-aloud function and that prevent the enabling of screen readers to render the text into a "specialized format." For purposes of this exemption, "specialized format," "digital text" and "authorized entities" shall have the same meaning as in 17 U.S.C. § 121.

This exemption was sought by the American Foundation for the Blind (AFB) and several library associations. Read-aloud functions on e-books permit the blind and visually impaired to access works that would be otherwise unavailable to them. However, many copyright owners employ digital rights management (DRM) to disable this feature.\textsuperscript{156}

The Office found that a blind person's use of a read-aloud function is a non-infringing use, and determined that an exemption was warranted. Acknowledging that a "particular class of works" could not be defined according to its users, it nevertheless tried to tailor the exemption to the group of users it aimed to benefit. It therefore created the exemption around literary works distributed in e-book format where all versions have disabled the read-aloud function. If there is a version on the market with the read-aloud function, the exemption would not apply, nor would it apply if the work is made available pursuant to 17 U.S.C. § 121.\textsuperscript{157}

The Copyright Office considered, and rejected, numerous other proposed exemptions. These include, for example, exemptions for all works for non-infringing uses; for "fair use works," for "thin copyright works," for works to which the user had initial lawful access; for public domain works; for musical works whose access controls make them inaccessible due to malfunction, damage or obsolescence; for various categories of works designed for use on specific platforms; and for reverse engineering for interoperability. There were many

\textsuperscript{153} Recommendation of the Register of Copyrights, supra note 149, at 49.
\textsuperscript{154} Id. at 46.
\textsuperscript{155} Id. at 52-59.
\textsuperscript{156} 68 Fed. Reg. at 62014.
\textsuperscript{157} Id.
requested exemptions with respect to circumventing access controls protecting movies on DVDs, including for all audiovisual works protected by access controls that interfere with the ability to skip promotional materials; all audiovisual works on DVDs not available in this geographic region; audiovisual works on DVDs encrypted by CSS, and so on.\textsuperscript{158} This is by no means an exhaustive list of the proposed exemptions but is merely intended to convey their breadth and scope.

Most of the proposed exemptions were rejected because (1) they were too broad to qualify as a permissible “class” of works, (2) they constituted impermissible use-based exemptions, (3) there was insufficient evidence of present or likely adverse effects on non-infringing uses of the proposed class of works, and/or (4) there was an existing statutory exemption relevant to the proposed class of works. The Copyright Office’s recommendations—in particular, its reasons for rejecting exemptions for certain proposed categories of works—are discussed in greater detail in Part VI.

2. Study Concerning Encryption Research and Technology

Under § 1201(g)(5), the Register of Copyrights and the Assistant Secretary for Communications and Information of the U.S. Department of Commerce were required to report jointly to Congress one year after the DMCA went into effect on the effect of § 1201 on encryption research and encryption measures.\textsuperscript{159} That report concluded that as of that time, there was no discernable impact on encryption research or encryption technology and that any legislative recommendations in connection with § 1201(g) would be premature.

3. Study Under Section 104 of the DMCA

This provision directed the Register of Copyrights and the Assistant Secretary for Communications and Information of the U.S. Department of Commerce to evaluate the effect of the DMCA and new technologies on the operation of § 109 (first sale doctrine) and § 117 (re copying of computer programs). The report, entitled “DMCA Section 104 Report,”\textsuperscript{160} was released in August 2001. The Copyright Office declined to recommend changing § 109 to permit digital transmission of copies, on the grounds that (i) there was no convincing evidence of current problems; (ii) to avoid electronic transmission resulting in two copies, there must be voluntary deletion of the first copy by the sender or automatic deletion by technological means, both of which are unavailable at this time; and (iii) digital transmission has a greater effect on the market for copies than does transfer of

\textsuperscript{158} \textit{Id.} at 62014-18.

\textsuperscript{159} U.S. Copyright Office, \textit{Joint Study of Section 1201(g) of the Digital Millennium Copyright Act, at} \url{http://www.copyright.gov/reports/studies/dmca_report.html}.

physical copies.\textsuperscript{161}

With regard to a possible modification of § 117, the Office recommended against adopting a general exemption from the reproduction right for all temporary copies incidental to lawful uses. It also recommended against expanding the archival exemption in § 117(a)(2), despite the mismatch between the exemption and common archival practices, which involve backing up a computer's hard drive on a regular basis. In its view, such practices are likely fair use. However, it suggested changing the law to eliminate a possible claim that those copies may be transferred pursuant to § 109.\textsuperscript{162}

Finally, the Office concluded that the DMCA had not had a significant negative effect on the operation of either § 109 or § 117. It saw a potential for a negative effect on § 117 but concluded that the impact currently was minimal, since end user licenses generally regulate permissible copying of software and distribution on CD-ROMs reduces the need for backup copies. It also saw a potential for a negative effect on the operation of § 109 in the context of works "tethered" to a particular hardware device. However, it concluded that since the practice was not widespread, and DRMs and DRM use still in the early stages of development, it was premature to recommend legislation.\textsuperscript{163}

\section*{E. Proposed Legislation and Regulations}

Three bills have been introduced in the 108th Congress to amend anti-circumvention law. The first bill, H.R. 107,\textsuperscript{164} is entitled "Digital Media Consumers' Rights Act of 2003." Under the heading "Fair Use Restoration," it contains a broad exemption to allow circumvention of a technological measure "in connection with the access to, or the use of, a work if such circumvention does not result in an infringement of the copyright in the work." It would also amend the anti-trafficking provisions of §§ 1201(a)(2) and 1201(b) to allow manufacture, distribution or making non-infringing use of a hardware or software product "capable of enabling significant non-infringing use of a copyrighted work." H.R. 107 would further permit trafficking in circumvention devices if the person "is acting solely in furtherance of scientific research into technological protection measures."

The balance of H.R. 107 focuses on alleged mislabeling of copy-protected media, setting out strict requirements for how copy-protected music discs must be labeled. It provides that selling or advertising copy-protected discs without the requisite warnings will constitute an unfair and deceptive trade practice. The bill would give the Federal Trade Commission the authority to develop rules to enforce these disclosure and labeling requirements, and also to establish labeling requirements for DVD audio discs and Super Audio CDs.

\begin{itemize}
\item \textsuperscript{161} \textit{Id.} at xx-xxi, 81-85.
\item \textsuperscript{162} \textit{Id.} at xxiii, xxviii-xxxi.
\item \textsuperscript{163} \textit{Id.} at xvi-xvii.
\end{itemize}
The second bill, H.R. 1066,\(^{165}\) is entitled “Benefit Authors without Limiting Advancement of Net Consumer Expectations Act of 2003,” or the “BALANCE Act.” Section 5 (“Permissible Circumvention to Enable Fair Use and Consumer Expectations”) would allow circumvention of access or rights control measures on lawfully obtained copies of a work, if such act is necessary to make non-infringing use of a work, and the copyright owner fails to make publicly available the necessary means to make non-infringing use without additional cost or burden to the user. The bill also provides that it would not be an infringement to manufacture, distribute or otherwise traffic in technological means to circumvent access controls or rights controls if such means are necessary to make a non-infringing use, and the copyright owner fails to make available the necessary means to make such use without additional cost or burden to the user. H.R. 1066 would also broaden exemptions to copyright and, as a consequence of its amendment of § 1201, the circumstances under which circumvention would be permitted.\(^{166}\)

S. 1621, the “Consumers, Schools and Libraries Digital Rights Management Awareness Act,”\(^{167}\) would, among other things, create a broad “digital first sale” privilege: it would grant owners of digital media products the right to dispose of their copy or transmission, provided the original is deleted. “Digital media products” include copies of copyrighted works distributed to the public in digital form, either electronically or fixed in a physical medium. The bill prohibits use of access controls that limit consumers’ ability to transfer digital media products through transmission, donation or resale.\(^{168}\)

The Federal Communications Commission (FCC) recently issued a ruling requiring digital television sets manufactured on or after July 1, 2005 to implement a technological protection measure for digital broadcast television, known as the “broadcast flag.”\(^{169}\) The broadcast flag technology will allow content owners to insert a data signal in the broadcast stream which would cause receivers to respond to restrict copying and redistribution of digital broadcast programs by consumers.

---


166. For example, § 3 of the BALANCE Act provides that it is not an infringement for someone who lawfully obtains a copy or transmission of a digital work to make archival copies or to perform or display the work or an adaptation thereof on a “digital media device” provided such performance or display is not public. It also contains a provision making unenforceable any “nonnegotiable license terms” to the extent they restrict or limit any of the limitations or exclusive rights under Title 17. Section 4 of the Act contains a “digital first sale” doctrine.


168. Id. at § 6. The bill also attempts to limit the FCC’s ability to mandate TPMs. Id. at § 3.

III. LEGISLATION IN OTHER COUNTRIES

A. EUROPEAN UNION

In 2001, the European Union (EU) adopted Directive 2001/29/EC of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights in the information society. Among other things, this directive mandates how the WIPO treaties are to be implemented in the laws of the EU member states. The EU member states are in the process of implementing the directive. It should be noted that in some respects, particularly regarding exceptions to copyright protection, the directive permits variations among the member states (and some variation in the course of the legislative process is inevitable).

1. Prohibition Against Circumventing a Technological Protection Measure

Member states are required to provide “adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.”

Technological measures include “any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts in respect of works or other subject-matter, which are not authorized by the rightholder . . . .” Such measures are deemed “effective” where “use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.”

2. Prohibition Against Trafficking in Circumvention Devices and Services

Member states are required to provide “adequate legal protection against the

171. Id. at art. 6(1). EU Directive 98/94/EC on the Legal Protection of Services Based on, or Consisting of, Conditional Access, 1998 O.J. (L320), has its own anti-circumvention provision in article 4 (prohibiting the distribution, installation, or commercial promotion of illicit reception devices). So too does EU Directive 91/250/EEC on the Legal Protection of Computer Programs. Art. 7(1)(c) 1991 O.J. (L122), (prohibiting distribution or possession of devices whose sole intended purpose is to circumvent technological protection measures on a computer program).
172. Unlike U.S. law, which applies only to copyrighted works, the EU directive also applies to works covered by related or “neighboring” rights (some but not all of which are covered by copyright in the United States) and database rights.
173. Council Directive 2001/29/EC, supra note 170, art. 6(3). The EU Directive defines a TPM as “effective” when use of a protected work is “controlled by the rightholders . . . .” The WIPO Copyright Treaty, discussed supra Part I.A, requires protection for technological measures “used by authors.” U.S. law does not restrict protection to measures used by copyright owners. Query whether the WIPO Treaty or the EU Directive require protection of TPMs applied by a party distributing a copyrighted work pursuant to a nonexclusive license from the copyright owner.
manufacture, import, distribution, sale, rental, advertisement for sale or rental, or
possession for commercial purposes of devices, products or components or the
provision of services":

- that are “promoted, advertised or marketed for the purpose of circumvention”;
- that “have only a limited commercially significant purpose or use other than
to circumvent”; or
- that are “primarily designed, produced, adapted or performed for the purpose
of enabling or facilitating the circumvention of, any effective technological
measures.174

3. Exemptions

The directive contains no specific privilege to circumvent technological
protection measures or to deal in circumvention devices. However, it requires
member states, “in the absence of voluntary measures taken by rightholders,
including agreements between rightholders and other parties concerned,” to take
appropriate measures to ensure that rightholders make available to beneficiaries of
certain exemptions or limitations the means of taking advantage of them (provided
the beneficiary has legal access).175

The exemptions and limitations to which this mandate applies include:176

- Art. 5(2)(a) (reproductions on paper or similar medium by
photographic or other technique with similar results, with fair
compensation);
- Art. 5(2)(c) (“specific acts of reproduction” by libraries, museums,
educational establishments and archives, not for direct or indirect
economic or commercial advantage; compensation not required by the
directive);
- Art. 5(2)(d) (ephemeral recordings by broadcasting organizations;
compensation not required by the directive);
- Art. 5(2)(e) (reproductions of broadcasts by social institutions such as
hospitals and prisons for noncommercial purposes, with fair
compensation);
- Art. 5(3)(a) (illustration for teaching or scientific research;
compensation not required by the directive);
- Art. 5(3)(b) (noncommercial uses for people with disabilities;
compensation not required by the directive);
- Art. 5(3)(c) (public security, proper performance of administrative,
parliamentary or judicial proceedings; compensation not required by
the directive).

174. Id. at art. 6(2).
175. Id. at art. 6(4), para. 1.
176. Member states may include in their laws the exemptions in Articles 5(2) and 5(3), but are not
required to do so. Accordingly, a member state’s responsibility for ensuring that technological measures
do not defeat rightholders’ ability to benefit from exemptions applies to these exemptions to the extent
they are included in that member state’s laws.
Some member states have "private use" privileges in their laws that permit users to make reproductions of copyrighted works for private, noncommercial purposes. The directive permits this exemption with respect to reproduction in any medium, provided the rightholder receives "fair compensation." Article 6(4) permits (but does not require) member states to take measures in respect of beneficiaries of this privilege "unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exemption or limitation..." The measures to support the "private use" privilege are subject to the "fair compensation" required by Article 5(2)(b) and the requirement of Article 5(5) that exemptions be limited to "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." Moreover, member states may not "prevent[] rightholders from adopting adequate measures regarding the number of reproductions..." 

The directive further provides that the first and second subparagraphs of Article 6(4) (discussed above) "shall not apply to works or other subject matter 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 a time individually chosen by them." Thus, "pay-per-view" type services protected by technological measures are not subject to the requirement that rightholders make available the means of benefitting from copyright exemptions and limitations.

The recitals indicate certain additional exemptions. Recital 48 of the directive states: "In particular, this protection [in respect of technological measures] should not hinder research into cryptography." Recital 50 makes clear that the legal protection of technological protection measures does not apply with respect to computer programs, which are dealt with separately in Directive 91/250/EEC. Finally, Recital 51 provides: "The legal protection of technological measures applies without prejudice to public policy, as reflected in Article 5, or public security."

4. Responsibility of Equipment Manufacturers

Recital 48 states that the legal protection of technological protection measures "implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6."

5. Obligations of Rightholders

See Part III.A.3. above. Rightholders who use technological protection measures can either conclude voluntary agreements concerning the manner in

178. Id. at art. 6(4), para. 2.
179. Id. at art. 6(4), para. 4.
which the means of benefiting from exemptions or limitations will be made available to users with valid access, or member states will obligate them to make such means available.

6. Ongoing Monitoring

Forty-two months after the directive enters into force, and every three years thereafter, the Commission is to report to the European Parliament, the Council and the Economic and Social Council on the application of the directive, and in particular on articles 5, 6 and 8 “in the light of the development of the digital market.” The Commission is further directed to examine in particular whether article 6 provides sufficient protection and whether acts permitted by law are being adversely affected by technological protections.\(^{180}\)

The directive establishes a “contact committee” composed of representatives of the member states, inter alia, to examine the impact of the directive and to “act as a forum for the assessment of the digital market in works and other items, including private copying and the use of technological measures.”\(^{181}\)

B. Australia

Australia passed the Copyright Amendment (Digital Agenda) Act 2000 to amend the Copyright Act of 1968. Among other things, the new law implemented WIPO treaty obligations. It went into effect March 4, 2001.

1. Prohibition Against Circumventing a Technological Protection Measure

There is no prohibition against the act of circumventing.

2. Prohibition Against Trafficking in Circumvention Devices and Services

Under the new law, it is illegal to make, sell, let for hire, advertise, market, distribute for purposes of trade or exhibit circumvention devices, or to import them for these purposes, or to make them available online in a way that will prejudicially affect the rightholder, or to provide, advertise or market a circumvention service, if the person so doing knows or should know that the device or service will be used to facilitate circumvention.\(^{182}\)

A circumvention device is defined as “a device (including a computer program) having only a limited commercially significant purpose or use, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of an effective technological protection measure.”\(^{183}\) Circumvention services are similarly defined.

\(^{180}\) Id. at art. 12(1).

\(^{181}\) Id. at art. 12(3), (4).

\(^{182}\) Copyright Amendment (Digital Agenda) Act 2000, § 116A(1) 2000, (Austl.).

\(^{183}\) Id. at § 10(1).
A "technological protection measure" is defined as a device, product or component that is designed "in the ordinary course of its operation, to prevent or inhibit the infringement of copyright . . ." either (a) "by ensuring that access to the work or other subject-matter is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter)" with the authority of the rightholder or (b) "through a copy control mechanism." 184

3. Exemptions

- There is an exemption for acts lawfully done for law enforcement or national security purposes by the Commonwealth, a state or territory, or an authority of any of the foregoing. 185
- There is an exemption from the prohibition on selling or distributing circumvention devices or making them available online if three conditions are met:
  (i) the circumvention device must be supplied for use for a "permitted purpose"
  (ii) the person to whom the circumvention device is supplied must be a "qualified person" under the statute; and
  (iii) the qualified person receiving the circumvention device must supply a signed declaration that includes the name and address of the supplier; the name and address of the recipient of the device, and the basis on which the recipient is a "qualified person"; a statement that the device will be used only for a permitted purpose and identification of that purpose, with specific reference to the statutory section; and a statement that the copyright material is not readily available in a form that is not protected by a technological protection measure. 186

This exemption also applies with respect to providing circumvention services.

  - A "permitted purpose" is a use that implicates a proprietary right and falls within one of a specified group of statutory exemptions to copyright infringement, 187 including reproduction of computer programs to make interoperable products, correct errors and for security testing; 188 copying by Parliamentary libraries for members of Parliament; 189 certain lawful copying by libraries and archives for users, for other libraries and archives or for preservation; 190 use of copyrighted material for use by the

184. Id.
185. Id. at § 116A(2).
186. Id. at § 116A(3).
187. Id. at § 116A(7).
188. Id. at §§ 47D-F.
189. Id. at § 48A.
190. Id. at §§ 49, 50, 51A.
Commonwealth or a state;\textsuperscript{191} and certain permitted copying by educational institutions.\textsuperscript{192}

- A "qualified person" is someone authorized to copy the material for purposes of one of the statutory exemptions.\textsuperscript{193}

- It is a criminal offense to make a false declaration in connection with a circumvention device or service knowing it to be false, or in reckless disregard of whether it is false or misleading.\textsuperscript{194}

- There is an exemption from the prohibition on making or importing circumvention devices where it is established:

(i) that the device was made or imported for use for a permitted purpose and the copyright material is not readily available in a form that is not protected by a technological protection measure; or

(ii) that the device is made or imported to enable a person to supply the device for use only for a permitted purpose.\textsuperscript{195}

4. Responsibility of Equipment Manufacturers

None. See Part III.B.2, above.

5. Obligations of Rightholders

See Part III.B.3, above.

6. Ongoing Monitoring

None explicitly set forth in the statute.

C. JAPAN

Japan implemented the WIPO treaties in 1999 through amendment of its Copyright Law. The provisions comprise article 120bis of the Copyright Law (JCL) and provide for criminal imprisonment and fines. Article 120bis addresses trafficking in circumvention devices/programs and the act of circumventing as a business.\textsuperscript{196}

\begin{itemize}
\item[191.] \textit{Id.} at § 183.
\item[192.] \textit{Id.} at pt. V.B.
\item[193.] Digital Agenda Act, at § 116A(8).
\item[194.] \textit{Id.} at § 203G.
\item[195.] \textit{Id.} at § 116A(4).
\item[196.] Japan’s Copyright Law, JCL Article 120bis, provides:
The following shall be punishable by imprisonment for a term not exceeding one year or a fine not exceeding one million Yen;

(i) any person who transfers to the public the ownership of, or lends to the public, manufactures, imports or possesses for transfer of ownership or lending to the public, or offers for the use by the public, a device having a principal function for the circumvention of technological protection measures (such a device includes such a set of parts of a device}
In addition to the criminal sanctions in the amended Copyright Law, sales and related activities for devices and programs that circumvent technological measures to control use or copying of contents are classified as "unfair competition" under the Unfair Competition Prevention Law (sometimes translated Unfair Competition Law or Japan Anti-Unfair Competition Law (JAUCL)).

The Copyright Law and the Unfair Competition Prevention Law overlap to some extent in their prohibitions. The Copyright Law frames its prohibitions in terms of circumventing technological protection measures. It prohibits providing to the public a means for circumventing. It also prohibits the act of circumvention when done as a business. 197 The Copyright Law defines technological protection measures as "measures to prevent or deter such acts as constitute infringements on moral rights of authors or copyright mentioned in Article 17, paragraph (1) or moral rights of performers mentioned in Article 89, paragraph (1) or neighboring rights mentioned in Article 89, paragraph (6)." 198

On its face, the JCL's definition of technological protection measures is somewhat vague as to whether the JCL can reach an access control protection. However, a report by Japan's Office of Multimedia Copyright claims, "measures that restrict the viewing or listening of a work such as by scrambling (encrypting) a broadcast (so-called access control), do not qualify as technological measures because simple viewing or listening is not an act covered by copyright." 199 Also, the concept of technological protection measures under Copyright Law is technology-neutral under JCL Article 2 (xx).

---

197. JCL art. 120bis(iii).
198. JCL art. 2 (xx) provides:
"Technological protection measures" means measures to prevent or deter such acts as constitute infringements on moral rights of authors or copyright mentioned in Article 17, paragraph (1) or moral rights of performers mentioned in Articles 89, paragraph (1) or neighboring rights mentioned in Article 89, paragraph (6) (hereinafter in this item referred to as "copyright, etc.") ("deter" means to deter such acts as constitute infringements on copyright, etc. by causing considerable obstruction to the results of such acts; the same shall apply in Article 30, paragraph (1), item (ii)) by electronic or magnetic means or by other means not perceivable by human perception (in the next item referred to as "electro-magnetic means"), excluding such measures as used not at the will of the owner of copyright, etc., which adopt systems of recording in a memory or transmitting such signals as having specific effects on machines used for the exploitation of works, performances, phonograms, broadcasts or wire diffusions (in the next item referred to as "works, etc.") ("exploitation" includes acts which would constitute infringements on moral rights of authors or performers if done without the consent of the author or the performer), together with works, performances, phonograms, or sounds or images of broadcasts or wire diffusions.


The Unfair Competition Prevention Law frames its prohibitions in terms of sales and related activities for devices, media, and programs that circumvent "technical restriction" means to control use or copying of certain contents. The Unfair Competition Law specifically addresses both use controls, and access controls. The JAUCIL defines technical restriction means in terms of protecting the playing, execution, converting, or recording of audio or video content or programs. The technical restriction means must be used commercially and must work by electromagnetic method. Thus, the JAUCIL is neither media-neutral with respect to works protected, nor technology-neutral with respect to restriction means protected.

The following table summarizes the basic functions and applications of the two laws:

---

200. Japan's Unfair Competition Prevention Law [hereinafter JAUCIL], art. 2(1)(x), provides: The act of assigning, delivering, displaying for the purpose of assigning or delivering, exporting or importing devices that only have a function to enable people to play vision or audio, to execute of programs, or to record of vision, audio or programs that are restricted by the technical restriction means commercially used (excluding those used by other people for preventing others than specific people from playing vision and audio or executing programs, or recording vision, audio or programs) (including those incorporating such devices), or recording media or memory devices that record a program that only has the above function (including those combined with other programs) or the act of providing such program through electric telecommunication circuit.


201. JAUCIL, art. 2 (1)(xi) provides: The act of other people of assigning, delivering, displaying for the purpose of assigning or delivering, exporting or importing devices, in order to prevent others than specific people from playing vision and audio or executing programs, or recording vision, audio or programs, to others than such specific people, that only have a function to enable people to play vision or audio, to execute of programs, or to record of vision, audio or programs that are restricted by means of technical restriction means commercially used (including those incorporating such devices), or recording media or memory devices that record a program that only has the above function (including those combined with other programs) or the act of providing such program through electric telecommunication circuit.

Outline and Practices of Japanese Unfair Competition Prevention Law, supra note 200, at 23 (English translation).

202. JAUCIL, art. 2(5) provides: "Technical restriction means" is a means for restricting playing of vision or audio or executing of programs, or recording thereof, by electromagnetic method, that is, a method of recording or transmitting signals to which playing devices specifically respond, together with vision, audio or programs, or a method of recording or transmitting in recording media by converting vision, audio or programs to those of which playing devices need to be specifically converted.

<table>
<thead>
<tr>
<th>Sanctions:</th>
<th>Copyright Law</th>
<th>Unfair Competition Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Fine</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Criminal Imprisonment</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Civil Remedies</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

| Prohibited Activities: | | |
|-------------------------|--------------------------|
| Sales and Related Activity | X                         |
| Giving or Offering to Public | X                         |
| Act of Circumventing as a Business | X                  |

| Protected Measures: | | |
|---------------------|--------------------------|
| Access Control      | X                         |
| Use Control         | X                         |
| Technological Protection Measures | X                   |
| Technical Restriction Means | X                   |

| Technology: | | |
|-------------|--------------------------|
| Technology-Neutral | X                       |
| Electromagnetic Method | X                     |

| Media Covered: | | |
|----------------|--------------------------|
| Media-Neutral | X                         |
| Media-Specific | X                     |

| Purpose Test Used: | | |
|-------------------|--------------------------|
| Principal Function | X                         |
| Sole Function | X                         |

Finally, separate from the adoption of the WIPO treaties, if general tort principles were met, a person might be liable in a general tort for having engaged in

---

203. Demand for cessation, possible disposal and destruction of illegally produced goods and of tools and implements used in the illegal activity. JAUC, arts. 3(1) & (2).

204. This test may not be as restrictive as it initially appears. Japanese government commentators have clarified that the purpose test will be met if the device (or media or program) has no other function than circumventing technological protection measures in view of economics and commerce. Outline and Practices of Japanese Unfair Competition Prevention Law, supra note 200, at 22, available at http://www.apic.jiii.or.jp/facility/text/2-10.pdf. See also Japan ALAI Questionnaire Response of the Japan National Group to Questionnaires J.C., I.D.1 & I.D.2, ADJUNCTS AND ALTERNATIVES TO COPYRIGHT: PROCEEDINGS OF THE ALAI CONGRESS JUNE 13-17 2001 (2002) (prepared by Mr. Kentaro Endo and Prof. Hiroshi Saito), available at http://www.alai-usa.org/2001_conference/Reports/ Japan_jiab_en.doc. [hereinafter Japan ALAI Questionnaire Response]. Question 2.8 of questionnaire I.D.2: “Liability depends on whether a device has a ‘principal’ function for the circumvention of technological protections measures . . . .” The test may in fact be treated somewhat similarly to the first two prongs of the DMCA test: “primarily designed or produced for the purpose of circumventing,” “only limited commercially significant purpose or use other than to circumvent.” 17 U.S.C. § 1201(a)(2)(A) & (B); § 1201(b)(1)(A) & (B).
an act of circumvention or for having manufactured, distributed or furnished the means for a circumvention device. So, to summarize Japanese law on this issue:

1. Prohibition Against Circumventing a Technological Protection Measure

There is a prohibition against circumvention done commercially. The JCL provides criminal sanctions for "any person who, as a business, circumvents technological protection measures in response to a request from the public." There is no prohibition against noncommercial circumvention per se in the JCL. The JAUCCL does not prohibit circumventing a technological protection measure (nor a "technical restriction means").

2. Prohibition Against Trafficking in Circumvention Devices and Services

JCL article 120bis(i) provides criminal sanctions for trafficking in "a device having a principal function for the circumvention of technological protection measures... or copies of a program having a principal function for circumvention of technological protection measures." The article further provides that such a device "includes such a set of parts of a device as can be easily assembled."

The word trafficking (or the Japanese equivalent) is not used in the article. Instead, the article provides sanctions for "any person who transfers to the public the ownership of, or lends to the public, manufactures, imports or possesses for transfer of ownership or lending to the public, or offers for the use by the public, a device... or copies of a program having a principal function for circumvention of technological protection measures." The article apparently does not require that the activities of transfer be done for commercial purposes.

In addition, the act of assigning, delivering or displaying for the purpose of assigning or delivering, exporting or importing devices, media, or programs that circumvent technical restriction means is defined as unfair competition under JAUCCL. The law specifies restriction means for both use and access control.

3. Exemptions

There are no exemptions in the JCL. Note, however, that the act of circumventing is prohibited only when done "as a business" in response to a request from the public. The JAUCCL exempts circumvention for the purpose of testing and researching encryption systems.

---

205. See generally, Japan ALAI Questionnaire Response, supra note 204 at 1.C. Japan also has an Unauthorized Computer Access Law, which prohibits unauthorized computer access, but it is not directed at accessing a copyrighted work. Id.
206. JCL, art. 120bis(i).
207. JAUCCL, art. 2(1)(x) & (xi).
208. JCL, art. 120bis(ii).
209. JAUCCL, art. 11(1)(vii).
4. Responsibility of Equipment Manufacturers

Equipment manufacturers are not obligated in any way.

5. Obligations of Rightholders

Apparently, rightholders have no obligations.

6. Ongoing Monitoring

Apparently, there is no mandatory ongoing monitoring.

IV. LEGAL PROVISIONS THAT PROHIBIT CIRCUMVENTION OF PROTECTIVE MEASURES IN OTHER CONTEXTS

A. INTRODUCTION

The DMCA uses two basic methods to maintain the integrity of technological protection measures. First, it prohibits the circumvention of any technological protection measure that effectively controls access to a protected work. Second, the DMCA makes it illegal to manufacture or distribute any device that is primarily used to circumvent a technological measure that effectively controls access to or protects rights in a work.

The DMCA’s approach has met with some controversy. Although there was no legal prohibition on the conduct of circumvention per se before the Act, proponents of the anti-circumvention approach have sought to validate this method by identifying analogous provisions in domestic and international law that employ a similar approach. In response, opponents of the anti-circumvention approach argue that these alleged “analogous provisions” are in fact quite different from the broad prohibitions of the DMCA.210

As part of our study, we sought to identify domestic provisions that are analogous in some measure to the anti-circumvention provisions of the DMCA. Part IV.B, below, lists the provisions most often cited as precedents for an anticircumvention approach, as well as additional federal and state statutes that address circumvention-like situations. Part IV.C analyzes the different approaches used by the provisions and compares these approaches to the DMCA’s approach. Our conclusions concerning these “analogous” provisions are summarized briefly in Part IV.D.

B. ANALOGOUS PROVISIONS

The House and Senate Reports accompanying the DMCA cited various laws as analogous to the DMCA’s anti-circumvention provisions. In addition to these provisions, there are several federal and state laws that could provide precedent for

---

210. See, e.g., Vinje, supra note 12, at 432.
the DMCA’s anti-circumvention approach.

1. Provisions Cited as Analogous to the DMCA in Official Reports

   a. Audio Home Recording Act, 17 U.S.C. § 1002(a) & (c)

   The Audio Home Recording Act ("AHRA") is the provision most often cited as the "anti-circumvention" precedent to validate the DMCA’s approach. It is also the only federal statute we found among those cited that uses the term "circumvent." The Senate and House Reports both cited the AHRA as an anti-circumvention precedent.\(^ {211} \) So, too, did the White Paper, discussed in Part II.B, above.

   The AHRA protects sound recordings by requiring equipment manufacturers and distributors to implement a "Serial Copy Management System" (SCMS), which permits only first generation copies. Section 1002(c) addresses circumvention devices:

   No person shall import, manufacture, or distribute any device, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent any program or circuit which implements, in whole or in part, a system [like the Serial Copy Management System that prohibits unauthorized serial copying].

   The circumvention device prohibitions found in the AHRA and the DMCA appear quite similar. However, the DMCA is broader and more flexible than the AHRA, since the DMCA is not limited to a specific type of work or protection technology.\(^ {212} \) The DMCA’s express prohibition on the user’s act of circumvention has no analogy in the AHRA.\(^ {213} \)


   The Cable Act provides, "[n]o person shall intercept or receive or assist in intercepting or receiving any communication service offered over a cable system, unless specifically authorized to do so by a cable operator." It further defines "[a]ssist in interception or receiving" to include "the manufacture or distribution of equipment intended . . . for unauthorized reception."

   On its face, the Cable Act targets both unlawful users and the makers and

---


\(^ {212} \) The DMCA does enact a rights control mandate for analog videocassette recorders in 17 U.S.C. § 1201(k) (2003). However, the focus here is on the DMCA’s general anti-circumvention provisions.

\(^ {213} \) Plausibly, the AHRA also could be used against circumventing users who disable the SCMS on their own digital system, if such an act could be construed as "performing any service." The potential reach of the AHRA is unclear; in the only relevant case to illustrate enforcement of the AHRA, the manufacturers of the Rio, a device which records and plays digital music, were absolved of liability under the AHRA since the court decided that the Rio did not fall within the meaning of the Act. See Recording Indus. Ass’n of Am. v. Diamond Multimedia Sys. Inc., 180 F.3d 1072 (9th Cir. 1999). The AHRA is discussed further infra Part VI.C.2.
distributors of descrambling devices, just as the DMCA targets both circumventing users and the makers of circumvention devices. Enforcement of the Cable Act has focused mainly on makers or sellers of the decoding devices (sometimes called "black boxes"), although in a few cases, purchaser/users of cable descramblers have been held liable.\(^{214}\) In interpreting the Cable Act, courts have held that manufacturers must have acted with specific knowledge or with the intent that the devices would be used for unauthorized interception.\(^{215}\) The prohibition in the DMCA against circulating circumvention devices or providing services with "only limited commercially significant purpose or use" has no intent requirement. The alternative requirements that the device or service be "primarily designed or produced" for the purpose of circumventing a technological measure, or "marketed" for that purpose, do incorporate an element of intent (though theoretically a defendant could be found liable for circulating a device "primarily designed" for circumvention, even if defendant were not the creator). Criminal liability under the DMCA does have an intent requirement.


The Communications Act provides for civil and criminal proceedings against "[a]ny person who manufactures . . . or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device is primarily of assistance in the unauthorized decryption of satellite cable programming . . . ." Like the AHRA, this provision prohibits the manufacture and distribution of circumvention devices, but not the circumvention itself. The term "unauthorized decryption" is similar in meaning to the DMCA's term "circumvention," as the DMCA defines the term to include "[the decryption of] an encrypted work . . . without the authority of the copyright owner."

Critics argue that this provision is not analogous to the DMCA, because the satellite provision is limited to a specific situation and set of circumstances—the decryption, or circumvention, of a secured satellite signal which users have no lawful right to access without authorization.\(^{216}\) Users of copyrighted works do have certain limited rights to view or use a work without authorization (e.g., for fair use), they argue, and the DMCA's protection for TPMs might prevent users from gaining access to certain works and limit their ability to exercise copyright privileges. In short, in their view, limiting access to copyrighted works is less defensible than limiting access to satellite signals—even though those signals may contain copyrighted works. However, Congress was not persuaded that there is an unqualified right to access copyrighted works to take advantage of copyright privileges.\(^{217}\)

\(^{216}\) Vinje, supra note 12, at 433.
\(^{217}\) See, e.g., H.R. REP NO. 105-551, pt. 1, at 17 (1998); S. REP. NO. 105-190, at 11 (1998). At the same time, Congress recognized that access controls could have an impact on fair use, and so created

In a similar provision concerning satellite decryption, the North American Free Trade Agreement (NAFTA) requires that each member country make it (a) "a criminal offense to manufacture . . . or otherwise make available a device or system that is primarily of assistance in decoding an encrypted program-carrying satellite signal without the authorization of the lawful distributor of such signal; and (b) a civil offense to receive . . . an encrypted program-carrying satellite signal that has been decoded without the authorization of the lawful distributor of the signal." Like the DMCA, this language embraces both the reception of the decoded signal by the user as well as the manufacture of decoding devices.

2. Additional Provisions that Address Circumvention-Type Situations

The provisions described below do not address circumvention per se, but instead address similar types of situations involving unauthorized access to protected information. On the surface, direct comparisons with the DMCA seem strained, as these "access" measures directly protect information, while the DMCA's "anti-circumvention" measures protect technology that in turn protects information. However, the cited statutes show that the DMCA is not alone in protecting information from unauthorized use.


The Electronic Communications Privacy Act, colloquially called the "Federal Wiretap Act," makes it possible to prosecute anyone who "(a) intentionally intercepts . . . any wire, oral, or electronic communication; [or] (b) intentionally uses . . . any electronic, mechanical, or other device to intercept any oral communication." Section 2512 prohibits any person from intentionally manufacturing, selling, or possessing any device "knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications."

The Federal Wiretap Act prohibits "interception" rather than "circumvention." Unlawful interception occurs when the information at issue is readily available but is not intended to be received by the user. In contrast, unlawful circumvention requires the user to take aggressive technological steps to retrieve information that is not readily available. However, both interception and circumvention involve the unauthorized accessing of specific information. Perhaps this common aspect of unauthorized access accounts for the fact that the user and manufacturer anti-circumvention provisions of the DMCA mirror the twin provisions of the Federal Wiretap Act.
The Federal Wiretap Act includes limited and carefully articulated grants of power to lawfully intercept, just as the DMCA includes exemptions from the anticircumvention provisions. However, there are differences between the statutes. The Federal Wiretap Act contains a strict “intent” requirement. Criminal proceedings under the DMCA also have such an intent requirement, but the standard in civil proceedings is different (see discussion in Part IV.B.1.b, above). But in one respect the Federal Wiretap Act is more stringent than the DMCA: it makes it illegal to merely possess an interception device, so long as there is knowledge that it is an interception device.

b. Unauthorized Interception and Publication Provisions of the Communications Act, 47 U.S.C. § 605(a)

This provision states that, “[n]o person not being authorized by the sender shall intercept any radio communication and divulge or publish the . . . contents . . . to any person . . . [or] use such communication . . . for his own benefit or for the benefit of another not entitled thereto.” Like the Federal Wiretap Act, this provision deals with unauthorized access, rather than with circumvention per se.

c. The Stored Wire and Electronic Communications Act, 18 U.S.C. § 2701

The Stored Communications Act makes it illegal to “[i]ntentionally [access] without authorization a facility through which an electronic communication service is provided [or] intentionally [exceed] an authorization to access that facility.” Basically, the Act protects the privacy of e-mail and voice-mail. Again, although the Stored Communications Act is an “access” measure that directly protects information, like the DMCA, the Act is meant to apply to situations where an unauthorized user has circumvented a privacy device.

d. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030

The Computer Fraud and Abuse Act is aimed in particular at protecting the computers of financial institutions (including credit card companies) and government departments or agencies. A crime is committed when one “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains [certain kinds of information].” Although this is a “fraud” act in title, it is essentially concerned with unauthorized access. Like the DMCA, the statute does not contain an “intent to defraud” requirement; the Act only requires a showing of unauthorized access. In fact, defendants have been held liable under the federal Computer Fraud and Abuse Act even when they lacked an intent to defraud.218

Recently, in IMS Inquiry Management Systems, Ltd. v. Berkshire Information

the court confirmed that a civil action is available under the Computer Fraud and Abuse Act. The court held that the plaintiff, IMS, stated a claim under the Act against Berkshire, which had allegedly used the ID and password of an IMS client to gain access to IMS’s web-based tracking service and copy IMS’s reports. IMS further alleged that Berkshire had impaired the integrity of its data and caused IMS to incur significant costs for damage assessment and remedial measures.

e. Additional Federal “Access” Statutes

Additional federal statutes that prevent access in an effort to maintain the integrity of either certain devices or to protect certain information include regulations governing fraud in connection with access devices (which applies to, among other things, police “scanners”220 and prohibitions on tampering with aircraft smoke detectors.221 Again, while these provisions do not address circumvention per se, they provide examples of existing federal laws that either proscribe unauthorized access to information or prohibit interference with protection measures. In a general sense, these statutes might be viewed as precedent for anti-circumvention legislation. Finally, federal “breaking and entering” statutes, such as the federal law against breaking “the seal or lock of any railroad car, vessel, aircraft” may be seen as analogous to circumvention prohibitions; just as the DMCA makes it a crime to circumvent, without regard for any subsequent copyright infringement, “breaking and entering” laws make the forced access the crime, not necessarily any theft that might follow.222

3. Analogous State Laws

In addition to federal laws, there are numerous state laws that address the unauthorized access of information and/or protection and privacy measures.

a. State Laws Prohibiting Theft of Communication Services

Our research focused primarily on laws that predated the DMCA and provided precedent for its approach of banning predicate acts. However, it should be noted that since the DMCA was passed, a number of states have considered, and a few have passed, legislation aimed at theft of communication services. Such legislation

---

220. 18 U.S.C. § 1029 (2003) (criminalizing the act of one who, with “(a)(2) intent to defraud...traffics in or uses...an unauthorized access device...or (a)(7) uses, produces,...or possesses a telecommunications instrument...modified or altered to obtain unauthorized use of telecommunications services”).
221. FAA Air Carriers and Operators for Compensation or Hire, 14 C.F.R. § 121.317(i) (2003) (making it illegal to “tamper with, disable, or destroy any smoke detector installed in any airplane lavatory”).
222. 18 U.S.C. § 2117 (2003). Note that this provision is analogous only to the DMCA provision regarding the act of circumvention and not to the provision regarding the manufacture or making available of circumvention devices.
prohibits (i) using or distributing devices for theft of a communications service, (ii) using or distributing devices to conceal the place of origin or destination of a communication for purposes of theft of a communications service, and/or (iii) using or distributing any unlawful access device, or any plans or instructions to make an unlawful access device primarily designed or distributed to defeat technological protection used in connection with communications service. "Communications service" is defined broadly to include virtually any wire or wireless service provided for a charge. Some consumer groups staunchly oppose such laws, which they have termed "super DMCA.s."223

b. State Computer Trespass Laws

Computer "trespass" laws describe the offending conduct in terms of "unauthorized access" to digital information. For example, in Washington, it is unlawful if any person, "without authorization, intentionally gains access to a computer system or electronic data base of another; and (a) the access is made with the intent to commit another crime."224 Similarly, Arizona state law makes illegal the "[a]ccessing, altering, damaging or destroying . . . without authorization . . . of use of any computer, . . . with intent to devise a scheme to defraud."225 In New York, it is a crime if a person "knowingly uses [a computer] without authorization and: (1) he does so with an intent to commit or further the commission of any felony; or (2) he thereby knowingly gains access to computer material."226

c. State Provisions Concerning Burglars’s Tools, Lock Picks, Hot Wires

Like the federal "breaking and entering" laws described in the preceding section, these laws are concerned with particular devices that may be used to commit a theft, rather than with the theft itself. Therefore, they are similar to the specific DMCA provisions regarding manufacture and distribution of circumvention devices. In Washington, for example, a person is guilty if he may "make or mend or cause to be made or mended, or have in his possession, any engine, machine, tool, false key, pick lock, bit, nippers, or implement adapted, designed, or commonly used for the commission of burglary under circumstances evincing an intent to use or employ."227 A similar California law incorporates an interesting addition: anyone selling a lock-pick must obtain contact information of the buyer.228

227. WASH. REV. CODE ANN. § 9A.52.060 (2001). Unlike the DMCA, possession with intent is enough to establish guilt under this state law.
d. State Provisions Against Deactivating Inventory Control Devices

State laws that prohibit devices to bypass or evade inventory control devices, which in turn prevent shoplifting, are, in a broad sense, analogous to the DMCA provisions, as they protect the integrity of protection devices. In North Carolina, it is illegal willfully to conceal merchandise "by using a lead-lined or aluminum-lined bag . . . or a similar device to prevent the activation of any anti-shoplifting or inventory control device." 229 A Florida statute goes further, and makes it a crime to "possess, or use or attempt to use, any antishoplifting or inventory control device countermeasure" within any retail premises. 230 Possession of such a device on retail premises is enough; intent is assumed. These shoplifting statutes are similar to the DMCA in that each involves the evasion of a protection measure.

C. Analysis of Measures

The provisions discussed above illustrate that anti-circumvention type laws take a variety of forms. First, the laws vary with respect to their approach to the offense; some focus on the circumventing action while others focus on the device used to circumvent. Second, the laws vary in the manner in which they define the circumvention-type act. While several of the laws have an approach similar to that of the DMCA, the term "circumvent" is used only in the Audio Home Recording Act. In other statutes, the circumvention-like behavior is described as "decryption," "interception," or "unauthorized access."

1. Action Versus Device Prohibitions

A threshold issue in analyzing these provisions is the degree to which they prohibit a certain action on the part of the user versus the degree to which they focus on a device being used. For example, the Audio Home Recording Act focuses on devices, mandating use of SCMS on one hand and banning use of devices that primarily serve to circumvent the SCMS on the other. Similarly, the satellite decryption provision of the Communications Act focuses on the manufacture and distribution of a satellite descrambler, but not on the use to which the descrambled material might ultimately be put. Making or possessing burglar's tools and shoplifting devices can be illegal, irrespective of use.

Conversely, the "Unauthorized Interception and Publication" provision of the Communications Act focuses on the activities of interception and publication, without respect to any device the user may operate in the interception. The Stored Wire and Electronic Communications Act, the Computer Fraud and Abuse Act, computer trespass statutes and "breaking and entering" statutes focus on activities of the user without any provisions for devices.

The DMCA incorporates both action and device prohibitions. Several other

provisions also contain a twin focus. The Cable Communications Policy Act criminalizes the unauthorized interception of cable service, as well as “assisting” in the unauthorized interception, which includes the manufacture and distribution of a cable descrambling device. Similarly, the Federal Wiretap Act criminalizes the interception of a communication as well as the manufacture, sale, or possession of a device designed for surreptitious interception.

2. Circumvention Defined and Compared

Here we examine how the laws frame the circumvention-type activity, i.e., the manner in which the user or the device gains access to otherwise protected information, regardless of whether the statutes focus on a device or an activity.

a. Circumvention

The DMCA’s definition of “to circumvent” an access control is: “to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.” This definition resembles language in the AHRA, which essentially prohibits devices that “avoid, bypass, remove, deactivate, or otherwise circumvent” SCMS. The essential element of the circumvention concept is the existence of a technological barrier between the user and the work which must be broken or bypassed before the user can gain access to protected material. Many of the terms below can be seen as specific kinds of circumvention, probably meant to be embraced by the DMCA’s definition. On the other hand, some of the terms below, such as “unauthorized access,” are not specifically circumventing acts.

b. Descrambling/Decryption

“Descrambling” and “decryption” are essentially particular forms of “circumvention,” designed to bypass a specific type of TPM, encryption. Neither term is actually used in the provision regarding cable descramblers, but the satellite decryption provision does specifically address the “unauthorized decryption of satellite cable programming.”231 The decryption concept also appears in the NAFTA treaty, which addresses devices “primarily of assistance in decoding an encrypted program-carrying satellite signal” and makes it a civil offense “to receive... an encrypted program-carrying satellite signal that has been decoded.”232 Similarly, the provision of the Communications Act regarding cable “descramblers” specifically addresses not the descrambling, but the unauthorized “interception” or “reception” of a cable system. It makes no mention of the descrambling of such a system or of any barrier that must be bypassed; rather, the

---

descrambling is inferred in the reception.

c. Deactivation/Removal/Destruction

Deactivation and removal are encompassed within a larger circumvention concept, especially when they act against some barrier or technological device. Destruction might be understood as simply a more extreme form of deactivation. Outside of the digital realm, the prohibition on disabling aircraft smoke detectors offers an analog to the deactivation of a technological protection device, as does the North Carolina anti-shoplifting statute that attacks the use of a device "to prevent the activation of any anti-shoplifting or inventory control device."

d. Breaking and Entering

"Breaking and entering" statutes represent another non-digital analogy to computer circumvention. These statutes are concerned with the act of circumventing the barrier of a locked door and not with any crime committed once the premises has been entered. Similarly, the DMCA is concerned with the act of passing the barrier of the "locked" program and not with the copyright infringement that might occur once the protected material has been accessed.

e. Unauthorized Access

This term is broader than circumvention, because it does not always require the existence of a technological barrier. The language "intentionally accesses without authorization" appears in the Stored Wire and Electronic Communications Act, the Computer Fraud and Abuse Act and state and federal computer trespass statutes. "Access" statutes are concerned with the user's unauthorized contact with the protected material, as opposed to the anti-circumvention approach, which focuses on actions with respect to the technological measure that protects the material. Thus, in IMS Inquiry Management Systems, Ltd. v. Berkshire Information Systems, the court held that Berkshire's use of an IMS customer's password to access IMS's website did not amount to "circumvention" under § 1201. However, IMS did state a claim under the Computer Fraud and Abuse Act, which prohibits intentional and unauthorized access to a protected computer but does not require that the access be obtained through circumvention of technological controls.

f. Interception/Reception

Interception and reception seem to be more closely linked to access than to circumvention *per se*. For example, the Federal Wiretap Act prohibits the intentional interception of any wire, oral or electronic communication. The "interception" does not necessarily require overcoming a protective mechanism.

Rather, the interception is merely an action by which a user gains access to information.

D. SUMMARY

All of the statutes cited as analogies for § 1201 in the legislative history—and the additional laws described above—can be distinguished in some way, large or small, from § 1201. In addition to the criticisms discussed above, some have argued that the analogous provisions are less troubling, as a policy matter, because the predicate conduct has no valid purpose or goal (in contrast, they claim, to circumventing controls on a copyrighted work). However, this argument does not effectively refute the analogies to the cable and satellite provisions which also protect against unauthorized access to copyrighted works.\footnote{234} Section 1201 is broader than its most frequently cited predecessors in that it applies not just to a particular type of technological measure or to works delivered by a particular means (cable or satellite transmission).\footnote{235} However, as our discussion illustrates, despite the differences, these measures demonstrate that the approach taken in § 1201 is far from unprecedented.

V. TECHNOLOGICAL PROTECTION MEASURES AND DIGITAL RIGHTS MANAGEMENT TECHNOLOGIES

There are many technological protection devices in use and under development, and the landscape changes rapidly. The market for technological protection mechanisms—although very active—is still relatively young. There is a time lag between developing a technology and making it commercially available, particularly where the technology, to be effective, requires cooperation between content owners and playback device manufacturers. Many forms of protection never successfully make the transition from theory or prototype to commercially available technology. Other forms of protection become commercially available but are not widely adopted due to widespread consumer rejection.\footnote{236} Just as the technology of protection changes rapidly, so too does the technology of

\footnote{234} This argument is more effective in refuting the analogies to laws that prohibit disabling smoke detectors or carrying devices to counter anti-shoplifting mechanisms, for which no legitimate purpose is readily apparent.

\footnote{235} On the other hand, the Cable Act prohibits unauthorized access even to public domain material delivered by cable, so in that respect is broader.

\footnote{236} See, e.g., Stephanie Miles, Behind Death of Divx Were Angry Customers, CNET NEWS.COM, June 17, 1999, available at http://news.com.com/2100-1040-227248.html. In the e-book market, publishers have realized that “DRM technologies need to allow flexible usage of content so that the user experience is not frustrating.” F. Hill Slowinski, What Consumers Want in Digital Rights Management (DRM): Making Content as Widely Available as Possible in Ways that Satisfy Consumer Preference, AAP/ALA WHITE PAPER (2003), available at http://dx.doi.org/10.1003/whitepaper1. Consumer acceptance may be more readily forthcoming where the protection accompanies a new platform with enhanced features. For example, DVDs contain movies in digital form with useful playback features and often have additional material not contained in the original, which makes the protection features somewhat more palatable to users.
circumvention. As a National Research Council report explained: "The best that
can be hoped for is steady improvement in [technological protection services']
quality and affordability and keeping a step ahead of those bent on defeating the
systems."\textsuperscript{237}

Ultimately, the nature of the technological protection used (if, indeed, any form
of protection is used at all) will likely vary among content owners and among
works, depending on the value of the work, the risk of unauthorized distribution
(related in large part to the business model through which the work is marketed),
consumer response and consumer alternatives. We merely describe here some
prominent examples of technological protection devices currently in use or under
consideration.

A. COMMON TECHNOLOGICAL PROTECTION DEVICES

Digital watermarks and encryption, described below, are common components
of technological protection devices.

1. Watermarks

A watermark is basically a message within a digitized image, video or audio file,
designed to be difficult to remove. This message may be perceptible or
imperceptible to users, and can be either fragile or robust. A robust mark survives
any alterations to the original, such as file compression, decompression or
cropping. A fragile mark may be damaged or destroyed through such alterations;
its degradation or absence can be used to determine if there have been any changes
to the original.\textsuperscript{238}

A watermark can be used in many different ways to protect intellectual property.
The most basic example would be a perceptible watermark that indicates ownership
rights in an image. In essence, this is a "no trespassing" sign that serves the same
purpose as a copyright notice on a physical copy of a work. Web sites that market
images sometimes use perceptible watermarks; upon payment of a license fee, the
seller will deliver an image without the mark.\textsuperscript{239} In addition to basic ownership
information, a digital watermark can contain contact and licensing information so
that a person who wants to use the work can more easily contact the rightholder.

In a closed system—i.e., one that requires special hardware or software to view
a work—the watermark can serve as an integral part of an access or use control.
For example, a mark could be inserted to permit the making of a certain number of
copies (or first but not second generation copies), after which the hardware would
no longer make copies. Watermarks can also be used as part of a technological
screening device to prevent recording or playback of works that have been copied

\textsuperscript{237} Nat'l Research Council, The Digital Dilemma: Intellectual Property in the
Information Age 153 (2000).

\textsuperscript{238} See id., app. E, at 296-98.

\textsuperscript{239} See, e.g., http://www.corbis.com (where a user who is not logged in will see available images
displayed with the Corbis watermark).
(or compressed) without authorization in such a system. This concept underlay the dormant (and apparently defunct) Secure Digital Music Initiative (SDMI) discussed further in Part V.D.1.b below.

To be effective, watermarks must be difficult to detect or remove. An often-used analogy for effective watermarking is the proverbial “needle in a haystack.” Imagine that the haystack is a digitized work and that instead of one needle, there are thousands hidden inside. The needles comprise the watermark. While the rightholder has a map to all the needles, called a key, someone else would have to hunt down and remove each needle without disturbing the hay. In an aurally perceptible work, a watermark can be hidden in the frequencies that are inaudible to humans or tucked away in other parts of the signal that are not perceptually relevant. Similarly, in visual works, small portions of an image—a pixel here and there—can be altered to embed a mark that is not perceptible when the image is viewed as a whole. Generally, the more information contained in a work, the easier it is to hide a watermark. Nevertheless, perceptibility of watermarks continues to be debated.

Digital watermarks can be used to detect the presence of unauthorized copies of a work. In this regard they function not so much as a protection mechanism—they do not, themselves, preclude making copies. Rather, they provide a tool through which content owners can determine the extent of unauthorized copying of their works and can take legal action when infringements occur. See the discussion of tracking in Part V.B.4, below.

2. Encryption

Encryption is a method of disguising or encoding information so that only certain users can remove the code and view the information in its original, non-encrypted form. A system of encryption is based on algorithms, or formulas. A very basic algorithm might be “shift by n,” where each letter used in the message is shifted n spaces (where n is a number from one to twenty-five corresponding to the positions of the remaining letters of the alphabet). For example, if the encryption key is n=3, the encrypted version of MEET TONIGHT IN PARK would be PHHW WRQLJKW LQ SDUN.

This simple shifting cipher would never be an adequate encryption method because the set of all possible keys is too small. It would not take a computer (or a human being, for that matter) very long to try each of the twenty-five possible letter shifts and stop at the right key when it found recognizable text. Obviously, the larger the possible number of keys, the more powerful the encryption. One more robust method is called a one-time pad and uses a key that is the same length as the clear text. A digital file that is represented by a ten-digit series of 1’s and 0’s would have a key that was also ten digits long and would result in a ten-digit ciphertext. The problem with a longer key is that it makes the encryption and decryption process slower.

240. NAT’L RESEARCH COUNCIL, supra note 237, at 167.
There are two kinds of encryption systems: *symmetric* and *asymmetric*. Symmetric encryption systems use the same key (the secret key) to encrypt and decrypt a message, while asymmetric systems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Asymmetric encryption systems are also called *public key/private key* encryption. The problem with symmetric encryption systems is transporting the secret key from the sender to the recipient securely. If someone could send the secret key securely, then she would not need to encrypt the message in the first place; she could just send the information through her secure channel. Symmetric encryption systems are still useful; however, the key is generally shorter than the encrypted message and can be sent separately with a much higher degree of security.241

Public key/private key encryption was developed in response to the shortcomings of symmetric encryption.242 With its two key-system, the private key is kept secret while the public key is made available to anyone who might need it. If S wanted to send an encrypted message to R, S would find and use R’s public key to encrypt the message and only R, who has kept his private key a secret, could later decrypt the message. Because public key/private key systems are slower than symmetric-key systems, they are not as well suited for encrypting large files, such as audio or video.

A practical solution for protecting large files is a combination of symmetric and asymmetric systems. The information can be encrypted using a faster, symmetric-key system with a small key space. Then, the symmetric key exchange problem can be solved by using the more robust public key/private key encryption to send the key to the recipient. The small key space, which usually means weaker protection, is not a problem, because its small size allows it to be sent efficiently with slower public key/private key encryption.

Even sophisticated encryption systems are not without weaknesses, however. For one thing, once the work is decrypted or “in the clear,” it can usually be sent or transmitted to additional users without authorization (unless use of the work is governed by a sophisticated DRM system, as described below). Moreover, public key/private key encryption methods depend on the integrity of the key, and if the key at the recipient’s end can be discovered, the encrypted material can be discovered.

**B. FUNCTIONS OF TECHNOLOGICAL PROTECTION MEASURES**

Technological protection measures can be characterized by function, as was done in the DMCA.

---

241. *Id.* at 156-58.
1. Access Controls

Access controls are measures that prevent someone from viewing, reading, hearing and/or otherwise perceiving the work without authorization from the rightholder. Perhaps the most basic and frequently encountered form of access control is password protection, in which the user must provide identification, frequently a unique password, in order to get access to protected material. The passwords necessary to use the LexisNexis or Westlaw databases are examples of this type of protection. Also very common are IP address controls, which limit access to protected works to requests from specific computers or networks (common in the case of databases or software whose use is contractually limited to a particular campus, corporation or other entity). Another commonly encountered access control is the scrambling of satellite signals to prevent programming from being viewed by those who have not subscribed or paid.

Access controls commonly regulate whether one gets access to the protected material. However, they also can limit the number of times or the duration of the period that the material can be accessed. For example, MovieLink is an online movie "rental" service that allows a user to download a movie to her computer for viewing, for a fee. She then has thirty days to watch the movie. However, once she begins watching it, she can access it only for twenty-four hours (after which the movie deletes itself from her hard drive).243

2. Use Controls

Use controls are technological measures that limit whether and to what extent a work can be copied, communicated, viewed or played. For example, technological controls often attached to motion pictures distributed on VHS tapes (usually referred to as "Macrovision," for the company that develops and markets the most commonly used form of such protection) deter copying by effecting a substantial degradation of quality in any copy produced from the protected tape. The Serial Copy Management System (SCMS), discussed below, is a use control measure that allows an unlimited number of first generation copies of a sound recording but does not allow copies to be made from those copies (i.e., "second generation copies"). Use controls may also provide a usage metering function.

3. Protection for the Integrity and Authenticity of Information

Technological controls can establish the authenticity of information (whether it comes from the source claimed) and the integrity of the protected document (whether any alterations have been made, purposely or inadvertently). This information is valuable to all parties concerned: the recipient, the author, and the publisher. Even users who operate in an environment where payment for use is not

a principal concern (certain scholars and academics, for example) value this function of protective technology.

4. Tracking

A distinct digital watermark can serve as a “fingerprint” that can provide an audit trail from which to trace an infringing copy to the original. While the technology does not prevent unauthorized copying, it can make it more detectable and assist in policing infringing uses. Webcrawler are programs that methodically search the internet for copies of specified material and report where and when they were found. They are used by the recording industry to detect unauthorized copies of sound recordings. They are also used to track usage for licensing purposes. The “fingerprint” for which they search, however, need not be a watermark internal to the work. A digital fingerprint can be generated based on statistical measurements of a recording’s sound. Like watermarks, such digital fingerprints are not themselves technological protection devices but can be an integral part of a technological protection device. Use of programs that monitor networks for unauthorized copies of protected works based on fingerprints is controversial, however.

C. DIGITAL RIGHTS MANAGEMENT SYSTEMS

“Digital rights management” or “DRM” is not a term of art and can be defined in various ways. The term commonly refers to a system through which content

245. See, e.g., Audible Magic’s Capabilities May Charm the Industry, Billboard Magazine, Jan. 11, 2003, pg. 33. Audible Magic’s technology works by “listening” to a recording and generating a unique fingerprint for it; it apparently can identify the recording “under all compression levels and across any format.” Id.
247. Examples of definitions of “DRM” include the following:
[A] system of information technology (IT) components and services, along with corresponding law, policies and business models, which strive to distribute and control intellectual property and its rights. Product authenticity, user charges, terms-of-use and expiration of rights are typical concerns of DRM.

Technology systems facilitating the trusted, dynamic management of rights in any kind of digital information, throughout its lifecycle and wherever and however it is distributed.


DRM systems are based on digital technologies that describe and identify content, and enforce rules set by right holder or prescribed by law for the distribution and use of content. . . . TPMs generally are designed to impede access or copying, while DRM systems do not impede access or copying per se, but rather create an environment in which various types of use, including copying, are only practically possible in compliance with the terms set by the right holders.
is made available to users in electronic form online, pursuant to conditions (such as payment, extent of access or copying) established by the content owner. Most DRM systems employ some form of technological controls to prevent unauthorized access to and use of works they contain, although the protection may be as simple as password control. 248

In some DRM systems, the subject works are encrypted and can be viewed, printed, played or downloaded under specified license terms and conditions which may include start time, duration, number of plays or copies, limitation to specific devices, price, etc. and which may vary with the status of the user. In some cases, the same terms and conditions apply to all works; in others, the individual rightholder can decide on the terms applicable to her works. 249 The license terms can travel with the encrypted content or separately. Keeping the license information separate from the content provides the rightholders with the flexibility to change the terms of the license without altering the content or its distribution scheme.

Typically, an end-user identifies the content she wants and then seeks permission for the desired use. Such inquiries are automated and handled through a rights clearinghouse. The clearinghouse will provide the terms of use for the particular work and, if applicable, the category of user. It will also assure payment is made or other requirements complied with before transmitting the key to allow the user to decrypt the work. A user may be able to license access on behalf of other recipients and be billed on the basis of usage metering. In a system oriented toward academic users, usage metering can also serve as a measure of the prominence or visibility of a work. Systems designed for commercial use by individual end users incorporate credit card or other payment schemes.

In many systems, once the work has been paid for by the end user and received in “clear” unencrypted form, there is no technical obstacle to copying and further disseminating it. But some sophisticated DRM systems (known as “trusted systems”) employ “persistent protection.” They will allow transmissions only to particular devices or for particular uses. In some cases, a would-be user may actually acquire the encrypted content before seeking permission for use by, for example, downloading it from the web or receiving it from another user. However, due to “persistent protection” attached to the work, the user will not be able to access it until he agrees to the terms of the license and receives the appropriate encryption key. 250

Many forms of technological protection—arguably the most effective ones—


248. DRM and technological protection mechanisms are not equivalent. Works can be protected with technological protection devices separate and apart from a comprehensive DRM system—for example, a technological measure known as CSS protects DVDs from unauthorized copying.

249. Note that for some rightholders, attribution and the integrity of the original are at least as important as payment.

250. See I. TROTTER HARDY, supra note 242, at 76; NAT’L RESEARCH COUNCIL, supra note 237 at 163, 167-70.
require cooperation among rightholders, developers and distributors of protection devices, and manufacturers of consumer devices, such as DVD players, that must respond to the protection mechanisms for them to be effective.\textsuperscript{251}

\section*{D. Measures Employed}

\subsection*{1. Music Industry}

\paragraph*{a. SCMS}

In the early 1990s, as digital audio tape players and recorders were about to be introduced in the U.S., the music industry became concerned about the prospect of digital copying. While unauthorized copies of sound recordings were clearly being made before that time, the degradation of quality that took place with each successive analog copy put a brake on unauthorized copying. But digital technology allowed perfect serial copies of a work to be produced, so that “brake” was no longer effective. The music industry attempted to delay the introduction of digital audio recording devices until protective mechanisms could be negotiated with the consumer electronics industry. Their negotiations culminated in the Audio Home Recording Act (AHRA)\textsuperscript{252} Under the AHRA, consumer device manufacturers were required to implement the Serial Copy Management System (SCMS). SCMS permits an unlimited number of copies to be made from an original copy (i.e., one sold or distributed with the rightholder’s authorization), known as “first generation copies,” but does not allow any copies to be made from those copies, which would be “second generation copies.”

As the market developed, however, compact discs (CDs) rather than digital audio tape became the dominant medium of distribution for sound recordings. Until recently, CDs have been distributed largely without technological protection measures.

\paragraph*{b. SDMI}

As unauthorized digital copies became increasingly common, the music industry sought a solution through the Secure Digital Music Initiative (SDMI), formed in 1998. SDMI is a consortium of recording companies, technology companies and manufacturers of consumer electronics devices.\textsuperscript{253} Its goal was to develop a secure

\begin{footnotesize}
\begin{itemize}
\end{itemize}
\end{footnotesize}
architecture for delivering music in digital form. Part of the plan was to have SDMI-compliant devices screen out copies made without authorization. In 1999, SDMI adopted a watermarking specification developed by Verance to facilitate the screening function. However, the parties were unable to agree among themselves to develop only devices that are SDMI compliant, i.e., ones that would play "secure" music but screen out and reject playback of unauthorized copies. Accordingly, few such devices were developed, and those that were had to compete in the marketplace with devices that could play both secure and unauthorized music. Since there was little music directed solely to SDMI compliant devices, consumers had little incentive to buy them.

SDMI has fallen by the wayside. In September 2000, SDMI issued a public challenge to computer programmers to try to hack its digital watermark. Programmers succeeded within weeks. Since then, the SDMI initiative appears to have died.

c. Copy-Protected CDs

Record companies recently began releasing limited numbers of copy-protected compact discs. Among the technology companies involved early in creating such protection were SunnComm (with its MediaCloQ technology—now called MediaMax CD3), Macrovision (with its SafeAudio technology), Midbar Technology (with its "Cactus Data Shield"), later acquired by Macrovision, and ContentGuard. Introduction of copy-protected CDs created a backlash by consumers. Some have brought suits claiming that such works do not perform


255. The Sony Memory Stick Walkman, one of the first SDMI-compliant devices, "bombed" in the marketplace, "primarily because of various copyright protection features that were onerous for consumers." Sara Robinson, Sony vs. Sony, EWEEK, Mar. 26, 2001, available at http://www.eewek.com/article2/0,3959,96887,00.asp.


properly in portable CD players or CD-ROM drives and are not fairly labeled to so indicate.\textsuperscript{262} Philips Electronics, owner of the CD trademarks, has objected to use of the trademarks on discs that use copy protection.\textsuperscript{263} Some further argue that use of such technologies violates the spirit if not the letter of the AHRA.\textsuperscript{264}

d. DVD Audio

DVD Audio was to have been protected by a successor to CSS, but those plans were abandoned after the creation and widespread distribution of DeCSS.\textsuperscript{265} Instead, CPPM (Content Protection for Pre-Recorded Media) was selected as the technological mechanism to protect DVD Audio.\textsuperscript{266} CPPM, developed by Intel, IBM, Matsushita and Toshiba, is a more sophisticated form of encryption than CSS.\textsuperscript{267}

e. Internet Distribution

The most prominent online music distribution service is iTunes, launched by the Apple Computer Company. With a vast catalog of music from all five major U.S. record labels and agreements with 200 independent labels, iTunes sells individual songs for $0.99 each. Once songs are purchased, they can be copied to CDs or Apple's handheld MP3 player called "iPod." To protect the content it distributes from unlicensed reproduction, iTunes utilizes Apple's proprietary FairPlay DRM technology.\textsuperscript{268} FairPlay allows users to download their music purchases to any

---


\textsuperscript{262} A consumer suit against SunnComm and the distributor of a protected CD alleged that the CD label was misleading. The parties settled out of court, with the defendants agreeing to provide a more explicit warning to consumers. See Lisa M. Bowman, Consumer Claims Victory in CD Lawsuit, CNET NEWS, Feb. 22, 2002, available at http://news.com.com/2100-1023-843114.html. A class action lawsuit has been filed against five major record companies that have distributed musical recordings on copy-protected CDs, alleging breach of warranty, negligent misrepresentation and violations of California's consumer rights laws. Dickey v. Universal Music Group, et al., No. 02-0264 (Cal. Sup. Ct. L.A. County, filed June 11, 2002), available at http://www.milberg.com/pdf/audiocs/complaint.pdf. The suit was brought on behalf of purchasers of defective compact discs whose technological protection is alleged to render the discs "unreproducible or unstable for use in many personal computers." Id. at par.16.

\textsuperscript{263} Chris Marlow, Philips: Protected CDs Not Compact Discs at All, HOLLYWOOD REP., Jan. 16, 2002. Sony Electronics, co-inventor with Philips of the CD format, apparently agrees with Philips' position, despite the fact that Sony Music has released at least seventy copy-protected CDs in Europe. See Amy Harmon, CD Technology Stops Copies but it Starts a Controversy, N.Y. TIMES, Mar. 1, 2002, at C1.

\textsuperscript{264} Harmon, supra note 263, at C1. Congressman Rick Boucher has introduced H.R. 107, "The Digital Media Consumers' Rights Act of 2003," to remedy the alleged mislabeling of copy-protected CDs. See discussion of H.R. 107, supra Part II.E.

\textsuperscript{265} See discussion of CSS and of DeCSS and Universal City Studios, Inc. v. Corley, supra Part II.C.

\textsuperscript{266} See discussion of 4C, infra Part V.E.


number of iPods but limits them to three computers. FairPlay also enables customers to create custom playlists but limits the total number of copies to ten.\textsuperscript{269}

Other online music distribution services in this very active market\textsuperscript{270} include Napster 2.0,\textsuperscript{271} MusicMatch,\textsuperscript{272} Wal-Mart,\textsuperscript{273} BuyMusic,\textsuperscript{274} and the Rhapsody service.\textsuperscript{275} Sony has announced a new online music store, Connect, that will allow downloads at $0.99 per song to a variety of playback devices.\textsuperscript{276} The two major players offering DRM systems to music distributors are Microsoft and RealNetworks.

Pressplay, a joint venture between Sony Music Entertainment and Universal Music Group,\textsuperscript{277} is a digital music subscription service. Pressplay uses Microsoft's Windows Media DRM to deter unauthorized use of content available through the service.

MusicNet is an online music delivery company that supplies interactive music services that consumer brands (such as AOL) offer to their customers.\textsuperscript{278} Unlike Pressplay and iTunes, MusicNet does not offer on-demand music directly to consumers. The company, which contains the music catalogs of major and independent record labels, uses DRM technology provided by both Microsoft and RealNetworks to protect its content from piracy.

Another player in the online music field, Liquid Audio,\textsuperscript{279} uses its own software and DRM technology to facilitate publishing, hosting and distributing secure digital music content over the internet.\textsuperscript{280} Like MusicNet, Liquid Audio partners with companies wishing to distribute digital media content over the internet. Some of
2. Motion Picture Industry

   a. Macrovision

The motion picture industry began employing copy protection on VHS tapes some years ago. That protection is commonly referred to as "Macrovision," for the company that markets it. Macrovision attaches to the automatic gain control circuit in the VCR, distorting the signals and degrading the quality of the copy made. Although (like many other protection mechanisms) it can be circumvented, copies made from VHS tapes are generally analog copies whose quality diminishes over time.282

   b. CSS

The motion picture industry was reluctant to release movies in digital form, on digital versatile discs (DVDs), without a technological mechanism to protect against unauthorized copying and distribution. Since DVDs were a new technology without an installed base of players, a protection mechanism could be built into the playback devices from the start. Matsushita Electric Industrial Co. Ltd. (MEI) together with Toshiba Corp. developed the Content Scramble System (CSS) under the aegis of the Copy Protection Technical Working Group (CPTWG). CPTWG is an informal association of motion picture studios, consumer electronics manufacturers and the computer industry.283

CSS is a technology used by motion picture studios to encrypt DVD contents. Only licensed devices—DVD players and DVD ROM drives—can decrypt and play the DVD contents. The CSS decryption licenses, which permit consumer equipment manufacturers to embed keys to unlock the decrypted contents to play on their devices, require that content be sent only to authorized outputs, including analog outputs and secure digital outputs. They generally prohibit copies being made.

CSS also contains a geographic region-coding feature. Playback devices sold in a particular region can play only DVDs authorized for playback in that region.284

---


283. Marks & Turnbull, supra note 251, at 13-14 & Annex B.

284. There are currently six geographic regions: 1. USA and Canada; 2. Europe, Middle East, South Africa and Japan; 3. Southeast Asia and East Asia; 4. Central and South America, Mexico, Australia and New Zealand; 5. Eastern Europe, Indian subcontinent, Africa, North Korea and Mongolia; and 6. China. See FAQ, THE MAC DVD RESOURCE, at http://www.wormintheapple.gr/macdvd/
The region coding aspect of the CSS technology and license has been extremely controversial in the United States, where it has been raised repeatedly in the Copyright Office rulemaking proceeding and in legal literature. It is also the subject of an inquiry in Australia, and the European Commission has launched an investigation.

The CSS technology has in general been very controversial. It was hacked in 1999 by a young Norwegian teenager, Jon Johansen, who developed a utility known as “DeCSS” to remove the protection from DVDs. Subsequent distribution of DeCSS was the subject of the Universal City Studios v. Corley lawsuit, discussed in Part II.C above.

c. DTCP

From the perspective of a rightholder, one flaw in protecting a work by means of encryption is that once the work is decrypted and “in the clear” (as it must be to be viewed or heard by consumers), it can be further disseminated. The Digital Transmission Content Protection (DTCP) system is a mechanism for protecting proprietary content against unauthorized interception or retransmission as it travels across digital interfaces. Developed by a group of consumer electronics and computer companies, DTCP restricts certain uses of content—e.g., copying prerecorded media, video-on-demand or pay-per-view, or transmitting any content against unauthorized internet transmission. At the same time, it permits consumers to copy broadcast programs and move copies among servers within the home.

DTCP includes encryption on content transmitted between “source” devices (such as a set-top box) and playback devices (such as a television or a personal computer). A source device will not transfer content to a playback device until it first verifies that the playback device is “trusted.” The transmission from source devices also indicates whether content can be copied. The DTCP system allows some limited amount of copying but may be used to prevent copying of prerecorded media, pay-per-view broadcasts and the like. Rightholders can encode

faq.html. In addition, Region 7 is “undefined” and Region 8 is used by airlines and others. See DVD Regional Codes, TECHRONICS.COM, at http://www.techronics.com/uk/shop/510-dvd-region-codes.html.


their works in various ways, e.g., copy never, copy one generation, copy but no retransmission, etc. 289

d. Protection for Internet Distribution

Movielink is currently the most prominent online movie rental service 290 and is backed by several major motion picture studios. 291 Users can download movies for viewing on their computers. Once downloaded, they have thirty days in which to view the movie (but once they have viewed it, they can access it only for the succeeding twenty-four hours). 292 Movielink has chosen to use both Microsoft Windows Media and RealNetworks Media Commerce Suite to provide DRM and streaming technology. 293

3. Book Publishing

Adobe, a leader in the e-book marketplace, does not require proprietary hardware. Adobe users can download Adobe Acrobat eBook Reader software from the company's website at no cost. 294 Once the software is installed in a user's computer, she may purchase content from the Adobe "bookstore" and access the work directly through her computer. Adobe is currently affiliated with numerous content distributors, including Amazon.com and eBooks.com. Its software places a variety of printing and copying restrictions on content, depending on the individual publisher's guidelines.

Microsoft's Microsoft Reader also may be downloaded free of charge from its website. The Microsoft Reader is compatible with Windows-based laptop and desktop computers. 295 Like Adobe, Microsoft provides flexible digital rights solutions that can vary depending on the publisher. Many publishers offer e-books that are compatible with both the Microsoft Reader and the Adobe Acrobat eBook Reader that may be downloaded directly from the publisher's website. 296

---

289. Cunard, supra note 286, at 31-33.
290. Other examples of online video services include CINEMANOW, at http://www.cinemanow.com (motion pictures), and SOAPCITY, at http://www.soapcity.com (soap operas).
296. Amazon.com and eBooks.com offer e-books compatible with the Microsoft Reader. Random House also distributes e-books compatible with Adobe Reader, Microsoft Reader and Palm Reader, available at http://www.contentlinkinc.com. Rosetta Books, in addition to delivering e-books in Microsoft and Adobe formats, also makes available e-books in formats that can be read on personal digital assistants through Palm Digital and Mobi Pocket. See About eBooks, ROSETTA BOOKS, at
Another popular e-book viewing format is the Palm Reader, a product of Palm Digital Media. Readers can download the Reader from Palm Digital Media’s website at no cost.\(^{297}\) Palm focuses on handheld computers, also known as personal digital assistants (PDAs), as the format for e-books. Palm Reader software is available for either Palm OS or Pocket PC handhelds and Macintosh or Windows computers. Palm also has a flexible digital rights system similar to its competitors.\(^{298}\)

Finally, the MobiPocket Reader is a fast-growing e-book format.\(^{299}\) The MobiPocket Reader allows users to download and read e-books on many different hardware systems including smartphones, PDAs and personal computers. MobiPocket software is compatible with several different platforms, including Microsoft Smartphone 2002, SymbianOS smartphones, Palm OS, Pocket PC and Windows PC platforms.\(^{300}\) In addition, MobiPocket provides its own internal Digital Rights Management system, through its secure wholesale and distribution center known as eBookBase. MobiPocket’s internal DRM servers provide for secure delivery of e-book products directly to customers through retailer websites.\(^{301}\)

E. TPMS AND TECHNOLOGY COMPANIES

Several large technology companies and consortia are developing technological protection systems that will apply to various types of content to be used in various types of receiving and playback devices or specifications that will form the basis of such systems. (There is, of course, overlap between the protective measures discussed above in connection with specific types of content and the initiatives discussed below).

Some of the better known companies and consortia include:\(^{302}\)

Adobe Systems Incorporated, (Adobe), is one of the world’s largest software companies, popularly known for its publishing programs, such as Adobe Acrobat Reader and the Adobe Acrobat eBook Reader (now available in the same


\(^{297}\) The software is available at http://www.palmdigitalmedia.com. Palm also offers an advanced version of its software called the Palm Reader Pro.

\(^{298}\) Palm, like Microsoft and Adobe, employs OverDrive Inc. as one of its DRM providers. OverDrive refers to Microsoft, Adobe and Palm as its “strategic partners.” See http://www.overdrive.com/drm_solutions.


\(^{302}\) As noted above, this is not a comprehensive list; it is merely a selection of some of the larger or more visible technological protection endeavors. For a more extensive listing of technology companies, consortia, products and initiatives, see Lyon, supra note 247; HUGENHOLTZ ET AL., supra note 247, at 5-8.
application)\textsuperscript{303} and Adobe Photoshop. Adobe has developed its own digital rights protection system, Adobe DRM, which helps publishers protect their works through establishment of specific user rights and limiting distribution to authorized users.\textsuperscript{304} Adobe DRM is based on PDF format and is designed to provide flexibility for publishers and users of e-books. Adobe’s technological protection system extends beyond e-books as well. For example, Adobe Content Server 3.0 is designed to provide security and rights management not only for its partners, including e-book vendors, but also for libraries, enterprises and government agencies interested in protection of digital content.\textsuperscript{305}

\textbf{ContentGuard}, a company majority-owned by Xerox with a minority investment from Microsoft, is pushing for the industry-wide adoption of the eXensible rights Markup Language ("XrML"). XrML is a general-purpose, XML-based digital rights specification grammar for expressing rights and conditions associated with digital content, services, or any digital resource.\textsuperscript{306} Born at Xerox’s Palo Alto Research Center, XrML was developed as an open standard. ContentGuard sells programming tools for working with XrML-based systems. XrML is not a complete DRM system but could provide a uniform rights management specification for DRM systems.

The \textbf{Copy Protection Technical Working Group}, (CPTWG), is an industry working group formed to study and evaluate content protection technologies. CPTWG does not itself develop technology, but it provides a forum for collaboration among technology and entertainment companies. It has encouraged the development of a number of protection technologies, for example, CSS, DTCP and HDCP, discussed below. One recent initiative of the CPTWG was the Broadcast Protection Discussion Group (BPDG), a cross-industry working group that includes companies from the entertainment, consumer electronics and information technology sectors, as well as consumer representatives. BPDG was formed to evaluate the merits of a technical solution using a “broadcast flag” (bits embedded in broadcast signals) for preventing unauthorized redistribution—particularly over the internet—of digital broadcast television. The group’s report was released in 2002.\textsuperscript{307} The broadcast flag technology is the subject of a recent ruling by the Federal Communications Commission, discussed in Part I.E above.

\begin{flushleft}
\textsuperscript{303} See supra note 294.
\textsuperscript{306} See XrML Frequently Asked Questions, XrML, at http://www.xrml.org/faq.asp#1. For additional explication of the digital rights concept, see Courtney E. Howard, Content Control, ELECTRONIC PUBLISHING (Feb. 2003), at http://ep.pennnet.com/Articles/Article_Display.cfm?Section=Articles&Subsection=Display&ARTICLE_ID=166994&KEYWORD=DRM ("The digital rights language is the component that enables the DRM system provider to describe the rights and conditions in the form of a license for any piece of content. Using a rights language will mean the system you’re buying, acquiring, or building will have the flexibility and scalability for specifying any right and any condition you want and ensuring those conditions and rights persistently travel with the content.").
\end{flushleft}
DOI/International DOI Foundation. Various publishing and technology companies and other content owners have been experimenting with the Digital Object Identifier (DOI) System. A DOI is a unique, persistent identifier that is assigned to content and registered in the DOI directory. It has been referred to as a “bar code” for intellectual property and can be used to identify any intellectual property that is expressed in digital form. Rightholders can obtain a prefix for a DOI from the International DOI Foundation or from a Registration Agency. The rightholder then determines a specific suffix identifying the particular piece of data to which it gets affixed. There are significant challenges to implementing a DOI system, including developing a supporting infrastructure that can handle the assignment of unique identifiers, a directory of references and locations and a database of rights information. Currently over 35 organizations are members of the International DOI Foundation.

The Digital Transmission Licensing Authority, (DTLA), (also known as “5C”) was established by Hitachi, Intel, Matsushita, Sony and Toshiba to license their jointly developed Digital Transmission Content Protection (DTCP) technology discussed above.

The DVD Copy Control AssociationB, (DVD CCA), is the not-for-profit entity that licenses CSS to manufacturers of DVD players.

The 4C Entity, (4C), includes IBM, Intel, Panasonic and Toshiba. The 4C companies developed and licensed CPRM and CPPM (Content Protection for Recordable Media and Content Protection for Pre-Recorded Media), an encryption specification to protect content of portable data storage media (such as recordable DVDs and Flash memory) from unauthorized copying. It enables interchange of stored content among different devices manufactured by different companies. 4C also developed CPSA (Content Protection System Architecture), an integrated framework for managing data protected by different protection technologies.

IBM, a member of 5C (discussed above) and partner with RealNetworks in the development of XMCL (discussed below), has developed the Electronic Media Management System (EMMS). EMMS is an end-to-end DRM system for the secure distribution of all forms of digital media, including music and other audio content. In addition to technology aimed at the music industry, IBM has developed eXtensible Content Protection (xCP). Building on the company’s

312. See Content Protection for Recordable Media, 4C ENTITY, at http://www.4centity.com/tech/cprm/.
existing CPRM and CPPM digital rights management technologies.\(^\text{315}\) xCP enables content to be played securely on media devices (e.g., cell phones, DVD players, Personal Digital Assistants, TV’s, MP3’s) grouped within a “home” network.\(^\text{316}\) Each home network is assigned a “key.” The key is then embedded within each device on the network. When copy-protected content is streamed to (or played within) the home, the key “unlocks” the encrypted content and enables it to be played. Devices outside the network (i.e., those lacking the key) are denied access to the content.\(^\text{317}\)

**Info2Clear** is one of Europe’s leading providers of digital rights management, secure digital content delivery systems and copyright registration and clearance. Info2Clear provides an array of DRM services to companies, publishers, the digital music industry, and others.\(^\text{318}\) Info2Clear has also developed SecureAttachment, a service based on Adobe Content Server that enables users to send valuable or confidential documents electronically as e-mail attachments, without the threat of unauthorized redistribution by recipients. SecureAttachment targets the corporate world in general and more specifically the world of company advisers, law firms, investment bankers, the medical world, and the pharmaceutical industry.\(^\text{319}\) Additionally, Info2Clear recently announced the creation of the Rights Management Academy, designed to provide courses and consulting services to organizations seeking to prevent unauthorized proliferation of their proprietary digital content.\(^\text{320}\)

Intel developed **HDCP** (High-Bandwidth Digital Content Protection), a specification to protect digital entertainment content across a connection to a digital monitor. Specifically, HDCP protects digital entertainment content that uses the Digital Video Interface (DVI)\(^\text{321}\) by encrypting the transmission between the video source (e.g., a computer or set-top box) and the receiver that provides the display (e.g., LCD monitor or television). HDCP is licensed by Digital Content Protection, LLC.\(^\text{322}\) Intel also participated in the development of CPRM/CPPM and DTCP.

\(^{315}\) For a description of Content Protection for Recordable Media, see 4C ENTITTY, *supra* note 312.

\(^{316}\) For an in depth explanation of how xCP works, see Press Release, IBM, xCP: eXtensible Content Protection, *at* http://www1.ibm.com/solutions/digitalmedia/doc/content/bin/xCPWhitepaper finalist.pdf.


\(^{318}\) *See Our Services*, Info2CLEAR, *at* http://www.info2clear.com/EN/services.asp.


\(^{321}\) DVI is a specification created by the Digital Display Working Group to accommodate both analog and digital monitors. *See DVI*, WHATIS.COM, *at* http://whatis.techtarget.com/definition/0,sid9,gci805034,00.html; *Interface Game*, PC MAGAZINE, Feb. 6, 2001, available at http://www.pcmag.com/article2/0,1759,39761,00.asp.

InterTrust developed an encryption-based DRM system, Rights/System for music, video and publishing files. It sold server and client software to encrypt, distribute and decrypt content and supported multiple business and distribution models. InterTrust was acquired by Sony and Philips in 2002.\(^{323}\)

Macrovision develops copy protection, DRM and electronic license management technologies for the video, music and software industries. It is perhaps best known for its anti-copy technology for video products.\(^{324}\) Macrovision’s product line includes FLEXnet and SAMsuite, which provide for software licensing and asset management; and SafeDisc, which provides CD/DVD copy protection. Macrovision’s CDS products provide copy protection for music copyright owners. CDS is promoted as inhibiting unauthorized copying or file-trading while maintaining original audio quality.\(^{325}\) Macrovision released its latest generation of CDS, called CDS-300, in January 2004. CDS-300 is designed to safeguard music CDs and incorporates Windows Media DRM. It enables content owners to determine the level of usage rights (e.g., the number of copies that can be made, or the ability to export files to compliant portable electronic devices). CDS-300 is also engineered to be updated periodically in order to stay ahead of hackers.\(^{326}\)

Microsoft has developed its own DRM technology, called Windows Media DRM. This system provides content providers with a secure platform over which to distribute digital media files. The latest release, known as Windows Media DRM 9 Series, supports realtime encryption ("Live DRM") which enables content to be delivered simultaneously to consumers as it happens.\(^{327}\)

With a program called Windows Media Rights Manager, a media file is encrypted, and a license is issued. This file can only be played by the person who has obtained a valid license. Windows Media Rights Manager functions both as the license clearinghouse, authenticating the consumer’s request for a license, and as the license issuer. Windows Media Player 9 includes DRM technology, including a feature that queries an online license server before playing any content, streaming or otherwise. The security system includes Microsoft’s Secure Audio Path technology, which authenticates the device driver to protect against piracy.\(^{328}\)

Complementing Windows DRM technology is Microsoft’s “Palladium,” a software architecture that greatly enhances the security of a computer. Since

---


renamed "Next-Generation Secure Computing Base for Windows," it is based on the TCPA computing platform, with added features. It is designed to provide an environment in which content and applications cannot be tampered with, and applications can engage in secure communications with vendors. It ensures that a remote trusted system will follow instructions, and it controls what an end user can do with content (e.g., limiting whether and under what circumstances it can be played, modified, etc.).

Next-Generation Secure Computing Base for Windows facilitates DRM by allowing content holders to determine the number of times or the time period during which a user can listen to or view the content, whether or not copies can be made and so on. It will also make it harder to use unlicensed software by detecting and refusing to run unauthorized software. It will facilitate a software rental market, since it will allow the vendor to terminate use of the software if payment is not made.

In addition to these technological developments, Microsoft partnered with Xerox on ContentGuard XrML. Microsoft Reader (discussed above under e-books), built around Microsoft’s Digital Asset Server, is based on XrML.

The Open eBook Forum. Publishers are working closely with DRM developers to develop standards and software tools that combine protection for publishers with flexible access for users. The Open eBook Forum (OeBF) is an organization comprised of “hardware and software companies, publishers, accessibility advocates, authors, users of electronic books, and related organizations” that is working towards establishing industry standards to advance the competitiveness and acceptance of e-books. The OeBF is attempting to develop standardized web page programming code that imbeds ownership information and a verification system that can check a reader’s authorization to access a particular work. The principal achievement of this group so far has been the development of the Open eBook Publication Structure specification based on HTML and XML. This accomplishment merely enables e-Books to be published on a broader number of platforms and does not significantly advance efforts to protect electronically published works. The OeBF has a group focusing on creating a commercially viable standard for interoperability of DRM systems.


331. Information on the Open eBook Forum can be found at OPEN EBOOK FORUM, at http://www.openebook.org.


RealNetworks has developed the eXtensible Media Commerce Language ("XMCL"), an open XML-based language for distributing proprietary material over the internet. Supported from the time of its launch by a number of leading technology and media industry companies, XMCL is designed to standardize the language for internet media business. XMCL is a competitor of XrML. RealNetworks has also created RealSystem, an application suite that allows streaming or downloading of encrypted, watermarked content. Its use requires installation of license management software on the client computer.

In an effort to provide increasingly secure digital distribution (and to outperform Microsoft), RealNetworks has developed its own DRM system. Like its industry-wide counterparts, Helix DRM 10 is a platform for secure media content delivery. But unlike its competitors, Helix’s DRM platform is engineered to solve the conundrum faced by consumer electronics manufactures and content providers of having to support a variety of disparate platforms. According to the company, Helix is designed to enable “content owners to deliver secure content to any PC or non-PC device using a single DRM and gives device makers a single engine to support all formats.”

The Secure Digital Music Initiative, (SDMI), discussed above.

The Trusted Computing Platform Alliance, (TCPA), is an industry working group initially formed by Intel, Compaq, Hewlett-Packard and IBM. It was later expanded to include 150 participating companies, including Microsoft. TCPA is developing specifications to provide security in computer and communications platforms, starting with the PC.

Xerox (see ContentGuard, above).

VI. DISCUSSION

The discussion and conclusions of this report are based on several premises. First, we assume that the United States will continue to protect technological protection measures to the extent required by the WIPO treaties. Second, we

335. See id.
340. See discussion supra, Part I. The WIPO treaties require adhering countries to provide "adequate legal protection and effective legal remedies against the circumvention of effective technological measures," used by authors to restrict unauthorized acts in respect of their protected
believe that there are ways that the DMCA could be amended, consistent with those treaties, to provide users greater ability to exercise copyright privileges. Third, we assume that the use of technological protection measures ("TPMs") is a rational business decision for some copyright owners.

We begin below by discussing the principal criticisms that have been leveled at the anti-circumvention provisions of the DMCA and then go on to consider the various solutions that have been proposed to overhaul or replace § 1201. Finally, we address areas where additional exemptions may be appropriate now or in the future, either through judicial interpretation of the law or statutory amendment.

A. CRITICISMS OF THE DMCA

Criticisms of the anti-circumvention provisions of the DMCA have been the subject of numerous speeches, articles and briefs, as well as petitions for exemptions in the Copyright Office's rulemaking proceedings. The principal criticisms leveled at the DMCA are listed below.

1. The DMCA Will Promote Digital Lockup and Lead to a "Pay-Per-Use" Society

Even before the DMCA was passed, the prospect of legally enforceable technological controls raised the specter of a "pay-per-use" society in which works would be locked up and every encounter with a work, even reading or browsing, would require payment.

2. The DMCA Inhibits Fair Use and Other Copyright Privileges

Critics claim the DMCA's prohibition on circumventing access controls restricts the ability to access copyrighted materials to take advantage of fair use and other copyright privileges. The Copyright Office rulemaking proceedings do not, in their view, provide an adequate failsafe mechanism. They also argue that the device distribution restrictions impede fair use.

3. The DMCA Inhibits Free Speech and Violates the First Amendment

Circumvention devices in the form of software are themselves protected speech, the argument goes, and therefore prohibiting their dissemination violates the First Amendment. DMCA critics also argue that fair use is an essential means by which the copyright law accommodates the First Amendment and ensures free speech; by restricting the means to make fair use, the law violates the First Amendment rights.

341. It is impossible to list the myriad ways in which users have claimed copyright privileges have been inhibited, but a review of the exemptions sought in the recent rulemaking proceeding is instructive in this regard. See generally Recommendation of the Register of Copyrights, supra note 149, at 82-189.
342. See discussion infra Parts VI.B.5, VI.C.1.b & VI.E.4.
343. See discussion infra Parts VI.B.4 & VI.C.1.
of users.  

4. The DMCA Will Limit Access to Public Domain Works

Critics fear that distributors will “lock up” public domain works with access controls, and that circumvention devices will be unavailable due to the anti-trafficking provisions. Moreover, they claim that the DMCA encourages distributors to assert control over public domain works by repackaging them with copyright-protected works to avoid the possibility of circumvention.

5. The DMCA’s Anti-Trafficking Provisions Eliminate the Practical Ability to Enjoy Copyright Privileges

There are a number of exemptions to the ban against circumventing access controls (including those provided pursuant to the rulemaking proceeding) and no statutory bar to circumventing use controls. At the same time, trafficking in circumvention devices is severely restricted by the law. It is prohibited to manufacture or distribute devices that were created for the purpose of circumventing a technological access or use control, or that have no commercially significant purpose or use other than circumvention or to market devices for circumvention purposes. Because this test is so stringent, the DMCA’s critics claim that few devices will be available to enable permissible uses, and without such devices, users’ privileges are essentially meaningless. A film student, for example, may have no means to make excerpts of films for a project, even though there is no prohibition on circumventing copy controls.

6. The DMCA Lets Copyright Owners Defeat Privileges Under the First Sale Doctrine by Supporting Access Restrictions that “Tether” Works to Particular Playback Devices

Access controls may limit copies of digital works to use on a particular playback device (e.g., a computer or handheld device) or on a particular platform (e.g., licensed DVD players or computer drives). DMCA critics contend that such controls deprive users of their privileges under the “first sale doctrine,” which entitles the owner of a particular copy of a copyrighted work to sell or otherwise dispose of that copy.

344. See discussion infra Part VI.C.1.e.
345. See discussion infra Part VI.E.1.
346. See discussion infra Parts VI.B.4.a, VI.C.1 & VI.E.7.
348. See discussion infra Parts VI.B.4.b, VI.B.5 & VI.E.4.
7. The DMCA Prevents Legitimate Research Activities Involving Reverse Engineering and Investigation of Improved Encryption Methods

There are exemptions in the DMCA for reverse engineering and encryption research. However, critics argue that they are not broad enough to meet legitimate research needs and that the DMCA is having a chilling effect on these activities.\(^{349}\)

8. The DMCA Restricts Competition in the Replacement Parts Market

In response to the *Lexmark* and *Chamberlain* decisions, discussed above in Part II, critics have condemned attempts to use the DMCA’s anti-circumvention provisions to restrict competition in the replacement parts market.\(^{350}\)

9. The Anti-Circumvention Approach of the DMCA Is Futile

Some commentators argue that because of the ready availability of tools for circumvention, as well as the inevitable appearance of clear, unencrypted copies of copyrighted works on peer-to-peer networks, the anti-circumvention approach of the DMCA can never be effective in limiting infringement.\(^{351}\)

**B. FACTORS UNDERLYING THE DEBATE ABOUT § 1201**

Why has § 1201 been so controversial? In order to answer this question it is useful to examine some of the factors and premises that underlie the debate about the anti-circumvention law.

1. The Access Right in § 1201

First, many users have genuine concerns about the new access right § 1201 provides to copyright owners and the potential ability of rightholders to foreclose legitimate uses of copyrighted works. Although distribution methods and available copying technology created de facto access constraints before digital technologies emerged, there is a very real difference between the physical and technological constraints that once existed and the legal right that § 1201 provides. In a society that values free access to information and widespread availability of works of authorship, the prospect of digital lockup is an alarming one.

2. Section 1201 Is a “Lightning Rod”

It was our observation that § 1201 has become a focus for criticism that results from user dissatisfaction concerning issues that relate in some way to copyrighted works but not necessarily to § 1201 or even to copyright law. Such issues include,

\(^{349}\) See discussion *infra* Part VI.E.6.

\(^{350}\) See discussion *infra* Part VI.E.5.

\(^{351}\) See discussion *infra* Part VI.C.2.
for example, the prices they pay for the works, frustrations concerning license terms, their own budgetary constraints and, in the last few years, concerns about the duration of copyright.

3. Polarization

There is a lack of constructive discourse on the true scope of the problem and how to address it, in large part because the views in the copyright field are highly polarized. On the one hand, critics of anti-circumvention laws describe the law’s supporters as “Hollywood and its allies” and the DMCA as a “guild monopoly.” Copyright owners are cast as money-hungry businesses trying to extract the maximum possible payment for every conceivable use of their works, seeking at every turn to thwart the fundamental goal of copyright—to benefit the public. Some critics are unwilling to acknowledge that digital copying and transmission poses any significant economic threat, rationalizing that piracy has always been inevitable. To the extent there is infringement, they ascribe the problem to “copyright industries” managed by Luddites who refuse to adopt the new business models (details usually unspecified) that will make them deserving of compensation by users.

On the other hand are the law’s supporters, authors and copyright owners who perceive themselves as beset on all sides by “pirates” who want to copy and distribute their works without payment. They acknowledge that fair use exists (at least in the abstract) but regard the vast majority of those who seek to copy without authorization as infringers. Conceding that a small number of fair uses might be impaired by TPMs, they see this as a necessary price to pay by a public not sufficiently grateful for the works they create and make available with new distribution mechanisms.

Neither “side” will readily concede the legitimacy of the other’s concerns. One of our roundtable participants characterized the debate as a “battle of the specters”—users see the specter of copyright owners locking up all works so that no one can use them, even for scholarship, and copyright owners see the specter of their works freely distributed on the internet. Users do not see the copyright owners’ specter as something to worry about, the roundtable participant feared, though in his view the copyright owners’ specter of works freely available on the internet was becoming a reality faster than digital lockup. Many users, however, would dispute that.

353. Samuelson, supra note 9, at 5. On the other side, according to Samuelson, were “Silicon Valley and its allies,” though she points out that those allies include librarians and educators.
4. Exaggerated Perceptions of User Privileges

An exaggerated perception of the scope of fair use and other privileges in the copyright law has contributed to the controversy over § 1201. Some of the privileges users feel they are being denied have not been recognized by Congress or the courts. The extent to which permissible uses have been foreclosed is exaggerated, because the scope of permissible uses is exaggerated. Users' chagrin at the possible effects of § 1201 is based in significant part on uses they would like to make rather than uses they are legally entitled to make.

a. Fair Use

Transformative uses—uses that build on or add to the original—are at the heart of the fair use doctrine.\(^{355}\) New technologies such as the photocopy machine, the video recorder and the computer have enabled users to make complete copies of works easily and cheaply. These “consumptive use copies” are made for the convenience of the user (and sometimes her family and friends) merely to enjoy at a later time or a different place or upon the occurrence of a particular contingency.\(^{356}\) Some consumptive use copying is privileged, such as in-home copying of broadcast television for later viewing,\(^{357}\) copying sound recordings pursuant to § 1008 and making backup copies of computer programs.\(^{358}\) There is, however, no general private right of copying for noncommercial use. Nor is there an automatic right to copy even for purposes favored in the statute, such as education, scholarship or research.\(^{359}\)

Among the activities users have sought most vigorously to preserve in the name of “fair use” are consumptive uses: the making of backup copies, ostensibly for archival purposes, and “space-shifting,” which involves making multiple convenience copies of a copyrighted work for use in different locations. But there is no recognized privilege to make backup copies of all types of copyrighted works or even of all works in digital form.\(^{360}\) The copyright law provides for archival

---

356. See discussion of consumptive use copying in Jane C. Ginsburg, Authors and Users in Copyright, 45 J. COPYRIGHT SOC'TY 1 (1997). But see Martin Senftleben, Copyright, Limitations and the Three-Step Test 298-99 (2004) (disputing the distinction between consumptive and transformative uses, since the “consumptive users” of today may be the authors of tomorrow).
360. See Recommendation of the Register of Copyrights, supra note 149, at 106 (no court decisions support claim that backup copies of audiovisual works are fair use); U.S. v. Elcom, Ltd., 203
copies only in specific cases. For example, § 117 permits backup copies of computer programs, and § 108 permits library archival and preservation copies.

Similarly, there is no established fair use privilege to make additional copies of a protected work for “space-shifting” purposes, such as for use at another location or on another platform. The Audio Home Recording Act (“AHRA”) contains a privilege to make analog and certain digital copies of musical recordings, but due to its narrow definitions, works copied by means of computers do not qualify for the AHRA privilege.361 No court has concluded that the fair use doctrine supports a general space-shifting privilege.362

Users argue that the Supreme Court’s decision in Sony Corp. of America v. Universal City Studios, Inc.363 supports a conclusion that making archival or space-shifting copies qualifies as fair use. But as Register of Copyrights Marybeth Peters has explained,364 such claims are based on a “misreading” of Sony. The Sony case held that time-shifting was fair use because it merely enabled a viewer to see a work he had been invited to see for free at a later time. There was no demonstrated market harm, actual or potential. The Court did not consider whether other activities related to home taping activities, such as taping pay television, creating a library of recorded programs or distributing the recordings, qualify as fair use.

Even more troubling to some users is the prospect that not all fair uses in the analog world will necessarily be preserved in the digital world.365 Historically, some types of uses have been regarded as fair because of “market failure”: they were “technically infringing, but too expensive and complicated to prohibit” in the absence of an effective licensing mechanism.366 However, as digital rights

F. Supp. 2d 1111, 1135 (N.D. Cal. 2002) (no generally recognized right for users to make a backup copy of a protected work other than a computer program).

361. The AHRA provides, inter alia, that consumers may not be sued for copyright infringement based on their noncommercial use of “digital audio recording devices” to make “digital audio musical recordings.” However, to qualify as a “digital audio recording device” a machine must be “designed or marketed for the primary purpose . . . of making a digital audio copied recording” for private use. 17 U.S.C. § 1001(3). Thus, most computers do not qualify as digital audio recording devices, and copies made using such computers—which include copies made via peer-to-peer file sharing software—do not qualify for the § 1008 immunity.

362. See Recommendation of the Register of Copyrights, supra note 149, at 139. The Ninth Circuit’s decision in Recording Indus. Ass’n of Am. v. Diamond Multimedia Sys, 180 F.3d 1072 (9th Cir. 1999), has been cited as the basis for a fair use privilege for space-shifting. See, e.g., Elcom, 203 F. Supp. 2d at 1135. However, as the Elcom court explained, the Ninth Circuit’s discussion related to the Audio Home Recording Act. Accord, Recommendation of the Register of Copyrights, supra note 149, at 130 n.234.


management systems develop to provide easy and efficient licensing mechanisms, treating such uses as fair may no longer be appropriate. 367 “Market failure” does not explain all types of fair use, and efficient licensing schemes will not eliminate all fair use, but they will eliminate the justification for deeming some uses to be fair.

b. The First Sale Doctrine

The first sale doctrine, codified in § 109 of the Copyright Act, provides that the owner of a particular lawfully made copy of a work is entitled to “sell or otherwise dispose of the possession” of that copy. The doctrine is grounded in the right to alienate physical property. 368 It applies to physical copies, which can be in digital or analog form. But it has nothing to do with making reproductions, so it does not permit transmission of an electronic copy over a computer network, which necessarily entails making a copy. 369 Accordingly, there is a privilege under the first sale doctrine to give away or sell a DVD containing an authorized copy of a motion picture, but there is no first sale privilege to electronically retransmit a copy of a motion picture downloaded via Movielink. 370 The Copyright Office has rejected the notion that requiring copies of copyrighted works to be played on a particular platform (e.g., a RealPlayer) interferes with user privileges under the first sale doctrine. The first sale doctrine is, however, potentially implicated when a work is distributed in a physical medium but its use is limited to certain specific machines (e.g., where a copy of a computer program distributed on a CD-ROM can be loaded only on a limited number of computers). 371

367. See, e.g., Am. Geophysical Union v. Texaco, Inc., 60 F.3d 913, 931 (2d Cir. 1994) (“[I]t is sensible that a particular unauthorized use should be considered ‘more fair’ when there is no ready market or means to pay for the use, while such an unauthorized use should be considered ‘less fair’ when there is a ready market or means to pay for the use.”).


369. DMCA SECTION 104 REPORT, supra note 160, at 78-80.

370. Arguing that the copyright law should be “technology neutral,” a number of people have advocated expanding § 109 to allow digital transmission of a work provided the original is deleted so that copies do not proliferate. See, e.g., DMCA SECTION 104 REPORT, supra note 160, at 45. Although the copyright law is in general technology-neutral, the first sale doctrine is not. It pertains to physical copies and is grounded in the common law principle against restraints on the alienation of tangible property. Id. at 20. The Copyright Office considered proposals to amend the first sale doctrine to permit digital transmission of copies in a study pursuant to § 104 of the DMCA, concluded in 2001. The Office declined to make such a recommendation for two reasons. First, it found that the analogy often made between digital transmission and physical transfer is inapt. Digital transmission can substitute for a large number of copies since time, space and cost present no barrier to distribution. Second, it concluded that “forward and delete” technology that would avoid proliferation of copies is not currently in use, nor does there appear to be consumer interest in it. Id. at 96-101. If forward and delete technology were available and widely implemented, so that a “digital first sale” doctrine did not result in a proliferation of retention copies, it might be appropriate to reexamine this conclusion. However, any digital first sale doctrine would have to be subject to contractual limitations on access to and use of copyrighted works to avoid undermining conditional access distribution models.

371. See discussion infra Part VI.E.4.
5. The Meaning of "Access"

There are fundamental differences in views as to what it means to have "access" to a work, and whether or not pay-per-view is desirable. Access can be considered the ability to experience or apprehend a work—in other words, to view, read or listen to it.\textsuperscript{372} Some of the broad claims DMCA critics make about users being deprived of access to works equate access not with the ability to experience a work but with the ability to obtain a work free of any restrictions as to duration, scope or conditions of use, or as to the type of platform on which the work can be used or played.

The latter interpretation of access is too broad to provide a meaningful evaluation of the impact of § 1201 or of the necessity for circumventing controls. Consumers are not, for example, denied access to DVDs in any meaningful way merely because use of DVDs is restricted to authorized playback devices, when those devices are readily available in the marketplace.

That interpretation is also at odds with the goals of the DMCA, which was designed, among other things, specifically to enable new forms of distribution such as pay-per-view by giving copyright owners tools to prevent circumvention of access controls. The House Commerce Committee Report explained:

\begin{quote}
[A]n increasing number of intellectual property works are being distributed using a "client-server" model, where the work is effectively "borrowed" by the user (e.g., infrequent users of expensive software purchase a certain number of uses, or viewers watch a movie on a pay-per-view basis). To operate in this new environment, content providers will need both the technology to make new uses possible and the legal framework to ensure they can protect their work from piracy.\textsuperscript{373}
\end{quote}

In other words, providing copyright owners with the ability to preclude unlimited access was a goal of the DMCA, not just an unforeseen and unfortunate consequence.\textsuperscript{374} Pay-per-use models often are access-enhancing, since they afford users the opportunity to read, view or experience the materials they seek without imposing the costs of an unlimited access option.\textsuperscript{375} A number of new access-enhancing products and services have been introduced since the DMCA became law, such as the popular iTunes and other new music subscription services\textsuperscript{376} and Movielink, CinemaNow and SoapCity for internet delivery of movies and


\textsuperscript{374} Conditional access models are often referred to as "pay-per-use" although there are many conditional access arrangements that do not require payment for each use, but allow use for a specified period of time, use for a number of views. use during the period one is enrolled in an institution and so on.


television programming. 377 Those products rely on and were enabled by TPMs. It is too early to tell whether the DMCA will ultimately be successful in achieving the wide range of consumer options for accessing and enjoying works that its drafters envisioned. However, indications so far are that it has benefited consumers by encouraging copyright owners to make their works available at a variety of different price and convenience points.

As we discuss further below, requiring that initial authorized access must yield unlimited use would make conditional access business models, including pay-per-use, impossible to maintain. All access would have to be conditioned on payment of the "unlimited access" price, 378 depriving users of the opportunity to obtain limited use copies at a lower price.

6. Other Benefits of Technological Controls

The discussion of technological protections often focuses on the use of such controls solely to extract payment or limit copying. However, TPMs are not only use-limiting but can also be use-facilitating. Our roundtable discussions with academics and academic publishers focused less on the commercial aspects of TPMs than on the potential role of TPMs in protecting the integrity of works. Participants emphasized their need to know if a work such as a scientific article came from a trustworthy source and to know whether and how works may have been changed or modified. Ensuring credit—and, to a lesser extent, payment—to an author whose work is used was also a concern. The participants saw technological protection as a means to address concerns about integrity and attribution.

TPMs can also be use-facilitating when they function as part of a digital rights management system that provides an efficient licensing mechanism. Not all uses are privileged: sometimes a user's contemplated use is beyond the scope of fair use, or it is sufficiently doubtful that the user would choose not to proceed without permission. 379 In such cases, absent a quick and efficient means of licensing, the user will choose not to use the preexisting work. Facilitating licenses and permissions where they are necessary is potentially an important function of TPMs.

C. ALTERNATIVES TO SECTION 1201

We consider below a number of possible approaches to remedy the perceived

---


378. See Recommendation of the Register of Copyrights, supra note 149, at 92 (If subsequent controls could be circumvented once initial lawful access was obtained, "[a]ll loans, rentals, or conditional access would be required to be priced at the same as the full sale price of the work, since users would be free to circumvent the access controls that enforced limitations as to time and scope.").

flaws in § 1201.

1. Exempt Circumvention for Any “Legitimate Purpose” or “Non-infringing Use”

   a. Background

   Since the anti-circumvention legislation was first proposed in the Green Paper, concerns have been raised that protection for TPMs would jeopardize users’ privileges, since TPMs cannot imitate the nuanced exceptions, such as fair use, that the copyright law provides. As Kamiel Koelman puts it: “[I]t appears to be impossible to reconcile an effective restriction of technological measures with (all) the limitations on copyright. Technology—at this stage—is simply too crude to accommodate all the subtleties of the law.”380 The Copyright Office rulemaking procedure was designed to provide a “failsafe” mechanism to enable fair use, but some have questioned whether this mechanism is sufficient.

   Perhaps the most commonly advanced solution to the DMCA’s flaws is to amend the law to permit circumvention of access controls for any “legitimate” or “non-infringing” use.381 Such purposes would encompass any user exemption or privilege available under the Copyright Act. Usually this proposal is accompanied by a corollary proposal, to change the anti-trafficking provisions to allow circulation of devices to enable circumvention of TPMs for legitimate or non-infringing purposes.382

   Proponents of a broad exemption argue that fair use is an essential part of copyright (indeed, some argue, a constitutionally mandated part) from which society derives great benefit. In their view, technological controls should not prevent someone without authorization from reading or browsing works, making it impossible for them to extract ideas or information or to exercise the range of fair uses—commentary, criticism, research, scholarship and so on.383 Even a user with

381. Professor Pamela Samuelson, who wrote one of the earliest and most comprehensive articles supporting such an exemption, posits a number of legitimate reasons for circumventing a copyrighted work besides those specifically enumerated in the statute. She acknowledges that courts may find other ways to reach “just results” in such cases but nevertheless argues for a broad “legitimate purposes” exemption in § 1201 “so that courts will not have to thrash to reach appropriate results.” Samuelson, supra note 9, at 28.
382. Id. at 29-40; see also Jason M. Schultz, Taking a Bite Out of Circumvention: A View from Librarians and Educators, Mich. Telecomm. & Tech. L. Rev. 1 (1999/2000); Pete Singer, Mounting a Fair Use Defense to the Anti-Circumvention Provisions in the Digital Millennium Copyright Act, 28 Dayton L. Rev. 111 (2002). Some have argued that the fair use exemption was imported into § 1201, based on § 1201(c)(1). See, e.g., Lunney, supra note 354, at 846. However, the courts have rejected this argument. See, Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 321-23 (S.D.N.Y. 2000), aff’d sub nom. Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001). A fair use exemption is impossible to square with the structure of the statute, including the rulemaking proceeding, and the legislative history.
383. “Fair use” is used in this section for ease of reference and embraces as well other uses specifically permitted by the Copyright Act, such as archiving under § 108, backup copies of computer programs under § 117, etc.
initial lawful access may be limited in terms of the scope (for example, the user may have access to some but not all of the materials in a database), duration or nature of the access (for example, the user may be permitted to view or listen to works but not to reproduce them).\footnote{384} 

The lack of available devices for circumventing access controls and copy controls exacerbates the problem. These restrictions, taken together, limit not only "traditional" fair use privileges but also such activities as time-shifting, "space-shifting" and making backup copies and copies to share with family and friends.\footnote{385} Critics contrast this regime with the analog world, where, once one acquired a copy of a work, one had unlimited access to it and the ability to transfer it to another. They see access controls as creating an unprecedented new right that will lead to "digital lockup" and create a society in which users will have to pay each time they view a copyrighted work.\footnote{386}

From this perspective, a broad exemption from § 1201—for "any legitimate purpose" or "any non-infringing use"—will ensure that the traditional rights users have long enjoyed can continue to flourish in the digital world.\footnote{387} This is the premise of two bills pending in Congress, H.R. 107 and H.R. 1066, discussed below.

But is a fair use exemption as good an idea as its supporters claim? Those who advocate such an exemption often fail to address the fundamental—and legitimate—concerns that underlie the legislation: how do we protect works in digital form from unauthorized copying and distribution and preserve the incentive to invest effort and resources to create them? Authors are not just crying wolf: the enormous popularity of file-sharing programs like Kazaa suggest that unauthorized copying (certainly as to some kinds of copyrighted works) has become common and that many users of such programs do not care whether the works they copy are protected by copyright or not.\footnote{388} Some piracy has always been a cost of doing business, but there comes a point at which it is realistic—and unfair—to expect paying customers to subsidize widespread free use.

As author Mark Stefik points out:

Arguments about fair use for digital works sometimes tacitly (and incorrectly) assume that publishing risks in the digital medium are similar to those in the paper medium. However, while it is, as discussed earlier, unlikely that an infringer will make and


\footnote{385}{But see discussion supra Part VI.B.4.}

\footnote{386}{See, e.g., Laura N. Gasaway, \textit{Anti-Circumvention: A View from Librarians and Educators, in Adjuncts and Alternatives to Copyright: Proceedings of the ALA! Congress June 13-17, 2001 103 (Jane C. Ginsburg & June M. Besek eds., 2002); Siva Vaidhyanathan, Copyrights and Copywrongs 177-79 (2001).}


\footnote{388}{See, e.g., Lee Rainie \textit{et al., The State of Music Downloading and File-Sharing Online} (April 2004), at http://www.pewinternet.org/pdfs/PIP_Filesharing_April_04.pdf; Mary Madden & Amanda Lenthart, \textit{Music Downloading, File-Sharing and Copyright} (July 2003), at http://www.pewinternet.org/pdfs/PIP_Copyright_Memo.pdf.}
distribute thousands of paper copies of a work, he or she can copy and mail a thousand digital copies with a single keystroke at no expense whatever. In other words, publishers who granted unrestricted access to each and every anonymous user on the basis of fair use would routinely risk the loss of their copyrighted assets.\footnote{389}

It is commonly suggested that copyright owners simply adopt "new business models" to solve their problems, but these suggestions are notably short on specifics as to how new business models can meet consumer expectations and still provide a return sufficient to warrant investment.\footnote{390} New business models may be part of the answer, but they will not eliminate the need for § 1201. Even new business models may need TPMs to preserve their benefits for authorized users by keeping out free riders.\footnote{391} The problem is more acute if the new business models have smaller profit margins.\footnote{392}

\textit{b. Fair Use and Access Controls}

Should users be entitled to bypass access controls to make a fair use? There has never been a right to gain access to copyrighted material in order to make fair use of it. There is no right to break into a locked room to use a reference book kept there; no right to enter a movie theatre to see a movie in order to write a review; and no right to hack into a database to get access to materials maintained there—whether or not protected by copyright. There’s not even a right to stand in bookstores or at newsstands to read works there as a substitute for purchasing them (though frequently there is an opportunity to do so). In the analog world, people frequently have broad, if not unlimited, access to works, but that access is usually obtained by paying a price (purchasing a book, for example)—though that price

\footnote{389} Mark Stefik, The Internet Edge 96-97 (1999).
\footnote{390} See, e.g., Editorial, \textit{Face the (Digital) Music}, \textit{Wall St. J.}, Dec. 2, 2002, at A18. As Lionel Sobel has observed: “It is one thing to say a new model is necessary. It is quite another to suggest how that model might work. A general description of how a new model may work is not enough... [t]he devil is in the details.” Lionel S. Sobel, \textit{DRMs as an Enabler of Business Models: ISPs as Digital Retailers}, 18 \textit{Berkeley Tech. L.J.} 667 (2003).
\footnote{391} See Sobel, supra note 390, at 669 (“DRM [Digital Rights Management] appears to be at the foundation of whatever business models will actually succeed in the digital age.”). See also Digital Communications Council, Committee for Economic Development, \textit{Promoting Innovation and Economic Growth: The Special Problem of Digital Intellectual Property} 35 (March 2004), at http://www.ced.org/docs/report/PDF (“... some forms of digital rights management are likely to be part of the solution to today’s controversy.”). New business models such as iTunes and MovieLink rely on TPMs, and lack of effective TPMs can affect the features provided to users. For example, Apple’s iTunes originally contained a feature known as “Rendezvous” that permitted customers to let friends listen to but not download their music. When hackers began offering programs like “iLeach” and “iSlurp” to enable others not just to listen but also to download—effectively permitting the streaming of music over the internet—Apple responded by disabling the Rendezvous feature (however, still permitting iTunes to be used on a user’s local area network at home or at work). Neil Straus, \textit{Apple iTunes Music Store Bears Fruit}, \textit{San Diego Union-Trib.}, June 2, 2003, at C3.
\footnote{392} Consider, for example, music downloads. A customer who once might have purchased a $12.00 CD might now purchase only three or four songs at $0.99 each, for a total price of $3.96. Assuming that $0.70 per song goes to the recording company, there will be a significant drop in revenue (and, in all likelihood, in profits).
may not always have been apparent to the end user, who may have obtained a copy from a school or library. Some have argued that access controls are a substitute for de facto limitations on access that long existed due to technological limitations on copying.\textsuperscript{393}

Many critics of § 1201 concede there is no right to bypass access controls to gain access where no payment has been made\textsuperscript{394} but complain about controls that limit subsequent access. They seek an exemption to permit circumvention of controls whenever a user has lawfully obtained a copy of the work.\textsuperscript{395} H.R. 1066, for example (discussed in more detail below), provides a right to circumvent technological controls on a lawfully obtained copy or a lawfully received transmission of a work. Is it appropriate to mandate that once a copy, or lawful access to a copy, is obtained, no limits may permissibly be placed on that access, other than that the material cannot be infringed?

A fundamental goal of § 1201 was to increase the options available to consumers, in terms of choice and convenience, and allow those who neither need nor desire unlimited access to obtain more limited use at a lower price. In this respect, the promise of the DMCA is just beginning to be realized. Recently we have begun to see online movie downloads for a fraction of the cost of purchasing a DVD, a range of online music delivery services, experimentation with disposable DVDs and so on.\textsuperscript{396} These are positive, user-friendly developments. However, a rule that essentially mandates unlimited access upon initial lawful access eviscerates the protection on which such models are based. As Professor Jane Ginsburg has observed:

The whole point of digital delivery, whether online, or in a limited-play freestanding package like our hypothetical DVD [that only allows three plays], is to permit price discrimination of a kind that consumers should find attractive. If the revised copyright law insists on treating these deliveries like exhaustion copies [over which


\textsuperscript{396} See Grover & Green, \textit{supra} note 377 (movies and television programming); Schwartz & Markoff, \textit{supra} note 376 (online music services); Amy Harmon, \textit{Penn State Will Pay to Allow Students to Download Music. N.Y. TIMES, Nov. 7, 2003, at A1} (new licensed Napster service funded through student fees will allow students to listen to unlimited songs, copy music files on up to three computers for use while in school or burn them to a CD for permanent use for $0.99 each); Eric A. Taub, \textit{DVDs Meant for Buying but Not for Keeping. N.Y. TIMES, July 21, 2003, at C1}. The disposable DVDs do not appear to be an unqualified success but nevertheless help to demonstrate the range of options being explored. See Katie Dean, \textit{Stores Nix Disposable Flicks}, \textit{WIRED NEWS}, Jan. 29, 2004, available at http://www.wired.com/news/digiewood/0,1412,62083,00.html. Even browsing does not appear foreclosed. See David Kirkpatrick, \textit{Amazon Plan Would Allow Searching Texts of Many Books, N.Y. TIMES, July 21, 2003, at C1} (describing searchable online database planned by Amazon.com including table of contents, first chapters and/or selected pages of works).
the copyright owner has no further control], there will be no point in offering works at
differently-priced levels of enjoyment.397

If access cannot effectively be restricted, then all consumers would have to pay
the price for unlimited access, regardless of whether they seek it. If and when
unlimited access options become unavailable or disproportionately costly—the fear
of many DMCA critics—that issue can be addressed. But, as discussed below, we
have not yet approached digital lockup.

c. The Effect of § 1201 on Fair Use

Does § 1201 “eliminate” fair use, as its critics claim? Uses at the core of the fair
use privilege—such as criticism, commentary and parody, research and scholarly
uses—remain available. As the Second Circuit explained in Universal City Studios
v. Corley, responding to claims that controls on DVDs restricted fair use:

[T]he DMCA does not impose even an arguable limitation on the opportunity to make
a variety of traditional fair uses of DVD movies, such as commenting on their content,
quoting excerpts from their screenplays, and even recording portions of the video
images and sounds on film or tape by pointing a camera, a camcorder, or a
microphone at a monitor as it displays the DVD movie.398

A district court in California rejected a similar fair use argument with respect to
the technological controls on e-books:

[N]othing in the DMCA prevents anyone from quoting a work or comparing texts for
the purpose of study or criticism. It may be that from a technological perspective, the
fair user may find it more difficult to do so—quoting may have to occur the old-
fashioned way, by hand or by re-typing, rather than by “cutting and pasting” from
existing digital media. Nevertheless, fair use is still available. Defendant has cited no
authority which guarantees a fair user the right to the most technologically convenient
way to engage in fair use.399

The courts and the Copyright Office have consistently rejected the notion that
consumers are deprived of fair use when they are relegated to retyping or making
analog copies. Professor Pierre Sirinelli, assessing national laws protecting TPMs,
makes a similar point:

To say that a locked e-book is protected is one thing. To say that the novel the e-book
contains cannot be copied is another. Another version, on paper, of the same work
may exist. A handwritten copy can in any event be made. Similarly, to observe that a
film locked in a DVD is normally impossible to copy digitally is correct. But to assert
that it cannot be copied at all, even though one can use a video recorder to film its
screen output is false.

397. Ginsburg, supra note 365, at 87.
398. Universal City Studios v. Corley, 273 F.3d 429, 459 (2d Cir. 2001). Corley is discussed
supra Part II.C.
National laws attempt to give users zones of liberty. This does not mean they seek to guarantee the most convenient or high quality exercise of that liberty. In one case it is a matter of principle; in the other, one of comfort.400

Thus, the fair use privilege does not entitle a user to get the work in the format most convenient for her purposes. On the other hand, there is a continuum between “inconvenient” and “impossible.” There may well be circumstances in which the exercise of a privilege is so inconvenient as to be impossible, as a practical matter. We address this further in Part VI.E.7.

A common theme in discussions about the DMCA is that the law should respond to user expectations: in other words, if users have come to believe they are entitled to something for free, the law—and the fair use doctrine in particular—should respond accordingly. Register of Copyrights Marybeth Peters has challenged this view: “Consumer expectations are typically asserted and vindicated in the marketplace, not through fair use,” and “in and of themselves are not particularly relevant” to the fair use inquiry.401 She cautioned that “users of peer-to-peer services like Napster are becoming accustomed to the notion that creative works should be provided free without any restrictions on further copying and distribution. Such ‘consumer expectations’ are not only inconsistent with traditional fair use jurisprudence, they are destructive to copyright’s principles and purpose.”402

d. Accommodating Fair Use

Even though claims that fair use has been eliminated are overstated, there remains an area of genuine concern where fair uses cannot be undertaken because of technological restrictions. How should this be addressed? Is it necessary to provide an exemption for all legitimate uses (and to circulate circumvention devices) to accommodate these uses? In a perfect world, an exemption would address and enable only those uses, but this is not a perfect world. Devices are not as nuanced as the law.403 But if devices are widely available, they can be used for infringing as well as non-infringing uses. At that point, as one commentator explains, “[p]erhaps one might then just as well decide not to protect technological measures at all. It appears that the legislator must decide either to maintain the (copyright) limitations on the control that an information producer can exercise over the use of information, or to in effect protect technological measures.”404 In § 1201, Congress chose the latter course, weighing the tradeoffs and concluding that the potential inconvenience to fair uses was outweighed by the enhanced

402. Id. at 5.
403. See Bell, supra note 379, at 577-78.
404. Koelman, supra note 12, at 449.
consumer access that TPMs would enable.

Two bills pending in Congress have taken the former course, both providing a broad exemption from § 1201 for any circumvention that does not entail copyright infringement and a correspondingly broad exemption from the anti-trafficking provisions. Though characterized as providing new exemptions, both bills effectively repeal § 1201.

The first, H.R. 107, allows circumvention of a technological protection measure "in connection with the access to, or the use of, a work, if such circumvention does not result in infringement of the copyright in the work." It would also amend § 1201 to allow the manufacture and distribution of a circumvention device "capable of enabling significant non-infringing use of a copyrighted work." H.R. 107 would replace the more stringent anti-trafficking provisions of the DMCA with the "merely capable" standard articulated in Sony Corp. of America v. Universal City Studios.\(^{405}\) in spite of the fact that Congress expressly rejected the Sony standard in passing the DMCA.\(^{406}\) If the law were so amended, it would be unlikely to keep many devices off the market: it is difficult to imagine a circumvention device that could not in some measure be justified as enabling non-infringing use. H.R. 107 would eviscerate the DMCA's anti-trafficking provisions.

The second pending bill, H.R. 1066,\(^{407}\) would allow circumvention of technological control measures on a lawfully obtained copy or transmission of a work if it is necessary to make a non-infringing use and the copyright owner fails to make available the necessary means to make such use "without additional cost or burden" to the user. It would also permit the manufacture and distribution of circumvention devices if "such means are necessary to make a non-infringing use," the device is designed and produced for that purpose, and the copyright owner has not made such means available.

H.R. 1066's amendment to the anti-circumvention provision might appear on its face to be more limited than H.R. 107, because it allows users to circumvent only if the copyright owner fails to provide the "necessary means" to exercise fair use. However, the qualification that the means be made available "without additional cost or burden" apparently gives users broad ability to circumvent if the available means is not convenient.\(^{408}\) In addition, the requirement that the copyright owner provide "necessary means" to make non-infringing use is ambiguous. Does this mean, for example, the means necessary to make copies, and if so, how many copies? Does this mean that the copyright owner cannot allow streaming (listening


\(^{406}\) HOUSE MANAGER'S REPORT, supra note 68, at 9 ("The Sony test of 'capab[ility] of substantial non-infringing uses,' while still operative in cases claiming contributory infringement of copyright, is not part of this legislation.").

\(^{407}\) Discussed supra Part II.E. The bill contains several other amendments to the Copyright Act as well.

or viewing) for one price, but copying for a higher price? Or viewing privileges that time out, similar to rental?

The phrase “necessary means” evokes the standard in the EU Directive, which compels rightholders to make available to users the necessary means to avail themselves of certain exemptions and limitations to copyright.\textsuperscript{409} In fact, H.R. 1066 is far broader. Under the Directive, if rightholders do not make the means available, the responsibility to do so reverts to the member states, and is not left to individual users. Moreover, the Directive makes clear that at least in some cases, a rightholder can fulfill its obligations by making available the means to make a limited number of copies. The EU’s requirement attaches to a limited number of copyright exemptions—not all non-infringing uses. Also, the EU’s “means mandate” does not apply to “on demand” services.\textsuperscript{410}

In passing the DMCA, Congress recognized that the traditional “infringement remedies” model in which copyright owners rely on lawsuits to remedy and deter infringement was inadequate to protect copyrighted works in the internet environment, where copying and widespread dissemination can occur almost instantly. The DMCA represents Congress’s decision to help copyright owners protect their works by reinforcing barriers to infringement in the form of technological controls. Nowhere is this more apparent than in the House Commerce Committee’s response to a letter by copyright law professors objecting to the “unprecedented” provisions in the DMCA to expand copyright by regulating conduct separate and independent of infringement:

While the Committee on Commerce agrees with these distinguished professors, the Committee also recognizes that the digital environment poses a unique threat to the rights of copyright owners, and as such, necessitates protection against devices that undermine copyright interests. In contrast to the analog experience, digital technology enables pirates to reproduce and distribute perfect copies of works—at virtually no cost at all to the pirate. As technology advances, so must our laws.\textsuperscript{411}

H.R. 107 and H.R. 1066 deliberately reverse the DMCA’s approach, largely restricting copyright owners to traditional infringement remedies.\textsuperscript{412} But using lawsuits to remedy and deter infringement is, if anything, even less viable now than it was five years ago when the DMCA was passed. Infringement has become more common through the use of peer-to-peer file sharing programs and more geographically dispersed as the internet becomes available to users in countries around the world. Infringers can be difficult to identify (a problem compounded by servers that enable anonymous use), and issues of jurisdiction and venue, and the


\textsuperscript{410} Id. The exemption for infringement in the Australian statute also pertains only to a subset of non-infringing uses.


\textsuperscript{412} Adding an intent requirement to §§ 1201(a)(2) and 1201(b) would not be a satisfactory solution, either: once devices are on the market they are available for anyone to use, regardless of the initial distributor’s intent.
expense of litigation create significant obstacles to the "infringement remedies" model. The RIAA's recent experience in pursuing file-sharers demonstrates the limitations of trying to deter or remedy infringement through litigation.413

Then how can we accommodate fair uses? There is no tidy answer, but as explained in Parts VI.D and VI.E below, we believe there are currently enough checks in the system to accommodate fair use, and the means exist to make further accommodations in a manner less all-encompassing than the proposals for "non-infringing use" exemptions.

e. Constitutional Concerns

Critics of § 1201 claim that it violates the First Amendment.414 Principally, they argue that circumvention software is speech, and limiting its distribution is an impermissible content-based restriction. They also claim § 1201's anti-trafficking provisions violate the First Amendment rights of users, who need circumvention devices to exercise their fair use privileges. These arguments have been raised and rejected in Universal City Studios v. Corley (both at the district court level in Reimerdes and at the appellate level in 321 Studios and U.S. v. Elcom).415

Those courts have uniformly held that that circumvention software, though it qualifies as speech, also has a functional aspect. Because § 1201 is directed at the functional rather than the speech component of circumvention software, the statute survives First Amendment scrutiny if it serves a substantial governmental objective unrelated to the suppression of free expression and does not burden substantially more speech than necessary to achieve that objective.416 The courts have had no trouble concluding that § 1201 meets this test.417 The Corley court recognized that the government might have chosen alternative means of preventing unauthorized access to decrypted copyrighted materials but was not required to adopt the least restrictive means.418

The courts have been no more receptive to arguments that barring distribution of
circumvention devices prevents the exercise of fair use in violation of the First Amendment. In *Corley*, the court found insufficient evidence of the effect of § 1201 on fair uses to invalidate the statute based on harm to users’ First Amendment interests. However, it expressed skepticism as to whether fair use was compelled by the First Amendment.\(^\text{419}\) It went on to conclude that in any event, there is no constitutional requirement that fair use be made in the format of the original or in the user’s preferred format.\(^\text{420}\) The *Elcom* and *321 Studios* courts have reached similar results.\(^\text{421}\)

The courts have rejected two more First Amendment challenges: *Reimerdes* held that granting a preliminary injunction against the distribution of DeCSS was not an unconstitutional prior restraint.\(^\text{422}\) And the *Elcom* court rejected defendant’s argument that § 1201 was unconstitutionally vague in violation of the First Amendment.\(^\text{423}\)

In short, none of the First Amendment challenges to the DMCA has met with success.\(^\text{424}\) The courts have interpreted circumvention device distributors’—and users’—First Amendment rights far more narrowly than the DMCA’s critics have. This does not mean that the DMCA is immune from First Amendment challenge but only that the cases that have arisen to date have not been persuasive. A more effective challenge might be mounted in a case where the underlying work is “inaccessible” in the sense of being imperceptible without circumvention. This might occur, for example, where a work is embedded in software.\(^\text{425}\)

2. Audio Home Recording Act Model/Levies

Some commentators have offered the Audio Recording Act (AHRA) as a desirable alternative model to the DMCA’s approach. The AHRA was designed to protect the music industry from the perceived threat posed by digital audio recording devices that could make successive generations of perfect digital copies, which were about to enter the market when the law was passed. Under the AHRA, (a) all digital audio recording devices were required to implement SCMS, a technology that allows an unlimited number of first generation copies but no second generation copies; (b) a levy was imposed on the sale of digital audio

---

419. *Id.* at 459.
420. *Id.* at 458.
424. Other constitutional challenges to the DMCA have been similarly unsuccessful. *Elcom* rejected defendants’ claim that § 1201 was vague in violation of the due process clause. *Elcom*, 203 F. Supp. 2d at 1122-25; *Corley* rejected as “premature and speculative” the argument that § 1201 violates the “limited times” restriction in the Copyright Clause. *Corley*, 273 F.3d at 444. Both *Elcom*, 203 F. Supp. 2d at 1137-41, and *321 Studios*, 2004 U.S. Dist LEXIS 2771 at *46-51, held that Congress had constitutional authority to enact § 1201.
425. In this respect, the facts of *Edelman v. N2H2, Inc.*, 263 F. Supp. 2d 137 (D. Mass. 2003), case, discussed supra Part II.C, would have presented a stronger claim to a constitutional privilege to circumvent than did *Corley* had there not been jurisdictional issues and an existing exemption that appeared to cover the circumvention.
recording devices and media, for the benefit of copyright owners of sound recordings and musical compositions; and (c) consumers were given immunity from copyright infringement suits with respect to certain noncommercial copying of musical recordings.\textsuperscript{426}

In their amicus brief in support of defendants in \textit{Universal City Studios v. Corley}, Professors Yochai Benkler and Lawrence Lessig advocated the AHRA as a technological protection model superior to the DMCA. They argued that the ability to make unlimited first generation copies accommodates fair use and other copyright privileges and thus reduces the burden on free speech.\textsuperscript{427} However, it is unclear how “first generation copying only” would facilitate the exercise of copyright privileges, as Professors Benkler and Lessig envision. If a copy uploaded to the internet was deemed a first generation copy, users could not copy it further. If the internet-available copy were deemed an “original,” users could make first generation copies, but any further copying—even for transformative purposes such as to incorporate excerpts in a critique—would presumably be precluded by the technological protection against second generation copies.

Other commentators have suggested that the AHRA approach is more effective because its technology mandate to equipment manufacturers ensures broader coverage than the DMCA, while its implementation of a single, specific technology allows Congress to achieve a better balance between copyright owners’ and users’ interests.\textsuperscript{428} So far as we are aware, no one else has advocated replacing the DMCA with a wholesale extension of the AHRA to all types of copyrighted works. There are, however, aspects of the AHRA approach in various proposals for reform, discussed below.

The FCC’s “broadcast flag” initiative contains elements of the AHRA model. The broadcast flag technology is designed to protect and promote the distribution of high-definition television programming. Like the AHRA, the broadcast flag initiative mandates a specific mechanism (the so-called broadcast flag), which will enable copyright owners to decide whether to allow transfer of their HDTV programming over the internet. The intent is not, however, to restrict copying. The FCC, in a November Report and Order,\textsuperscript{429} required that, beginning in 2005, all HDTV receiving devices must incorporate the broadcast flag mechanism. There are different technologies capable of implementing the broadcast flag mechanism, and the FCC’s order provides the procedure for qualifying technologies as compliant, a process which the FCC will oversee.\textsuperscript{430} Unlike the AHRA, the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{426} 17 U.S.C. §§ 1004-06.
\item \textsuperscript{427} Brief of Amici Curiae Yochai Benkler and Lawrence Lessig, \textit{Corley}, 273 F.3d at 429 (No. 00-9185), \textit{available at} http://www.eff.org.
\item \textsuperscript{428} See, e.g., Benton Gaffney, \textit{Copyright Statutes that Regulate Technology: A Comparative Analysis of the AHRA and the DMCA}, 75 \textit{WASH. L. REV.} 611 (2000).
\item \textsuperscript{430} \textit{Id.}
\end{itemize}
\end{footnotesize}
broadcast flag initiative does not incorporate a levy system, nor does it provide consumers with immunity from suit for copyright infringement.

Regardless of what the future holds for the broadcast flag mechanism, it is doubtful that a model that requires a specific mandated technology is practical or desirable as a substitute in all copyright fields for the more flexible approach of the DMCA, which contains no mandate (other than with respect to VTRs) and protects a wide range of devices. There is a unity of interest among copyright owners in the television programming area that does not exist across all copyright fields. It is important to preserve a flexible approach that encourages copyright owners and technology providers to experiment with different technologies and provide different levels of protection according to their needs and the realities of the marketplace.

The AHRA is, by many accounts, a failure. It was designed to address a specific technology and is a victim of its narrow definitions. Technology evolved rapidly after its passage, so that the marketplace bypassed digital audio tape and recorders in favor of other, more popular means of distribution (and copying). Today musical recordings are distributed principally on CDs (and increasingly through online music services) rather than on digital audio tape, and CDs are copied and "shared" via personal computers which are exempt from the levy scheme and the immunity provided by the AHRA. The AHRA and its technological protection measures have little relevance in today's market. It is unclear whether the broadcast flag is susceptible to a similar fate (it was recently announced and not yet implemented)—specifically, whether its technology mandate provides sufficient flexibility to accommodate developing technology and new forms of distribution.

Some commentators have suggested AHRA-type levies as a way of responding to digital technologies and high speed communications that threaten traditional distribution models. Professor William Fisher has proposed a "governmentally administered rewards system" for films and musical recordings—an alternative system of compensation that substitutes for copyright rights. Revenues would be derived from taxes, either in the form of an income tax or a tax on the goods and services used to gain access to and copy those works, such as computers, hard drives, MP3 players and ISP access fees. Revenues would be distributed to copyright owners according to the frequency with which their works are used. In exchange, consumers could watch or listen to films and musical recordings without payment. The proposal envisions a registration requirement, and mandatory technology only to the extent necessary to embed or accompany the work with identifying material to permit tracking for assessment of payments to authors.

Professor Neil Netanel has proposed a "Noncommercial Use Levy" to compensate copyright owners for unauthorized peer-to-peer file sharing of their

431. See Recording Indus. Ass'n of Am., v. Diamond Multimedia Sys., 180 F.3d 1072 (9th Cir. 1999).

works. The levy would be assessed on internet access, consumer electronic devices used to copy, download or store copyrighted materials, and storage media. Users, in exchange, would have immunity from copyright infringement for noncommercial copying, distribution, performance and even adaptation of copyrighted works.\(^{433}\) His system would apply to all copyrighted works, and copyright owners would be compensated based on frequency of access. Access data would be collected by ISPs. Netanel’s proposed levy scheme, like Fisher’s, requires technology to enable usage monitoring, but it is unclear whether a specific technology would be required or alternatives would be available.

A detailed discussion of these proposals, or of levies generally, is beyond the scope of this report. However, levies should be considered a solution of last resort. They are not a panacea, as they have many problems of their own. The amount of any levy would be hotly contested. Collection and allocation would be complicated and costly. The Copyright Office and all affected parties continue to struggle to find a cost effective way to allocate fairly the proceeds of existing compulsory licenses.\(^{434}\) Levies generated from the sale of recording media and playback devices that exist in various countries throughout the world have generated divisive national treatment issues.\(^{435}\) Moreover, a levy scheme that would apply across the range of copyrighted works by imposing a compulsory license in place of exclusive rights would violate U.S. obligations under international treaties.\(^{436}\)

In any event, adopting a levy system as either Fisher or Netanel have suggested is highly unlikely at this time. Substituting a right of remuneration for a private right would require a fundamental alteration to the copyright law.\(^{437}\) Such a profound change would be strongly resisted by authors, performers and copyright


\(^{436}\) Under the Berne Convention for the Protection of Literary and Artistic Works, the United States must provide authors with certain exclusive rights, including reproduction (art. 9), public performance (art. 11) and adaptation (art. 12). Article 13 permits compulsory licensing of musical compositions with equitable remuneration but does not apply to audiovisual works (“cinematographic” works). Article 11bis provides copyright owners with a broadcasting right, but article 11bis(2) permits Berne members to impose a compulsory license with equitable remuneration in connection with that right. However, it is doubtful whether a compulsory license can be imposed with respect to primary transmissions by wire, or to “on demand” wireless transmissions. The Agreement on Trade-Related Aspects of Intellectual Property (TRIPs) requires its members (including the United States) to comply with Berne requirements. Thus, a mandatory levy scheme could violate both Berne and TRIPs.

\(^{437}\) By “manageable levels,” we mean that enough users still pay for copies to provide a return sufficient to justify the investment of time and/or financial resources in the creation of works of authorship.
owners. The AHRA, in contrast, had the support of the affected parties.

If, ultimately, infringing copies cannot be confined to manageable levels through some combination of technological, legal and moral constraints, a levy regime may be unavoidable, at least for some types of works or uses. At that point, presumably copyright owners would support a levy scheme, although there would still be significant legal and logistical obstacles to implementing it.

Some computer scientists have predicted that TPMs will inevitably prove ineffective. They contend that technological protection will pose no obstacle to unauthorized use: even if only a handful of people circumvent technological protection, file-sharing networks and technologies (which they refer to collectively as "the darknet") will enable fast and efficient sharing of unencrypted content.438

While the darknet scenario is possible, we think it is premature to conclude that TPMs will inevitably prove worthless or that the majority of users will readily resort to the darknet rather than pay for authorized copies. TPMs were never envisioned to be an insurmountable obstacle to infringement. They do, however, serve an important role in defining the boundaries of permitted use and, coupled with improved educational efforts, can play an important role in limiting infringement. "[E]ven though DRM systems may be cracked, they will serve as speed bumps; most consumers will accept DRM limitations and not use available work-arounds, particularly if they feel that they are getting adequate value for their money—as can be seen from widespread consumer use of DVDs whose protection scheme was cracked several years ago."439

There are many other factors that could affect the likelihood that the darknet scenario will prevail, including the development of "self-help" mechanisms by copyright owners (or law enforcement personnel) to reduce the efficiency of the darknet; the introduction of new modes of distribution less amenable to copying and redistribution; the development of mechanisms to filter copyrighted materials and financial and/or legal incentives to use such filters;440 and the possibility that greater legal obligations will be imposed on distribution of file-sharing software used primarily for infringement.441

3. Regulated Circumvention Devices

Another approach to resolving the conflict between TPMs and users’ privileges is to enable users to obtain and use circumvention devices but regulate the manner in which they can obtain those devices and retain records of the identities of those who seek them. Australia has such a system: it allows users who are "qualified

441. See In re Aimster Copyright Litigation, 334 F.3d 643, 648 (7th Cir. 2003).
persons” to obtain circumvention devices or services. They must, however, first supply a declaration that includes their name and address, the basis on which they claim “qualified person” status, the name and address of the supplier, a statement that the device will be used only for a permitted purpose and specific identification of that purpose by reference to the relevant provision in the copyright law. Not all users’ privileges are embraced within this exemption. It covers reverse engineering and certain uses by libraries, archives and educational institutions and by the government.

Professor Alfred Yen has suggested a regulatory approach to the provision of circumvention devices, modeled on the federal gun control laws. Under his proposal, suppliers of circumvention devices and services would have to be licensed by the Copyright Office or the Department of Justice. Providers could be made accountable with “graduated penalties for irresponsible distribution and misuse” of circumvention technology. Persons seeking circumvention devices would have to provide their name and address and possibly submit to a background check for past transgressions. Circumvention devices could be provided only in face-to-face transactions and only in the form of hardware devices with unique serial numbers that would be recorded and included in any decrypted file produced by the device in the form of a digital watermark or fingerprint. In that way, infringing copies could be traced to the person who obtained the circumvention device.

Professor Yen’s proposal is problematic in many respects. One cannot help but question if the federal gun control model is successful enough to warrant serving as a model. Even if authorized gun dealers comply with restrictions, subsequent transfers undermine the system and have the potential to do so in Professor Yen’s model as well. Moreover, his proposal covers only hardware devices and face-to-face transactions, which is likely to make it unsatisfactory to those who seek a broad DMCA exemption for devices to enable fair use. Nevertheless, while one can take issue with various aspects of Professor Yen’s proposal, it is a constructive effort to find a middle ground in this difficult area.

Effective regulation of circumvention devices requires collecting and maintaining information about the identity of the putative fair user for tracking purposes. Some commentators have expressed concerns about the use of such information and the possibility that it will impinge on users’ privacy rights. They claim, among other things, that such information gathering will chill users’ ability to read and make other uses anonymously. Professors Dan Burk and Julie

442. See discussion of Australian law supra Part III.B.
443. However, as Professor Sirinelli has observed: “Everything depends on the user’s declarations.” A user might, for example, keep the device and use it for other purposes. The supplier would not be liable, nor the end user, if the declaration was not intentionally false when made. “One may therefore wonder how much protection this regime in fact accords to technological measures.” Pierre Sirinelli, supra note 400, at 384, 403.
445. Id. at 687.
Cohen have proposed a more modest form of regulation of circumvention devices.\textsuperscript{447} They suggest a “key access for fair use” in which keys would be held by a trusted third party. Users who want to exercise fair use would apply for and obtain a key. This could be done through a simple online procedure; no evaluation of the legitimacy of the application would be made.\textsuperscript{448} An agent would keep records of the keys under strict conditions to protect users’ privacy. Users’ identities could be revealed only pursuant to court order and only upon a showing of “actual piracy, as distinct from garden variety infringement or arguable fair use.”\textsuperscript{449} The keys would be copy-protected.\textsuperscript{450} By implication, each key would be unique so that copies made using the key could be traced to it.

The “key access” approach would not limit unauthorized access or use, since access could be obtained for the asking. Under this scheme, protection for technological controls would be reduced from an independent claim to an “aggravated infringement” cause of action in which the key access mechanism facilitates proof of the aggravated nature of the offense. Moreover, unless there is an enforceable means of restricting transfer of the keys, they serve no useful purpose.

All of the regulated circumvention device models have certain common factors. They require advance planning for fair use and entail expense to set up and manage the system. Professors Burk and Cohen attempt to minimize these factors, but the level of protection their system provides is correspondingly reduced. None of these systems appears to provide an effective barrier to infringement, but only (in some cases) possible assistance in identifying infringers.

4. “Fair Use by Design”/“Fair Use by Mandate”

“Fair use by design” refers to situations in which the design of a technical solution builds in some ability to take advantage of copyright exemptions.\textsuperscript{451} As Charles Clark stated, “The answer to the machine is in the machine.”\textsuperscript{452} While we use the term “fair use by design,” it might more aptly be named “non-infringing use by design,” since some of the schemes might be capable of accommodating other privileges, for example, enabling a backup copy of a computer program under § 117 or library preservation copies pursuant to § 108. A design to enable non-infringing use may be legally compelled, as in the AHRA, but in other cases, the decision of how (and the extent to which) to enable exemptions is left to the


\textsuperscript{448} \textit{Id.} at 63.

\textsuperscript{449} \textit{Id.} at 64.

\textsuperscript{450} Presumably they would also be nontransferable since an authorized after-market in keys would eliminate any advantage to be gained from the tracking.


rightholder, and certain capabilities are built into the business model. While “fair use by design” has its limitations (such schemes can never be as nuanced as our laws), it does have certain advantages. Fair use by design permits spontaneous uses and, depending on the scheme, anonymous uses.

“Fair use by mandate” describes circumstances in which rightholders are directed to enable non-infringing uses but not necessarily given specific instructions as to how that should be done. In some cases, non-infringing uses might be enabled by means of the design of the protection mechanism, but fair use by design is not merely a subset of “fair use by mandate,” for there are reasons other than a legal mandate to implement fair use by design. Similarly, there may be ways other than the design of the protection mechanism to implement fair use by mandate.

The EU Directive employs a “fair use by mandate” approach. Recognizing the tension between circumvention restrictions and copyright exemptions, its drafters left it in the first instance to copyright owners to find a solution. Member states are required to take steps to ensure that beneficiaries of certain copyright privileges that have lawful access to a work can take advantage of those privileges but only if rightholders fail to take “voluntary measures” to do so. The Directive does not limit the technological means a rightholder may use to enable exemptions. Presumably they might include such measures as the ability to make analog copies, non-uploadable copies, providing unrestricted copies in certain designated repositories or for the benefit of a particular group of users, and so on, but this will become clearer as the Directive is implemented and cases arise. Nor is it limited to technological means: it also contemplates the possibility that such measures might include agreements between rightholders and other parties concerned. This might be a realistic option in the case of certain privileges provided to libraries or to people with disabilities.

The Directive expressly approves the “fair use by design” approach. Building in some limited ability to copy appears to be one of the “voluntary measures” contemplated, as evidenced by Article 6(4), which concerns private copying. The Directive provides that measures by the rightholder that allow a limited number of private copies are deemed legally sufficient to satisfy the private copying privilege.

The “fair use by mandate/fair use by design” requirements of the Directive do not extend to works made available via on-demand services. No do they require copyright owners to make the means available to exercise all copyright privileges. This model may not be workable with a statute as vague as fair use.

455. Member states need not provide a private copying privilege, and may do so only with compensation to rightholders. Even if their laws include such a privilege, they are not required to ensure that rightholders provide the means to enable it. Council Directive 2001/29/EC, art. 6(4), 2001 O.J. (L 167/10).
456. The U.S. does have a limited “means mandate” in § 112(e)(8).
What other means might there be of implementing “fair use by design?” Kenneth Dam suggested “fair use buttons” within a work. For example, a “reviewer” button would provide access to an unrestricted copy of a work for review purposes, upon a declaration including identification, a statement of intent and an undertaking that the work would not be used for other purposes. His proposal is only briefly sketched out and raises a number of issues, including the necessity for tracking (for the declaration to be effective, there must be some ability to trace the unprotected copy to the reviewer) and the resulting difficulty in making anonymous uses.

Still, the possibility of incorporating different levels of use for different categories of users is an intriguing one. A teacher, for example, might be given a key to enable her to make a greater number of copies of certain type of works, or portions of works, for classroom use. Such proposals have inherent limitations, however. Fair uses are not limited to specific categories of works or individuals. And rightholders would likely be unwilling to provide keys for certain types of uses: as Dam recognizes, there is not likely to be a “parody” button.

“Fair use by design” techniques are subject to criticism, because they do not accommodate the full range of potential fair use; nor do they reflect the dynamic nature of the doctrine. There is no question that these techniques provide, at best, “rough justice.” In some instances, users will be technologically restricted from making uses that would qualify as fair (or at least restricted from making them in the most convenient manner). In others, however, they may be technologically empowered to make copies that would not qualify as fair use. While a rightholder could theoretically argue that such copies are infringing, it is hardly likely that someone would bring an action over a handful of copies, so over time the “design” may lead to de facto fair use, i.e., create a fair use floor, at least insofar as noncommercial use is involved. Thus, fair use by design techniques have the potential to redefine fair use, at least in some circumstances.

There are some significant advantages to “fair use by design.” Some systems, such as those in which a set number of copies can be made by the user, do not entail the expense of either the key access or the intermediary approach.

Aspects of fair use by design have been incorporated in a number of technological protection systems. For example, the copy control measure mandated by § 1201(k) for analog videotape may not preclude the copying of free broadcast television or basic cable programming. Other systems incorporating “fair use by design” include music downloading services, which permit users to play and download songs, usually to multiple computers and playback devices, the

459. Some people think there should be a fair use “floor” that provides a safe harbor from any claim of infringement. However, fair use is fact-based and depends on, among other things, how much of the work was taken and the significance of the material. Accordingly, it is difficult to establish an appropriate floor for all works and all uses.
460. For a description of online music services and their terms and conditions, see Schwartz & Markoff, supra note 376, at 31.
announced deal between the new Napster and Penn State, which also allows use of songs on multiple computers;\textsuperscript{461} the broadcast flag proposal, which is not intended to preclude any copying but merely uploading to the internet;\textsuperscript{462} CD copy protection that prevents users from uploading songs to file-sharing sites but allows them to make personal use copies;\textsuperscript{463} and databases (e.g., Lexis and Westlaw) that have restrictions on initial access but no persistent controls that preclude copying and forwarding material retrieved.\textsuperscript{464}

Should fair use by design be mandatory? In some manifestations it is, as in § 1201(k), the broadcast flag and the AHRA. However, in these examples it is a quid pro quo for mandated technological controls. Dam counsels against making his "fair use buttons" mandatory. But if fair use by design is not required, what incentive would copyright owners have to implement it? They may be prompted to do so by consumer wishes and expectations, by compromises in the course of negotiations with consumer equipment manufacturers concerning a protection system, or by other economic self-interest (e.g., there may be advertising revenue or other promotional value to permitting a user to forward a news article or other material).

5. Intermediary Model

Another suggestion for resolving the conflict between technological protection and users' privileges is to interpose an intermediary. This model is similar in some respects to the regulated circumvention devices model but provides greater control, since the devices themselves would not circulate. The intermediary would act as a gatekeeper for access to circumvention services or devices, which could be made available for use on an appropriate showing. Such an intermediary, it is posited, would deter use of circumvention devices and services for flagrant violations, presumably because records would permit the copy obtained through circumvention to be traced. The role of the intermediary could be purely ministerial, or, at the other end of the spectrum, the intermediary could have the responsibility to make judgments concerning the merits of the claim to a copyright exemption.

To the extent the intermediary's role is entirely ministerial, i.e., to obtain identifying information from the user and provide the services or access to a device which will yield a clear but trackable copy, the proposal is similar to Kenneth

\textsuperscript{461}. See, e.g., Harmon, supra note 396, at A1 (Napster service negotiated for Penn State students will allow students to listen to unlimited songs, copy music files on up to three computers for use while in school or burn them to a CD for permanent use for $0.99 each).


\textsuperscript{464}. The TEACH Act has aspects of fair use by design, since it authorizes educational institutions to make certain uses of copyrighted works (storage, transmission, performance and display) provided they implement technological controls to restrict other uses (retention or retransmission by recipients). See 17 U.S.C. § 110 (2).
Dam’s "fair use button" approach. But using an intermediary model would give the user greater control than in the Dam model, since the copyright owner would not be able to restrict the privileges that could be exercised. There would be no limitation due to lack of a "parody" button, for example.

At the other end of the spectrum, the intermediary could have a true gatekeeper role, evaluating the claim to an exemption and rejecting applicants who lack a valid claim of privilege. However, an arrangement where claims of privilege are routinely evaluated as a condition of access or copying would be troubling, as it would substitute the view of a fair use arbiter for that of a judge. While entitlement to certain exemptions might be easy to prove, it would not be fair or cost effective to entrust substantive fair use decisions to intermediaries without the consent of the relevant parties. Fair use is highly fact specific, controversial and difficult to determine. People are often critical of technological solutions because they are not as nuanced as the law. But the difficulties in evaluating fair use lie as much in the subtleties of the law and human nature as they do in the limitations of technology.

Is there a middle road for an intermediary? The intermediary could be given some limited responsibility to screen. In Australia, for example, the supplier of circumvention devices and services performs an intermediary role: neither devices nor services can be supplied until a declaration including identification, statement of qualified status and specific exemption to be taken advantage of. Presumably, a responsible intermediary will ensure that the declaration meets the statutory requirements before supplying the devices or services.

A limited gatekeeper function was one of the suggestions that came up in our roundtable discussions for regulating access to circumvention devices. One panel suggested having circumvention devices available, perhaps in libraries, with access regulated by a "notary circumventor" who would require a party wishing to use the device to provide identification and affirm that the use would be for a permitted

465. See the discussion supra Part VI.C.4. At this extreme, the intermediary also resembles Burk and Cohen's "key access" approach except that the devices themselves do not circulate. Burk & Cohen, supra note 447. In the intermediary model, the specific content is released from the controls, but all content protected by the same type of access device is not at risk (as might be the case if devices circulated).

466. The parties could, of course, agree to have claims decided by an arbiter.


468. As Tom Bell has observed, the difficulty in programming fair use into TPMs results not so much from shortcomings in technology as from our inability to understand and articulate the fair use doctrine in detail. Bell, supra note 379, at 587 n.135 (1998). Thus, the substitution of the judgment of an intermediary will not necessarily provide the definitive "fair use" result.

469. But see infra Part VI.C.3 & note 443.
purpose. However, the participants—many of whom were librarians—expressed concern over the prospect of policing use of such equipment beyond a ministerial role; they wanted no part in evaluating claims to exemptions. 470

Finally, while an intermediary model might discourage unauthorized uses, there is also a risk of discouraging legitimate uses. An intermediary system entails financial costs and discourages spontaneous uses and anonymous speech.

D. THE EXPERIENCE TO DATE DOES NOT JUSTIFY A SUBSTANTIAL CHANGE TO § 1201

Section 1201 has been successful in stimulating new means of distribution and promoting consumer choices with respect to a variety of works, particularly sound recordings, motion pictures and television programming, and literary works. It is premature to consider a major change, particularly when the alternative proposals have significant costs and uncertain benefits. Evidence of substantial burdens on copyright privileges is too sparse to justify a major overhaul of the statute now. We have questioned all of our roundtable participants and numerous students about the ways in which their non-infringing uses have been restricted by technological controls, but few had any concrete examples, and the examples they provided were often attributable to factors other than § 1201. Technological protections are not yet as pervasive, or as intrusive, as critics fear. One student’s response was telling: “It’s not that we are restricted in what we do, it’s that we’re afraid we might be in the future.”

Fears of digital lockup that may never materialize should not drive statutory changes. Section 1201 has generated new and exciting opportunities for consumers to experience works in more convenient (and sometimes cheaper) ways. Some uses, such as copying DVDs, are made inconvenient by technological controls, but this is a cost Congress was aware of in passing the law. Overall, the experience under § 1201 so far does not justify changing the law to eliminate independent protection for TPMs and relegating copyright owners solely to infringement remedies. We believe a more constructive approach is to analyze restrictions on non-infringing uses and determine where change is genuinely needed. If and when digital lockup becomes more pervasive, major changes can be considered.

As Professor Paul Goldstein explained in a recent article:

Both the critics and the proponents of anti-circumvention rules have probably overstated the capacity of encryption measures to close off access to literary and artistic works. The point most commonly overlooked is that works published in encrypted form will almost always be available in unencrypted form as well. (Computer interface specifications are the notable exception, which is why they are subject to an exemption.) One reason is simply that paying markets will in many cases continue to exist for works in both forms: indeed, many works, particularly those like mass market newspapers and magazines that are supported by advertising,

470. Section 108(f) of the Copyright Act, for example, provides that libraries will have no liability in connection with unsupervised use of reproduction equipment on their premises, provided the equipment displays a notice that copies may be subject to copyright law.
seem likely to exist only in unencrypted form.

Where copyright owners fail to make works available in unencrypted form, copyright users can be expected to do so through at least two means. First, even if downloading is technologically impeded, unauthorized copies remain inevitable. Anything that can be encrypted can be disencrypted, and the acts and means of disencryption will continue to be as difficult to police as copyright infringement itself. Encryption technologies and anti-circumvention technologies are speed bumbs, not traffic barriers. Second, any visual or aural signal must be seen or heard if a consumer is to be willing to pay for it—at least until the technology arrives that will enable the implantation of these signals directly into the brain. Any signal that can be seen or heard can also be copied, and without circumventing any encryption technology.\footnote{Paul Goldstein, Fair Use in a Changing World, 50 J. COPYRIGHT SOC’Y 133, 146-47 (2003). Of course, once a work is decrypted or its technological protection otherwise removed, fair use defenses apply in connection with its use. See also Center for Democracy and Technology, Implications of the Broadcast Flag: A Public Interest Primer (version 2.0), 7 n.3 (2003), available at http://www.cdt.org (“For the foreseeable future, it will not be possible to stop copies [of movies and other video content] (i) made from unprotected analog television outputs, (ii) made by sophisticated attackers who circumvent protections, (iii) made by those who place a camcorder in front of a television, or (iv) that come from within the studios themselves. It is well understood among technical experts that these ‘holes’ in copy protection schemes exist and will continue to exist for many years.”) (citations omitted).}

Digital lockup is not a present day reality. Most works available pursuant to conditional access arrangements are also available in other forms in the marketplace. For example, many online music services allow permanent downloads as well as streaming, and there are video services that enable permanent as well as temporary downloads. And, of course, unprotected formats remain an option for most works for the foreseeable future.

There are strong market pressures that discourage copyright owners from imposing unreasonable conditions. As one economist explains:

\begin{quote}
[T]he expressed concerns of many critics appear overly fearful. Higher user cost of access—subsuming money, time and effort—has been shown to have a significant depressive effect upon the number of digital articles that readers access. Accordingly, publishers who raise costs, fail to accommodate key user needs, or price gouge on complementary products, will face reduced demand for initial product and a lower resulting market price.\footnote{Einhorn, supra note 375, at 93. See also Perlmuter, supra note 393, at 368, 371 (“Commercial copyright owners are not interested in ‘locking up’ their works. They want the broadest possible dissemination to the largest possible audience.”).}
\end{quote}

Although the term “pay-per-use” can raise the specter of digital lockup, many of the business models that the DMCA enables do not require payment for each use but provide far broader access.\footnote{For example, the LexisNexis Academic product, introduced in 1998, provides 7.2 million students at 1,700 colleges and universities with access to the full texts of more than 5,200 newspapers, magazines and journals at an average cost of $1.59 per student. Within each institution, “a large number of simultaneous users can enjoy unlimited access to all data offered within the service, with no limits regarding connect time, number of searches conducted, or volume of material printed, downloaded or e-mailed.” Use of the service is governed by an access control mechanism, internet protocol (IP) address validation. In other words, the service is accessible only on computers whose IP...}
Although no single factor can ensure that fair use and other privileges are not foreclosed, a host of legal, technological and market factors work together to counter digital lock up and provide a "safety valve" to accommodate legitimate uses.

They are as follows:

- Most works available in digital form will also continue to be available in nondigital form for the foreseeable future.
- Analog means of copying are available. As Professor Goldstein points out, in the ordinary course of use most digital works (other than software) at some point are "in the clear" to be perceived by users and can then be copied in analog form.
- Many fair uses do not require digital (or even mechanical) copying. Fair use flourished for a hundred years before cheap and easy means of mechanical copying became available. People can quote, comment on and parody works without copying them digitally.
- Marketing models for some kinds of works (news websites, for example, many of which are funded by advertising) often permit and even encourage some copying and distribution of copyrighted materials.
- User preferences influence protection mechanisms. Users' desires for enhanced ability to make copies and other uses of copyrighted works are reflected in some of the models on the market. That trend is likely to continue as copyright owners are able to accommodate some types of uses (arguably even those that go beyond fair use) while maintaining protection against unlimited copying and redistribution. These accommodations are made first, because it is good business to make customers happy; and second, because implementation of complex technological protection systems require agreements among content owners, software developers and consumer device manufacturers. The latter have a strong interest in insuring that the devices they manufacture will enjoy widespread consumer acceptance.
- The Copyright Office rulemaking proceeding serves as a "failsafe" mechanism in two respects. It provides exemptions in circumstances where TPMs are a genuine obstacle to non-infringing uses. It also potentially acts as a "check" on copyright owners who know that their works are subject to exemptions if there is no alternative means of exercising non-infringing uses. We explore below in Part VI.E.7 a possible expansion of the Copyright Office's rulemaking authority.
- The courts provide their own "failsafe" mechanism. Courts should and do use equitable principles and common sense to avoid absurd or egregiously
unfair results.\textsuperscript{474} And although Congress did not import copyright’s “fair use” exemption into § 1201, Professor Jane Ginsburg has suggested that courts may not be precluded from developing a “fair circumvention” exemption. “Because fair use is a ‘general equitable defense,’ one might conclude that courts may—given an appropriate fact situation—apply it to § 1201(a) by articulating additional, and highly contextual, limitations on the prohibition on circumvention of access controls.”\textsuperscript{475} None of the fact situations so far have warranted creating such an exemption.

- Congress has the ability to create new exemptions as the need arises.

E. AREAS TO MONITOR

As discussed above, we believe the experience to date under § 1201 does not justify significant change to the statute. Some potential problems in the application of § 1201 have emerged, and others will undoubtedly emerge in the future. In some cases, problems can be resolved satisfactorily by the courts. Others may warrant a statutory amendment, but we believe such amendments should be tailored to address the specific issues that arise.

We consider below several specific areas in which § 1201 is alleged to create obstacles to privileged uses. The existing evidence does not support new statutory exemptions at this time, but some of these potential areas of concern require closer scrutiny, and all of them should be carefully monitored to ensure that means of making privileged uses are not foreclosed.

1. Access to Public Domain Works Protected by TPMs

Section 1201(a)(1)(A) prohibits circumvention of access controls only on “a work protected under this title.” When public domain works are distributed with technological controls, no exemption is necessary, since the statute by its terms does not prohibit circumvention of access controls on public domain works.

Where public domain works are distributed together with works protected under Title 17, protected by the same access controls, there are two conflicting imperatives. On one hand, there is the prohibition on circumventing access controls on copyrighted works; on the other, the public policy in favor of a free and vibrant public domain. A blanket exemption permitting circumvention to access public domain material regardless of the circumstances, however, risks having the tail wag the dog.\textsuperscript{476} All works contain public domain material, which can range from facts, ideas and concepts to the incidental use of a biblical quotation in an e-

\textsuperscript{474} Both Dan Burk and John Therien have suggested that courts use the doctrine of copyright misuse to curb overreaching uses of technological controls by copyright owners. See Dan Burk, Anti-Circumvention Misuse, 50 UCLA L. REV. 1095 (2003); Therien, supra note 414, at 1041-42.

\textsuperscript{475} Jane C. Ginsburg, Copyright Use and Excuse on the Internet, 24 COLUM.-VLA J.L. & ARTS 1, 9 (2000).

\textsuperscript{476} But see JESSICA LITMAN, DIGITAL COPYRIGHT 184 (2001) (advocating a right to circumvent to get access to ideas, facts and other public domain material embodied in protected works).
book or the Mona Lisa in the background of a motion picture on a DVD. Moreover, the public domain encompasses virtually all recorded material not protected by copyright, including such things as words, slogans and short phrases. A blanket exemption could be used to justify circumventing access controls in almost any situation.

Copyright does not allow public domain documents to be “privatized,” nor should § 1201 allow the copyright owner of a compilation to control uses of component public domain works. Although potentially troubling, this appears to be a problem of manageable dimensions, for as long as the public domain material is available elsewhere, the compilation copyright owner cannot exercise such control, and it is not necessary to circumvent.

Problems are most likely to arise in cases of “sole source” public domain material. Where an individual circumvents access controls to facilitate use only of public domain material not otherwise available, the courts are capable of applying the statute to achieve sensible results.477 Faced with a case alleging a violation of § 1201 to obtain public domain works, a court should take into account the nature of the public domain material: the necessity for the circumvention (e.g., is the public domain work readily available elsewhere?478 Is the protected work separately encoded?479) and the good faith of the circumventor (was the protected material left untouched?). If the public domain material is de minimis or embodied in a protected work (e.g., facts or ideas), it should not be grounds for circumvention.

2. Archiving and Preservation

Preservation of digital works is an essential part of creating and maintaining our cultural heritage. Technological controls should not be an obstacle to legitimate preservation activities.

The impact of such controls on archival and preservation functions of libraries and archives is difficult to assess. This issue surfaced in our roundtable discussions, but librarians who voiced fears over the potential effect of § 1201 on archiving activities conceded that their libraries had not (in the absence of TPMs) been doing the archiving activities that they feared § 1201 would preclude. They also expressed frustration about their inability to archive materials to which they had subscriptions for access, but not complete retention copies, and the apparent lack of archiving done by database and journal publishers. The first rulemaking

477. See Landau, supra note 394, at 303 (access to works containing public domain materials should be determined on a case-by-case basis).

478. Free content alternatives are increasingly available, though they may not contain all of the features of commercially published databases. Examples include Findlaw (public domain laws and judicial opinions), Project Gutenberg (public domain books in electronic form), ibiblio (open source software) and PubMed Central (scientific literature). Professor Laura Gasaway suggests that access controls will drive users to these free providers. Gasaway, supra note 384, at 302-06.

479. Such a requirement might be imposed if technologically feasible, and it appears copyright owners are abusing § 1201 or using it to bootstrap protection for public domain works.
noted similar phenomena. In the 2003 rulemaking, the library associations did not seek an exemption for archiving.

One of the four exemptions granted in the 2003 rulemaking related to archiving and preservation. It addresses a situation in which migration of computer programs on obsolete media to a computer system for storage and preservation is stymied, because the programs cannot be used on the new system due to an access control that requires the original media to be present. One can readily imagine other circumstances in which a library or archive has valid possession of a copy of a work but cannot access or copy it for archival or preservation purposes because of access controls.

Archiving digital materials appears not yet to be taking place in a systematic way, but § 1201 is not the sole or principal cause. There are many reasons, including limitations of time and financial resources, uncertainty as to who should undertake responsibility for archiving, the scope of existing copyright privileges related to archiving and preservation activities, restrictions in the license agreements through which the works (or access to the works) are acquired and (possibly) § 1201.

The Library of Congress has begun an initiative to collect and preserve digital content. The initiative, referred to as The National Digital Information Infrastructure Preservation Program (NDIIPP), is an ambitious project through which the Library is trying to ensure the preservation of valuable digital content by stimulating efforts to identify what should be preserved, who should preserve it and how preservation should be undertaken. It is focusing in the first instance on e-books and journals, digital sound recordings, digital television and video and websites. The Library’s plan includes, among other things, designing an architecture and identifying “best methods” for preservation; developing agreements with and guidelines for cooperating institutions to set out what will be collected and by whom; and identifying incentives for creators to deposit content and for institutions to undertake preservation. Among the issues to be explored are the intellectual property implications of preservation activities, including the possible effect of various security and protection devices.

The impact of § 1201 should be considered as part of the entire question of archiving digital works. If necessary, § 1201 should be amended to allow libraries and archives to circumvent access controls that preclude legitimate archiving and preservation activities, and to provide them with the necessary means to do so.

---


481. Their decision not to seek such an exemption may simply reflect the limitations on the Copyright Office’s ability to grant exemptions, as explained at 65 Fed. Reg. 64556, 64572 (proposed Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201).


483. See June M. Besek, Copyright Issues Relevant to the Creation of a Digital Archive: A Preliminary Assessment, in PRESERVING OUR DIGITAL HERITAGE, supra note 482, at app. 6 § 9.0.
3. Defects and Malfunctions

Owners of copies should not be legally precluded from circumventing where, due to a defect or malfunction, a technologically protected copy of a copyrighted work does not function as the copyright owner intended. In the first rulemaking, the Librarian of Congress granted an exemption for “literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness.”\textsuperscript{484} The Copyright Office suggested such an exemption might be appropriate across the range of copyrighted works but concluded that defining a class of works solely with reference to characteristics of its protective mechanism exceeded the scope of its rulemaking authority.\textsuperscript{485}

There was little evidentiary support for this exemption in the second rulemaking proceeding, even though the Office made clear that it was considering each exemption \textit{de novo}. The only evidence presented related to computer programs with damaged dongles (hardware locks), so the Office recommended a more narrowly tailored exemption: “computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete.”\textsuperscript{486}

Why did proposals addressing defects and malfunctions garner so little support in the rulemaking? One can only speculate. Perhaps defects and malfunctions are very rare, but that seems unlikely. Perhaps there was a misunderstanding about the fact that the rulemaking would consider previous exemptions \textit{“de novo,”} or perhaps people who had encountered problems mistakenly relied on others to make their case. It may also be that these problems are addressed by the market; people return or replace defective or malfunctioning media. Or it may simply be that people are circumventing access controls to deal with these problems, but such circumvention is “under the radar”: no harm is done because they merely achieve the access both parties intended, so even if the circumvention is brought to the rightholder’s attention, no action is taken.

In theory, an exemption to allow circumvention in the case of defect or malfunction (i.e., where the access control mechanism does not function in the way in which it was intended to function)\textsuperscript{487} would be appropriate. However, the lack of evidence in the rulemaking suggests that this is not an urgent problem that warrants a statutory exemption at this time. The courts can be relied on to reach fair and just results in the unlikely event that a copyright owner were to bring an action against a consumer who merely attempts to achieve the bargained-for access.

\textsuperscript{484} 65 Fed. Reg. at 64556-74.
\textsuperscript{485} Id. at 64565.
\textsuperscript{486} Recommendation of the Register of Copyrights, \textit{supra} note 149, at 82-189. As the Register’s Recommendation points out, the exemption is limited to dongles that actually malfunction and cannot be replaced, and does not extend to dongles that \textit{might} malfunction. Id. at 37-38.
\textsuperscript{487} 65 Fed. Reg. at 64565. The relevant intent is that of the rightholder, or someone who affixed the protective measure to the work under the authority of the rightholder. A copy is neither defective nor malfunctioning merely because it does not operate on the user’s choice of playback device; the standard should be whether it functions as the copyright owner intended.
4. Combined Access and Rights Controls/"Tethered" Devices

The term "tethered" is used to describe copies of works designed to be used on a particular platform (e.g., DVDs encoded with CSS that can be played back only on a licensed DVD player or drive), as well as copies whose use is limited to specific playback devices (e.g., the particular computer or handheld device on which the copy is downloaded). Platform and device limitations are generally imposed by means of access controls to enable copyright owners to maintain greater control over copying and redistribution of their works. The Copyright Office has characterized tethered works as a subset of a broader category of works whose access controls limit non-infringing post-sale uses (sometimes referred to as "merged" access and use controls).\footnote{\textit{See Recommendation of the Register of Copyrights, supra note 149 at 127-28. Such schemes include, for example, the SCMS system, many videogame technological protection systems, the CSS protection on DVDs, RealPlayer, etc.}}

Users complain that although there is no restriction on circumventing use controls for non-infringing purposes, they are effectively barred from doing so when circumventing use controls requires circumventing access controls. They seek an exemption to allow them to use tethered works on different, less restrictive platforms to enable fair use and other copyright privileges.

The difficulty, however, is that access controls are often an integral part of a protection scheme.\footnote{\textit{See Marks & Turnbull, supra note 251, at 11 ("Encryption of content is key for distinguishing clearly between authorized uses and unauthorized uses, especially in computer environments. No individual or device can decrypt content ‘by accident.’ Hence encryption of content is the keystone of current copy protection efforts.")}.} Technological platform limitations ensure that the playback device will recognize and respond to the technological measures that accompany the copy of the work. Except in certain cases (e.g., analog video recordings under \textsection 1201(k)), consumer equipment manufacturers have no obligation to design their playback devices to respond to technological use limitations. Such use limitations are commonly implemented by developing proprietary technology that limits the playback devices on which the works can run and licensing it to consumer equipment manufacturers who will agree to implement it only on devices that incorporate certain specified use controls.\footnote{\textit{Id. at 15. In order for such schemes to work, equipment manufacturers usually require assurances that sufficient content will be released exclusively in the format being implemented to justify manufacturing devices incorporating the licensed technology.}}

Complaints about access controls that require copies to be played on particular platforms go to the heart of technological protection systems. As the Copyright Office has observed, "Denying copyright owners the ability to limit the device on which a particular digital work will be rendered would necessarily foreclose the most useful protections of the DMCA."\footnote{\textit{Recommendation of the Register of Copyrights, supra note 149, at 130.}} Many users argue these protections should be foreclosed because they inhibit non-infringing uses. This appears to be an area where the interests of copyright owners and the desires users are starkly at odds.
Congress may not have envisioned precisely the kinds of TPMs that are currently available, but there can be no doubt it recognized that access controls might restrict fair use. To address this problem, it chose neither to create an exemption to circumvent access controls for fair use, nor an exemption to do so provided the user has initial lawful access. Instead, Congress designed specific, tailored exemptions as well as the rulemaking proceeding. The rulemaking process provides a means for creating an exemption if non-infringing uses of particular classes of works are shown to be adversely affected by access controls. The proceeding entails weighing a number of factors, including the availability for use of such works.

However, to date the Copyright Office has rejected requests for an exemption to enable platform shifting for fair use and other non-infringing purposes. The principal works for which such exemptions have been sought are e-books, sound recordings and audiovisual works. The Office rejected exemptions to enable platform shifting for such works, principally because the access controls that limit use to particular platforms “encourage copyright owners to provide works in new use-facilitating business models” and because, in most cases, alternative formats for non-infringing uses remain available. The Copyright Office continues to maintain that “there is no unqualified right to access works on any particular machine or device of the user’s choosing.”492

Congress decided, on balance, that it is more important that more people be able to experience more works in more different ways than to insist that all consumers have access to works in the most easily manipulable, retransmittable form. Congress and, accordingly, the Copyright Office have chosen to focus on the enhanced opportunities the new distribution mechanisms provide to consumers to experience and enjoy works they might not otherwise encounter. So long as meaningful outlets for exercising copyright privileges continue to exist, this is a rational approach. Whether nondigital or otherwise unrestricted formats will continue to be available for all works seems doubtful, but that does not mean that non-infringing uses will be unduly burdened, as discussed further in Part VI.D above. For the present, relying on the rulemaking process, which has the potential to provide more targeted relief, is preferable to amending the statute to provide an exemption for circumventing access controls on “tethered works.” Such an exemption is tantamount to creating an exemption to circumvention access controls for “non-infringing purposes” and is problematic for the reasons discussed in Part VI.C.1.

Finally, there is the issue of technological protection measures that restrict copies of works to use on a specific device or a small number of devices. Such controls are most common in the area of e-books, movie downloads and computer software. Critics of the DMCA argue that tethering works in this manner eliminates privileges under the first sale doctrine. Users complain that the controls are onerous, not only restricting the transfer of the copy to another party but sometimes also preventing use on a substitute device if the original fails.

492. 65 Fed. Reg. at 64569.
S. 1621,\textsuperscript{493} currently pending, attempts to prohibit the marketing of copies that cannot be transferred. It would create a "digital first sale doctrine" that applies to "digital media products"—all copyrighted works in digital form, whether distributed electronically or in a physical medium. It allows transmission of a copy as long as the original is deleted.\textsuperscript{494} The bill further provides that digital media products cannot be distributed with protective technology that limits consumer resale or donation to an educational institution. This bill appears to prohibit certain movie, e-book and software downloads that are restricted to only one or a limited number of machines.

Efforts to limit distribution of "tethered" works of this nature are premature. There is considerable likelihood that these issues will be resolved in the marketplace. Services, like Movielink and Sightsound.com, that restrict copies to the hardware upon which they are first accessed nevertheless appear to be precisely the new kinds of distribution mechanisms that § 1201 of the DMCA was designed to encourage.\textsuperscript{495} Many people prefer the convenience of such a service to going out to rent or buy, even with the single machine restriction. It is likely that the market will develop to allow broader use of downloaded works on different devices within the home or family, once copy protection can be maintained.

The e-book market has not been very successful, in part because it has been unable to provide a format and playback device and terms that appeal to a substantial percentage of consumers.\textsuperscript{496} However, there are positive indications that the market for music and e-book downloads is responding to consumer demands for greater flexibility by allowing use of downloaded material on multiple computers or playback devices.\textsuperscript{497} DTCP technology will permit downloads of audiovisual works to be used on different playback devices.\textsuperscript{498} These developments suggest that owners and distributors of copyrighted works recognize that it is in their own interest to provide greater flexibility in using copyrighted works.

In most cases, consumers appear to have alternatives to "tethered" works: in the

\textsuperscript{494} S. 1621 refers to deleting a media product upon transmission, but it applies to works embodied in physical media as well. Presumably one would have to erase or destroy the physical medium on which the work was distributed, as well as any copies uploaded to the user's computer to facilitate transmission, in order to ensure that multiple copies did not result from the transaction.
\textsuperscript{495} See, e.g., H.R. Rep. No. 105-551, pt. 2, at 23 (1998) ("[A]n increasing number of intellectual property works are being distributed using a 'client-server' model, where the work is effectively 'borrowed' by the user (e.g., infrequent users of expensive software purchase a certain number of uses, or viewers watch a movie on a pay-per-view basis). To operate in this environment, content providers will need both the technology to make new uses possible and the legal framework to ensure they can protect their work from piracy.").
\textsuperscript{496} But see Todd Zaua, Even in the Bright Light, an E-Book That's Easy on the Eyes, N.Y. TIMES, Apr. 22, 2004 (new Sony electronic reader is user-friendly and can store hundreds of e-books, which can be downloaded for sixty-day rental for under $5.00 each).
\textsuperscript{497} E.g., Belson, supra note 276 (new Sony Connect service will allow music downloads to a variety of Sony devices; portable devices for video downloads under development).
\textsuperscript{498} See, e.g., Cunard, supra note 286 (discussing the Digital Transmission Content Protection System (DTCP)).
case of movies, renting or buying a DVD to play on any licensed device; in the case of literary works, buying the work in hard copy or audiobook form. Without more evidence of harm, we should refrain from interfering in this dynamic market now.

5. The Replacement Parts Market

Lexmark v. Static Control and Chamberlain v. Skylink, discussed in Part II.C, have prompted concerns that § 1201 might be used by equipment manufacturers to limit competition in replacement parts. However, this is an issue that can likely be resolved by the courts.

Lexmark involved a dispute over Static Control’s manufacture of replacement toner cartridges for Lexmark printers. Before a Lexmark printer will operate, its “Printer Engine Program” communicates with the “Toner Loading Program” in the toner cartridge through an authentication sequence to ensure the presence of an authorized Lexmark cartridge. Static Control developed its SMARTek microchip to permit competing toner cartridges to be used with Lexmark printers. Lexmark sued, charging Static Control with copyright infringement and violation of § 1201. The court found Static Control’s SMARTek chip copied the Toner Loading program in its entirety and violated § 1201 by circumventing the authentication sequence that controlled access to Lexmark’s Printer Engine Program. The court entered a preliminary injunction against Static Control.

If Lexmark opened the door to equipment manufacturers to leverage the protection provided by § 1201 to preserve monopolies in replacement parts or maintenance and repair—as some have claimed—that would be troubling. But the statute appears to incorporate a solution for replacement parts manufacturers, as the Copyright Office observed in the most recent rulemaking proceeding.

Static Control sought an exemption from the Copyright Office through the rulemaking process to permit it to circumvent Lexmark’s access controls. The Copyright Office denied the exemption, explaining that the reverse engineering exemption in § 1201(f) had been available to Static Control and would in fact provide it with greater relief than an exemption from the Librarian of Congress. The Librarian can grant an exemption only with respect to the ban on circumventing access controls. Section 1201(f) also provides a limited

502. Although Static Control’s petition was not timely filed, the Copyright Office took note of the circumstances and initiated another round of comments directed specifically to Static Control’s petition. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 68 Fed. Reg. 6678-79 (Feb. 10, 2003) (to be codified at 37 C.F.R. pt. 201).
503. The reverse engineering exemption in § 1201(f) allows a party who has the right to use a copy of a computer program to circumvent an access control “for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs” provided that information is not readily available and the acts of identification and analysis do not constitute infringement. The reverse engineering exemption also allows, under certain circumstances, the development and distribution of
exemption from the anti-trafficking restrictions. If Static Control indeed copied Lexmark’s program (an issue on which the Copyright Office took no position) it would not qualify for the exemption. But the Copyright Office concluded that it was technologically possible for Static Control to have done so. In other words, the Office declined to create a new exemption for a party that failed to bring itself within the scope of an available exemption.  

Chamberlain v. Skylink involved a replacement transmitter for a garage door opener alleged to violate § 1201 by circumventing the verification measure in the “rolling code computer program” in Chamberlain’s garage door opener. The court granted Skylink’s motion for summary judgment. Although Skylink’s transmitter circumvented Chamberlain’s access control, the court decided that the circumvention was not “without authorization of the copyright owner.” According to the court, Chamberlain implicitly authorized circumvention by failing to notify its customers that they were limited to Chamberlain replacement transmitters in a market in which universal transmitters were commonly sold (including by Chamberlain itself). The court was clearly troubled by Chamberlain’s anti-competitive position, as a business matter as well as a legal matter: “Under Chamberlain’s theory, any customer who loses his or her Chamberlain transmitter, but manages to operate the opener either with a non-Chamberlain transmitter or by some other means of circumventing the rolling code, has violated the DMCA. In the court’s view, the statute does not require such a conclusion.”

The court did not address the reverse engineering exemption, which was apparently not urged by Skylink in its summary judgment motion. Evidence of independent development was disputed, although no copyright infringement claim was made with respect to the program in Chamberlain’s garage door opener.

In any event, these two cases illustrate that Congress—through the reverse engineering exemption in § 1201(f)—and the courts, share a concern about use of the DMCA to eliminate competition in interoperable computer programs or machine replacement parts. Equipment manufacturers should not be permitted to use the DMCA to monopolize the market for replacement parts. If that issue is not resolved by the courts, the statute should be amended to ensure that § 1201 cannot be used to assert control over uncopyrightable machine parts.

---

504. Recommendation of the Register of Copyrights, supra note 149, at 172-83.
506. Chamberlain Group, Inc. v. Skylink Techs., 292 F. Supp. 2d 1040, 1046 (N.D. Ill. 2003). The court attempted to distinguish Universal City Studios v. Reimerdes, discussed supra Part II.C., on the ground that it was not a case that involved implied authority, as plaintiffs there had authorized certain circumvention pursuant to license. Nevertheless, the Chamberlain case is likely to provide fodder for the debate over the role of consumer expectations in the enforcement of § 1201.
6. Reverse Engineering/Encryption Research

a. Reverse Engineering

The exemption in § 1201(f) was designed to ensure that legitimate software developers could reverse engineer to achieve interoperability of computer programs.\(^{507}\) Legislators wanted to preserve fair use/reverse engineering privileges as they existed prior to the DMCA and did so by defining the § 1201(f) privilege to reflect the holding in Sega Enterprises v. Accolade,\(^{508}\) the Ninth Circuit case that established that reverse engineering to achieve interoperability of computer programs was a fair use. As a result, while the fair use privilege as it relates to reverse engineering of computer programs is not restricted in its further development, the privilege to circumvent is limited by the terms of § 1201(f) to the privilege as it existed in 1998.

Computer programs differ from most other copyrighted works in that use in the ordinary course does not provide the user with the ability to apprehend the underlying work. Many computer programs are distributed only in machine-readable form so the human readable source code and many of the ideas it reflects are largely invisible to the user. To access or apprehend the work, the user must reverse engineer the machine-readable code to recreate the source code.

Thus, computer programs present a situation in which technological protection measures genuinely could obstruct “access.” There are strong policy justifications for refusing to allow § 1201 to prevent reverse engineering that qualifies as fair use. One possible solution is to amend § 1201(f) to allow circumvention for any reverse engineering that qualifies as fair use, so that the exemption can develop with the law of fair use. However, we question whether that is realistic, given the controversial nature of this provision and the difficulty of assessing “the law” at any given time, which can vary among circuits. To balance these conflicting concerns, we recommend that the reverse engineering exemption be reviewed periodically by Congress to ensure that the exemption in § 1201(f) for reverse engineering reflects the current scope of the fair use privilege as it applies in respect of reverse engineering. The Copyright Office could be required to report to Congress periodically (e.g., every five years) on the scope of the reverse engineering privilege under copyright law and how it compares to the § 1201(f) exemption.

b. Encryption Research

The effect of § 1201 on encryption research is another area that requires closer monitoring. As the House Commerce Committee observed,

The effectiveness of technological protection measures to protect theft of works depends, in large part, on the rapid and dynamic development of better technologies,
including encryption-based technological protection measures. The development of encryption sciences requires, in part, ongoing research and testing activities by scientists of existing encryption methods, in order to build on those advances, thus promoting and advancing encryption technology generally. This testing could involve attempts to circumvent or defeat encryption systems for the purpose of detecting flaws and learning how to develop more impregnable systems. The goals of this legislation would be poorly served if these provisions had the undesirable and unintended consequence of chilling legitimate research activities in the area of encryption.\textsuperscript{509}

Accordingly, the Commerce Committee recommended a statutory exemption for legitimate encryption research. That exemption was embodied in § 1201(g) of the DMCA, which also required the Copyright Office to report to Congress on the effect of § 1201 on encryption research, one year after the DMCA was passed.

The Copyright Office solicited comments in connection with the study, but since it was conducted before the prohibition on circumventing access controls went into effect, most of the comments were based on speculation as to how such measures might affect encryption research. The Office concluded that there was no "current, discernable impact on encryption and encryption research," and any recommendations would be "premature."\textsuperscript{510}

Since that time, arguments have been raised that § 1201 is having a "chilling effect" on legitimate encryption research.\textsuperscript{511} While the evidence is purely anecdotal, it suggests that a study now would be more timely than it was in 1999-2000. The scope of our study was insufficient to allow us conclude whether a broader exemption is necessary. We recommend that the Copyright Office undertake such a study and, if it finds that legitimate encryption research is adversely affected by the DMCA, make appropriate legislative recommendations to Congress.

7. Enabling Fair Use Without Permitting Circulation of Circumvention Devices

For the reasons discussed in Part VI.D above, technological controls do not generally appear to create unreasonable barriers to non-infringing uses of copyrighted works. If and when it becomes apparent that technological controls are creating significant problems and legitimate uses are stymied for lack of the means of circumvention, we should explore solutions that do not involve distribution of circumvention devices.

One possibility to be considered is a greater role for an intermediary with regard


\textsuperscript{510} U.S. Copyright Office and Nation Telecommunications and Information Administration, Joint Study of Section 1201(g) of the Digital Millennium Copyright Act (2000), available at http://www.copyright.gov/reports/studies/dmca_report.html.

\textsuperscript{511} See Michael Landau, The DMCA's Chilling Effect on Encryption Research, GIGALAW.COM, Sept. 2001, available at http://www.gigalaw.com/articles/2001-all/landau-2001-09-all.html. Some critics have argued that the exemption is too restrictive, because many of the most successful encryption researchers are freelance hackers who are not "engaged in a legitimate course of study" or "appropriately trained or experienced in the field of encryption technology." 17 U.S.C. § 1201(g)(3)(B).
to circumvention services (a "circumvention service provider"). Devices cannot
differentiate between public domain works and protected works, so that any device
capable of defeating technological controls on a public domain work would likely
be barred by the anti-trafficking provisions in § 1201(a)(2) or § 1201(b). However,
a circumvention service provider who offers services in good faith to "free" public
domain works from technological controls presumably could operate within the
statute: the services are primarily designed to provide access to and use of public
domain materials, have no other commercially significant purpose and are
marketed for that purpose. The circumvention service provider, to avoid liability,
would have to reasonably assure itself (or require its clients to do so) that the work
was in the public domain. For many works, it is quite feasible to satisfy this
requirement.

If the public domain work is packaged with a protected work and the same
 technological controls regulate access to both, the situation becomes less clear. As
 a technical matter, the circumvention service provider might be violating the law to
circumvent controls on the protected work to gain access to the public domain one.
But if the circumvention service provider acts in good faith and the circumvention
is not a pretext, a court might excuse it as incidental to getting access to the public
domain material. A circumvention service provider could protect itself—and
possibly avoid a claim that "freeing" the public domain material was a pretext for
gaining access to the copyrighted work—by providing an unencrypted copy only of
the public domain material.\footnote{512}

Could a circumvention service provider bypass access controls to enable a client
to take advantage of one of the exemptions provided in the statute or by the
Librarian of Congress pursuant to the rulemaking proceeding? What about
circumvention of copy controls? Unless the statute is changed, it would appear not.

One could argue that a circumvention service provider could circumvent copy
controls to enable the exercise of copyright exemptions: the anti-trafficking
provision in § 1201(b) is limited to services to circumvent controls that "effectively
protect a right of a copyright owner," and rights under § 106 are expressly made
subject to copyright exemptions, such as fair use. However, this interpretation
suggests that whether a technological control protects a "right of a copyright
owner" will inevitably depend on the intended use of the protected work. This does
not appear to be a persuasive reading of the statute. In any event, a circumvention
service provider would run considerable risk in making judgments about whether a
"right" is implicated based on the intended use.

In theory, the exemptions provided by the Librarian would be more amenable to
the services of a circumvention service provider, since they apply to identified
classes of works rather than to the uses to which those works may be put. Thus,
one possibility for providing greater flexibility is to change the law to grant a

\footnote{512. As discussed supra Part V.I.E.1, this would not be feasible where the public domain material
is embedded or incorporated in a protected work. The anti-trafficking provisions would be meaningless
if a circumvention service provider could strip protection and provide its client with a clear copy of a
protected work under the guise of providing access to the unprotectable facts and ideas.}
limited authorization to a circumvention service provider to facilitate exercise of class-based exemptions pursuant to the rulemaking. But for the reasons explained above, the circumvention service provider approach would have limited utility in the case of other, use-based exemptions.

Another possibility to provide more flexibility for the exercise of copyright exemptions in the face of technological controls would be to amend the law to expand the mandate of the Copyright Office. The rulemaking proceeding was, after all, a "failsafe mechanism," and perhaps, to better fulfill that role, it should be broadened. The principal criticisms of the rulemaking proceeding have been that the Copyright Office has interpreted its mandate too narrowly by imposing too great an evidentiary burden on those seeking an exemption and by refusing to recognize use-based classes.513 The most common criticism, however, is that the exemptions the Office grants are of little genuine effect, because it has no ability to grant an exemption from the anti-trafficking provisions to allow beneficiaries of exemptions to obtain circumvention devices or services.514

The Copyright Office's determination to require a showing of substantial adverse effect before it will grant an exemption appears to be consistent with Congress's intent. The House Commerce Committee, responsible for inserting the rulemaking procedure into the legislation, explained its purpose:

[Diminished access to copyrighted materials that are important to education, scholarship and other socially vital endeavors] could flow from a confluence of factors, including the elimination of print or other hard-copy versions, the permanent encryption of all electronic copies, and the adoption of business models that depend upon restricting distribution and availability, rather than upon maximizing it. In this scenario, it could be appropriate to modify the flat prohibition against the circumvention of effective technological measures that control access to copyrighted materials, in order to ensure that access for lawful purposes is not unjustifiably diminished.515

It would be difficult to reconcile a "less than substantial" showing of adverse effect with the circumstances Congress sought to address.

Indeed, diminished access—that is, reduced ability to apprehend or experience a work—is the common theme in the exemptions the Copyright Office has granted so far. All have involved works that are or will be inaccessible in the sense that they cannot be experienced by users without the exemption. The list of blocked sites in "Net Nanny" type programs, for example, cannot be perceived simply by running the software. The exemption for obsolete or malfunctioning dongles again provides relief where it is impossible to experience the work in the way it was intended. The exemption for works that cannot be run without the original media was designed to facilitate archiving of these works, since without the exemption,

---

514. E.g., Litman, supra note 476.
preservation copies would not be accessible, i.e., perceptible, to users. Finally, the exemption concerning e-books is designed to facilitate access—i.e., the ability to perceive a work—by a particular group of people who do not experience works in the same manner as the general population and would otherwise be deprived of “access.”

The requirement that the exemptions be based on characteristics of the class of works rather than of the user appears to be a reasonable interpretation of what is an obscurely written piece of statutory text.

Broadening the Office’s mandate to authorize it to create a limited exemption from the ban on trafficking in access control circumvention devices to allow beneficiaries to take advantage of the exemptions it creates is another way to make the anti-circumvention laws less onerous, without undercutting them completely by allowing wholesale circulation of devices. The Office could, for example, mandate that copyright owners make available the means to make privileged uses. Perhaps more effectively, it could mandate the particular ways in which copyright owners can make the means available, with input from the copyright owners as to the feasibility and risks of the various alternatives.\footnote{516}

There are various ways in which the means to make non-infringing uses might be made available, such as by providing users with an additional copy or copies of a work or the means to make such copies; or providing them with a means of making or obtaining protected excerpts; or providing them with a means of making unprotected excerpts of a limited number of bits; or by providing them with access to a server through which one could link to (but not download) protected excerpts. (Even the proverbial film student’s thesis might be accommodated in this manner). None of these approaches should be imposed without a careful assessment of the risks as well as the benefits, nor should relief be provided unless legitimate uses are unreasonably burdened.

VII. CONCLUSION

There is no perfect solution to the problem of protecting copyrighted works in the digital environment. Technological controls on copyrighted works affect the ease with which users can exercise privileges. However, requiring that users have unencumbered ability to use works diminishes the protection for copyrighted works and the ways in which they are made available to consumers in the digital environment.

Congress attempted to balance these interests in § 1201. The law involves genuine tradeoffs: Congress made a judgment that technological protection would foster innovation in new content delivery mechanisms in order to provide consumers with a range of new options for experiencing copyrighted works, recognizing that technological controls might diminish the convenience of non-

\footnote{516. In one sense, the e-book exemption granted in the last rulemaking to benefit the visually impaired is a type of means mandate: if copyright owners alter the technological controls to enable the read-aloud function or screen readers on any e-book version of a work, they will satisfy the access mandate, and no circumvention will be authorized.}
infringing uses. So far, the balance that Congress struck appears justified. Section 1201 has provided substantial benefits to consumers by encouraging the development of innovative new business models for delivering sound recordings, motion pictures, books and other copyrighted works to consumers.

On the other hand, there is little evidence at this point that technological controls are preventing privileged uses. Flexibility in the law, the realities of the digital environment and market imperatives appear to be accommodating legitimate uses. Most copyrighted works are available for fair uses, though not necessarily in a form amenable to the most technologically advanced forms of copying, re-manipulation and retransmission. Such limitations, however, are at the heart of the new business models that are emerging in the marketplace.

The reasons that DMCA critics offer for overhauling or replacing § 1201 are essentially the same ones presented to Congress in opposition to the legislation when it was under consideration. Congress took them into account in crafting § 1201. Based on the track record so far, § 1201 appears to be performing largely as Congress had envisioned and should not be overhauled or replaced. The benefits—more works available to consumers at a variety of price and convenience points—are real, and the costs have so far been manageable. It is important to continue to monitor § 1201’s effects and, where problems become apparent, develop specific, focused solutions. At the present time, however, we should allow the new business models enabled by § 1201 the opportunity to continue to flourish.
APPENDIX A

ALAI 2001 SPEAKERS AND PANELISTS

Listed below are the speakers and panelists who made presentations concerning technological protection of copyrighted works at the ALAI 2001 Congress in New York City and their affiliations at the time of the Congress. The titles of their written contributions to the proceedings are included below; those materials are reproduced in Adjuncts and Alternatives to Copyright: Proceedings of the ALAI Congress June 13-17, 2001 (Jane C. Ginsburg & June M. Besek eds., 2002).

TECHNOLOGICAL PROTECTION OF COPYRIGHTED WORKS AND COPYRIGHT MANAGEMENT SYSTEMS

A. OVERVIEW OF TECHNOLOGICAL PROTECTION MEASURES, AND COPYRIGHT MANAGEMENT SYSTEMS

Jeffrey P. Cunard
Debevoise & Plimpton, U.S.A.
Technological Protection of Copyrighted Works and Copyright Management Systems: A Brief Survey of the Landscape

Panel:
Tarja Koskinen-Olsson (session chair)
Kopiosto, Finland
IPR—Content on the Internet

Robert Bolick
The McGraw-Hill Companies, U.S.A.
DOI and eBook Standards

Nic Garnett
InteTrust Technologies, U.K./U.S.A.
Technological Protection of Copyright Works, and Copyright Management Systems

Daniel Gervais
Copyright Clearance Center, Canada
Rights Management Systems in Action: The Key Role of Copyright Collectives

Roland Louski
Info2clear, Belgium
Rights Management Systems in Action: Reprints and Permissions
Kate Wittenberg, Lewis E. Gilbert and David Millman
Electronic Publishing Initiative at Columbia [EPIC], U.S.A.

Universities and Intellectual Property

B. THE MARKET FOR DIGITAL WORKS OF AUTHORSHIP AND THE PROBLEM OF “DIGITAL LOCK-UP”

Professor William B. Cornish (session chair)
Cambridge University, U.K.
Session Chair’s Remarks

David O. Carson, General Counsel
U.S. Copyright Office, U.S.A.
The U.S. Copyright Office’s Anticircumvention Rulemaking

Michael A. Einhorn
Economist, formerly with U.S. Justice Department, Antitrust Division, U.S.A.
Digital Rights Management and Access Protection: An Economic Analysis

Professor Laura N. Gasaway
University of North Carolina, U.S.A.
Anti-Circumvention: A View from Librarians and Educators

Robert H. Kohn
Emusic.com, U.S.A.

C. SITUATING LEGAL PROTECTIONS FOR TECHNOLOGICAL MEASURES IN THE BROADER LEGAL LANDSCAPE

Lise Bertrand (session chair)
Canadian Broadcasting Corporation, Canada

Séverine Dusollier (general reporter)
Centre de Recherche en Informatique et Droit [CRID]
Situating Legal Protections for Copyright-Related Technological Measures in the Broader Legal Landscape: Anti-Circumvention Protection Outside Copyright

Professor Christophe Caron
University of Boulogne-sur-Mer, France
Brèves observations sur la protection des mesures techniques par le droit civil

Elliot N. Turrini
Assistant U.S. Attorney, District of New Jersey, Department of Justice, U.S.A.
U.S. Criminal Law’s Reinforcement of Technological Measures Protecting Property: Where the DMCA Fits In
D. What Is the Appropriate Scope of Copyright in a World of Technological Protections?

1. The New or Evolving “Access Right”

Professor Sam Ricketson (session chair)
University of Melbourne, Australia
The Access Right

Professor Jon Bing (general reporter)
University of Oslo, Norwegian Research Center for Computers and Law, Norway
The New or Evolving “Access Right”

Professor Thomas Hoeren
University of Münster, Germany
Access Right as a Postmodern Symbol of Copyright Deconstruction?

Professor Naoki Koizumi
Sophia University, Tokyo, Japan
The New or Evolving “Access Right” in Japan

Shira Perlmutter
AOL Time Warner, U.S.A.
The “Access Right” in the United States

Professor Alain Strowel
Facultés Universitaires Saint-Louis, Brussels, Belgium
The New or Evolving “Access Right”

2. The Scope of the Prohibition on Circumvention of Access and/or Rights Controls; Exceptions and Limitations

June M. Besek (session chair)
Columbia University School of Law, U.S.A.
Session Chair’s Remarks

Professor Pierre Sirinelli (general reporter)
University of Paris, Panthéon-Sorbonne, France
The Scope of Prohibition on Circumvention of Technological Measures: Exceptions

Kamiel J. Koelman
Institute for Information Law, University of Amsterdam, Netherlands
The Protection of Technological Measures vs. the Copyright Limitations

François Lajeunesse
Bell Canada, Canada
*The Protection of Technological Measures and the Exceptions and Limitations to Copyright*

**Professor Jessica Litman**
Wayne State University, U.S.A.
*The Breadth of the Anti-Trafficking Provisions and the Moral High Ground*

**Maria Martin-Prat**
IFPI (on leave from European Comission), Spain/U.K.
*The Relationship Between Protection and Exceptions in the EU “Information Society” Directive*

**ROUNDTABLE PARTICIPANTS**

Professor Jane Ginsburg and June Besek were moderators of the roundtables conducted in connection with the Kernochan Center’s DMCA study. The following individuals participated in the roundtables, which were conducted primarily in New York, but also in Los Angeles, San Francisco and Palo Alto. Affiliations at the time of their participation are listed for informational purposes, but it was understood that participants spoke in their individual capacities and not on behalf of their organizations or clients.

Daniel Abraham, Graphic Artists Guild
Alison F. Alifano, New York County Lawyers Association
Fritz Attaway, Motion Picture Association of America
Jon Baumgarten, Proskauer Rose LLP
Karen Bornath, Electronic Publishing Initiative at Columbia (EPIC)
Andrew Bridges, Wilson Sonsini Goodrich & Rosati (now with Winston & Strawn LLP)
Mary Case, Association of Research Libraries
Jeffrey Cunard, Debevoise & Plimpton
Joseph J. DiMona, BMI
Lisa Fish, Geology and Geosciences Libraries, Columbia University
Nic Garnett, InterTrust (now with the Simkins Partnership, London)
Laura Gasaway, University of North Carolina, Katherine R. Everett Law Library
Daniel Gervais, Copyright Clearance Center (now at University of Ottawa)
Lewis Gilbert, Columbia University
Jennifer Granick, Stanford Law School
Seth D. Greenstein, McDermott, Will & Emery
Daphne Gronich, Fox Group Legal
Robin Gross, Electronic Frontier Foundation
Leigh Gusts, Council on Foreign Relations
Alice Haemerli, Columbia Law School
Michelena Hallie, Viacom, Inc.
Carole E. Handler, Kaye, Scholer, Fierman, Hays & Handler LLP (now with Thelan Reid & Priest LLP)
James Hoover, Columbia Law School
Henry Horbaczewski, Reed-Elsevier Inc.
Bernt Hugenholtz, IVIR, University of Amsterdam
David Hughes, Sony Music
Bruce Joseph, Wiley, Rein & Fielding
Jared Jussim, Sony Pictures Entertainment
Adria G. Kaplan, Columbia Law School
David Kaplan, Newsweek and book author
Kim Kastens, Lamont-Doherty Earth Observatory, Columbia University
David Kellogg, Council on Foreign Relations
John M. Kernochan, Columbia Law School
Judith Klavans, Columbia University Libraries
Fred Koenigsberg, White & Case LLP
Bob Kohn, Emusic.com
Nancy Kranich, New York University Libraries
William Krepsick, Macrovision Corporation
Silke von Lewinski, Max Planck Institute for Foreign and International Patent, Copyright and Competition Law (Munich)
David Liebowitz, Verance Corp.
Joan Lippincott, CNI
Karen Mayer, Penguin Putnum Inc.
Kent McKeever, Columbia Law School
Jeffrey Mitnick, McGraw-Hill
Jeff Morgen, Friskit.com
Tom Moritz, American Museum of Natural History
Kay Murray, Authors Guild
Jeffrey Neuberger, Brown Raysman Millstein Felder & Steiner LLP
Madeleine M. Nichols, New York Public Library for the Performing Arts, Dance Division
Peter Nolan, The Walt Disney Company
Kaye Pace, Jon Wiley & Sons
Victor Perlman, American Society of Media Photographers
Shira Perlmutter, World Intellectual Property Organization (now with Time Warner)
Charles Phelps, University of Rochester
Mark Radcliffe, Gray Cary
Gloria Rohmann, New York University Libraries
Tom Rubin, Microsoft Corporation
Robert Schwartz, McDermott, Will & Emery
Cary Sherman, Recording Industry Association of America
Clay Shirky, writer
Teri Silvers, Columbia Law School
Neil A. Smith, Limbach & Limbach (now with Howard, Rice, Nemerovski,
Canady, Falk & Rabkin)
Katherine Spelman, Steinhart & Falconer (now with Piper & Rudnick LLP)
Michael Stern, Cooley Godward LLP
Alain Strowel, Saint-Louis University (Brussels), University of Liège and Nauta Dutilh
    (now at Covington & Burling, Brussels)
Lee Tien, Electronic Frontier Foundation
Siva Vaidhyanathan, Department of Culture and Communications, New York University
Frank Wattenberg, Math Forum
Jeremy Williams, Warner Brothers
Kate Wittenberg, Electronic Publishing Initiative at Columbia (EPIC)
Greg Wrenn, Yahoo, Inc.
Lee Zia, National Science Foundation