Stefan Bechtold

The Present and Future of Digital Rights Management – Musings on Emerging Legal Problems

in:
Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump (eds.),
Digital Rights Management – Technological, Economic, Legal and Political Aspects,
Springer, Berlin 2003, pp. 597-654

This article is available online at
http://www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf

TABLE OF CONTENTS

4.6 The Present and Future of Digital Rights Management — Musings on Emerging Legal Problems

Stefan Bechtold[1776]

Abstract: This article presents a roadmap of emerging legal problems in the area of Digital Rights Management (DRM). It argues against adopting fundamentalist viewpoints in the DRM policy debate. In particular, DRM technology is much more flexible than many DRM critics acknowledge. The article covers various problems that are less frequently discussed in legal and policy circles. It analyzes the relationship between DRM, fair use, and innovation, using rights locker architectures, dynamic DRM systems, the Creative Commons project, DRM technology license agreements, and security research as examples. It addresses the alleged dichotomy between DRM and copyright levy systems as well as the implications of DRM for privacy protection. By analyzing various technology platforms, it describes the implications DRM has for competition in platform markets as well as in complementary aftermarkets. Finally, the article assesses recent efforts to standardize DRM technology, both by the private sector (in particular TCPA and Palladium), and by the legislature.

I Introduction

Digital Rights Management (DRM) promises to offer a secure framework for distributing digital content (music, video, text, rare data etc.). DRM enables an electronic marketplace where previously unimaginable business models can be implemented. At the same time, DRM ensures that content providers — particularly copyright owners — receive adequate remuneration for the creation of the content that is distributed over the DRM system. And so, copyright owners lived happily ever after.

So goes the DRM story told by DRM disciples. If one listens to DRM opponents, however, the story sounds very different. In the United States and in Europe, much has been written about how DRM privatizes and replaces copyright law,[1777] how it undermines copyright limitations,[1778] threatens the interests of users and the public at large, inhibits creativity and innovation by unjustly extending intellectual property protection,[1779] how the law and economic anal-

[1776] Research Assistant, University of Tübingen Law School, Germany; Fellow, 2002–2003, Center for Internet and Society, Stanford Law School, USA. The author is grateful to Ross Anderson, Robert Gehring, Brian Hemphill, Kurt Jaeger, Lawrence Lessig, Yuko Noguchi, Roy Pfitzner, Graeme Proudler, David Safford, Tomas Sander, and Florian Wagner for helpful comments.

[1777] See: Lessig (1999): 130, 135; Gimbel (1998): 1683–1684.

[1778] See: Koelman, Helberger (2000): 189–192; Cohen (1998): 472–473; see also: Guibault (2002).

[1779] See: Lessig (2001). See also: The articles from the Duke Conference on the Public Domain 2001 in 66 Law and Contemporary Problems 1–483 (2003); Elkin–Koren, Netanel (2002).

E. Becker et al. (Eds.): Digital Rights Management, LNCS 2770, pp. 597–654, 2003.

ysis by DRM proponents is flawed,[1780] and how anti–circumvention regulations are overbroad and undermine fair use.[1781] And so, this version of the DRM story goes, at the dawn of the third millennium, the world of creativity and cultural production collapsed due to an unfortunate conspiracy of huge commercial conglomerates and biased legislators.

As with many controversial stories, both versions of the DRM story have elements of truth to them.[1782] However, as with many controversial stories, both also include elements of exaggeration and, sometimes, even falsity. Although the author shares most of the mentioned concerns about DRM,[1783] this article does not directly address them. Rather, it focuses on some aspects of DRM that are less frequently discussed in legal and policy circles, either because they have emerged only recently or because they are not as well publicized. Thereby, the article attempts to add several problems to the existing myriad of DRM–related problems.

At the same time, the article attempts to show that it is often futile and sometimes counterproductive to condemn DRM altogether. Digital rights management offers many tools by which some of the problems raised by DRM opponents can be solved. In particular, DRM technology is much more flexible and plastic than some DRM critics acknowledge. As understood in this article, "digital rights management" is a general term for a set of intertwining technologies that may be used to establish a secure distribution channel for digital content. Such technologies include encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamper–resistant hard– and software, key management and revocation as well as risk management architectures.[1784] All these technologies are used to *enforce* certain policies. In addition, most DRM systems also include certain technologies that enable the machine–readable *expression* of such policies, in particular

[1780] See: Cohen (1998).

[1781] See only: Samuelson (1999): 548–549. For some proposals to bring anti–circumvention regulations in accordance with copyright limitations, see: Burk, Cohen (2001); Burk (2003); see also: Foged (2002).

[1782] Actually, a third version of the DRM story exists. According to this version, all the policy discussions about DRM are essentially futile as it is either technically impossible to design a secure DRM system (see: Kelsey, Schneier (1998): 2) or unrealistic to expect DRM to eradicate P2P file sharing networks and other so–called "darknets" (see the Article from *Biddle, England, Peinado, Willman* within this book on page 344). While the author agrees with the second argument, the first agreement ignores that DRM is not only about technological protection. Although it is impossible to design a DRM system that is 100% technologically secure, DRM may still provide a very high level of security, as various technological and legal means of protection (including protection by copyright law, anti–circumvention regulations, usage contracts and technology license agreements) are intertwined in advanced DRM systems. For an analysis of the implications of these intertwining means of protection, see: Bechtold (2002/2003a). In the following, the article assumes that DRM systems are at least partially effective in protecting digital content.

[1783] See: Bechtold (2002/2003a).

[1784] See: Chapter 2 *Technological Aspects* within this book.

rights expression languages (RELs) and metadata.[1785] The specific technologies used vary from DRM system to DRM system. Depending on the particular combination of these technologies, the policy implications of various DRM systems vary greatly as well.

Instead of taking DRM systems as given constants that are exogenous to the policy process, this article joins an emerging scholarship which asks how DRM systems could be altered in a value–centered design process so that important policy and legal values are preserved.[1786] The article does not attempt to provide answers to all the questions raised. Rather, in providing a roadmap of emerging legal problems, it attempts to point to various aspects of the DRM debate that deserve further analysis and discussion. For this purpose, the article may sometimes oversimplify or exaggerate certain technological trends and possibilities as well as speculate about future developments. This is done, however, to stimulate further discussion about what is possible with DRM systems and to scrutinize various DRM characteristics that have been taken as given, unalterable facts hitherto.

The article proceeds as follows. In section II, four aspects of the interrelation among DRM, fair use, and innovation, which are under–represented in current DRM policy discussions, are described. Section III addresses the alleged dichotomy between DRM and levy systems. Section IV touches upon the impact of DRM on privacy protection. Section V analyzes the implications of DRM for competition in the DRM–protected platform market itself and in complementary markets. Section VI assesses recent efforts by the private sector and by legislatures to standardize and mandate DRM technology. Section VII concludes the article.

II DRM, Fair Use, and Innovation

Much has been written about the impacts DRM has on fair use and creativity. In the following section, four areas will be described that are less frequently discussed. As this section will show, DRM may indeed impede fair use[1787] and innovation. However, there are also aspects of DRM which can be used to protect fair use and foster openness and innovation.

[1785] For a general overview of the technologies used in DRM systems, see: Bechtold (2002): 19–145; Rosenblatt, Trippe, Mooney (2002).

[1786] For other examples of this scholarship, see: Burk, Cohen (2001); Cohen (2003); Mulligan, Burstein (2002); Fox, LaMacchia (2003); Erickson (2003). But see: Felten (2003).

[1787] The use of the term "fair use" in this article is meant to cover a broad range of copyright limitations. It is not meant to describe the U.S. concept of fair use in contrast to the more detailed copyright limitations that may be found in the copyright laws of many *droit d'auteur* countries in continental Europe.

II.1 Rights Locker Architectures

With the increasing mobility of people and the increasing spread of communication networks, media consumption patterns change. Formerly, consumers were satisfied if they could listen to music on their record player in their living room. Increasingly, consumers seem to demand that they can access and use their content from any media device they own. Thereby, they could listen to their favorite music at home, in their car, in the subway, at work, in the plane or in a hotel room.

DRM technology attempts to respond to this demand. The idea is to enable consumers to access any content at any time from any device they want in a DRM–protected environment. Such a system could give consumers instant access to the entire world of information and entertainment via their computer, MP3 player, PDA and cell phone, from any place in the world.

"Rights locker" architectures are the technology that promises to make this happen. In a DRM rights locker architecture, content is no longer stored on a particular device the consumer owns. Rather, it is centrally stored on a network server. This server is also a central depository for the permissions to use content which a consumer has purchased.[1788] If, in a DRM rights locker architecture, a consumer wants to listen to some audio content on his computer, the computer does not load the audio file from its local hard drive. Rather, it sends a request (together with some authorization information) to the central server. After the central server has verified the authenticity of the request, it streams the audio file back to the computer. If the consumer wants to listen to the same content on his wireless device a few hours later, the same procedure takes place. In such an architecture, local storage of content becomes unnecessary.[1789]

Rights locker architectures make digital rights portable among various platforms as permissions to use content are no longer bound to a particular device the consumer owns, but to the consumer himself.[1790] They also provide reliable backup mechanisms for such digital rights, as consumers do not have to fear to lose their rights due to hardware failures or by buying a new computer.[1791] Rights locker architectures therefore provide portability and recoverability of digital rights.

While rights locker architectures will not be implemented on a wide scale in the near future, many DRM technology companies are currently working on such systems. Given the limited memory storage of many wireless devices, rights locker architectures may become of particular importance in a future where wireless devices and networks play a role comparable to the Internet as we know it today.

[1788] See: Sander (2002): 66; Feigenbaum, Freedman, Sander, Shostack (2001): 101–104.

[1789] This is an oversimplification, of course. Even in a rights locker architecture, local storage will remain important due to bandwidth limitations, high costs for streaming content in wireless networks and network outages. The article accepts this oversimplification in order to highlight a certain trend.

[1790] See: Sander (2002): 66.

[1791] See: Id.

The current discussion about DRM and fair use is implicitly based on the assumption that consumers have copies of the protected content that are physically stored on devices the consumers own. Under such circumstances, it is reasonable to ask under what conditions the consumer is allowed to copy content from one device to another without the rights holders' permission; it is also reasonable to ask under what conditions the consumer is allowed to forward his copy to friends (as the copyright limitations for private copying and the fair use defense sometimes allow). These questions make sense in a world where data is physically stored on devices that are located in the realm of the consumer.

These questions become less important in a world where content is stored in a central location and only transmitted to authorized devices on demand. If all content any consumer could ever desire is available from a network server, no need seems to exist for a consumer to transfer content between his computer and his MP3 player, as both devices could download the content from the network. Why, then, should copyright law exempt such activities from copyright liability? Do rights locker architectures render any limitations to copyright protection that are based on the idea of "space shifting" obsolete? If, in a rights locker architecture, a consumer wants to recommend a video to a friend, he does not have to transmit the video file to his friend anymore. Rather, he may simply send him a link that points to the location of the video file on the central server. If the friend can download the movie from the network without problems, why should copyright law exempt copying among friends from copyright liability? What is the notion of fair use in a world where any content is available for everybody from any location at any time?[1792]

Although it is beyond the scope of this article to provide a comprehensive answer to such questions, it should be noted that fair use will still play an important role in rights locker architectures. Among other things, copyright limitations induce positive external effects that are important for subsequent creativity.[1793] The justification for such limitations will also apply in rights locker architectures. Yet, the characteristics of copyright limitations may have to change in a rights locker

[1792] Rights locker architectures make local storage of content unnecessary and challenge copyright limitations that assume the necessity of such storage. In this regard, they are similar to the challenges the GNU General Public License (GPL) is exposed to by application service providers (ASP) and web services. The GPL builds upon the assumption that software source code is distributed to programmers so that they can adapt and change the code. With both ASPs and web services, however, no need exists anymore to distribute any source or object code of computer programs. Rather, software programs are run on a central network server and are accessed through a web or another network user interface. Without the distribution of source code, the protection of the free software/open source idea by the GPL could fail. For more information, see *FSF Endorses New "GPL + Web Services" License, Requests Comment*, available at: http://www.kuro5hin.org/story/2002/3/20/154118/890 (Mar. 20, 2002); interview with Richard M. Stallman on Slashdot, available at: http://slashdot.org/interviews/00/05/01/1052216.shtml (May 1, 2000).

[1793] See: Bechtold (2002): 330–336; Gordon (2002a): 186; Burk, Cohen (2001): 43–47. See also: Gordon (2002b).

architecture. To achieve many (but not all) of the goals of current copyright limitations, it could be sufficient to grant consumers access to the rights locker without the rights holder's permission. In such a scenario, a consumer would not be allowed to receive a copy of some content from a friend without the rights holder's permission (because there would be no need to copy), but he would be allowed to receive the content from the rights locker depository without the rights holder's permission. Fair use, in other words, would not cover the physical copy of the content, but the attached rights that are stored in the rights locker.

While such an approach may not be a silver–bullet solution,[1794] it seems more than worth exploring. If the importance of physical copies disappears in a more and more networked world, copyright limitations that are based on physical assumptions may have to adapt as well.

II.2 Dynamic DRM Systems, Cumulative Innovation, and the Commons

Quite often, DRM systems are depicted as if it were in their technical nature to restrict creativity and suppress fair use. This section attempts to show why this description is partially incorrect. DRM deals with the "digital management of rights". What the characteristics and scope of these rights are is not determined by obscure technical necessities, but can be determined by technologists, lawyers, politicians — i.e. by the society as a whole. Fortunately, DRM technology is very malleable. Nothing in the "nature" of DRM requires that DRM be only used for restricting access to protected content or suppressing fair use privileges.[1795] Properly understood, DRM is a much more neutral technology than commonly acknowledged.

Dynamic DRM Systems

One argument against DRM is that it suppresses subsequent creativity. It is one of the persistent and widespread errors in the legal and even the economic analysis of innovation that creativity and innovation are a static process.[1796] Rather, both are cumulative and dynamic processes. Therefore, as any intellectual property, copyright law must ensure that by providing incentives for creativity, it does not overly restrict access to already existing works.[1797] This line of reasoning may also be applied to DRM systems. By over–protecting digital content with DRM systems, critics claim, subsequent creators are deprived of the possi-

[1794] Such a rights locker architecture that supports fair use would have to address several concerns. As Dan Burk and Julie Cohen have pointed out in a slightly different context, centralizing control over who can benefit from fair use privileges creates various institutional dangers; see: Burk, Cohen (2001): 59–65. A rights locker architecture would have to make sure that users can benefit from fair use privileges even if this runs contrary to the interests of rights holders and of the operator of the rights locker; see: id.: 60–64. Furthermore, such architecture could chill spontaneous uses; see: id.: 65–66.

[1795] For a powerful argument against the idea that technology cannot be regulated because of its innate "nature", see: Lessig (1999): 24–29.

[1796] See: Kitch (2000): 1738–1739.

bility to reuse this content. DRM systems, the argument goes, protect content in a static way and are therefore, in a long–term perspective, dangerous to innovation and creativity.

While the author agrees with the underlying economic analysis of this argument,[1798] and while it may be true that most current DRM implementations have such shortcomings, there is nothing in the "nature" of DRM that prevents it from addressing cumulative creativity and innovation. Rather, it is imaginable that DRM would provide tools to deal with cumulative and overlapping creativity.

Such a "dynamic" DRM system would have to meet two requirements. Firstly, it would have to provide a "rights expression language" in which cumulative creativity can be properly expressed. Secondly, it would have to be able to cope with the relationships among numerous rights holders of various generations. Both requirements will be described in more detail in the following.

DRM systems use so–called "metadata" to express "usage rules", i.e. the conditions under which protected content can be used and accessed by an authorized user. So–called "rights expression languages" (RELs) enable the content provider to express a rich set of usage rules in machine–readable metadata that can be attached to the content. One of the most well–known RELs is the "eXtensible rights Markup Language" (XrML).[1799] XrML is a "general–purpose language in XML used to describe the rights and conditions for using digital resources."[1800] With RELs such as XrML, the permission to copy, delete, modify, embed, execute, export, extract, annotate, aggregate, install, backup, loan, sell, give, lease, play, print, display, read, restore, transfer, uninstall, verify, save, obtain, issue, possess, and revoke content may be expressed in a machine–readable form.[1801] The grant of these rights may be conditioned upon a wide array of circumstances:

[1797] How intellectual property law should deal with this tension is an open question. For an overview of the debate, see: Galline, Scotchmer (2002); see also: Lemley (1997). For an argument that broad patents are socially beneficial because they stimulate further innovation, see: Kitch (1977); but see: Merges, Nelson (1990). For an account of the importance of having commons for innovation, see: Lessig (2001).

[1798] See: Bechtold (2002): 334–336.

[1799] See: http://www.xrml.org. XrML originally stems from research by Mark Stefik at Xerox PARC and is now under the auspices of ContentGuard. In April 2002, ContentGuard submitted XrML to OASIS, an XML interoperability standards consortium that plans to develop a standardized REL. Other rights expression languages include the "Open Digital Rights Language" (ODRL; http//www.odrl.net), the "eXtensible Media Commerce Language" (XMCL; http://www.xmcl.org), and the "eXtensible Access Control Markup Language" (XACML; http://www.xacml.org).

[1800] eXtensible rights Markup Language (XrML) 2.0 Specification, Part I: Primer 5, at http://www.xrml.org/get_XrML.asp (Nov. 20, 2001).

[1801] For an overview, see: Id.: 13; Open Digital Rights Language (ODRL), Version 1.1, 8, 33–34, available at: http://www.odrl.net/1.1/ODRL-11.pdf (Aug. 8, 2002); see also: http://www.giantstepsmts.com/DRM%20Watch/xrml20.htm. For a more detailed description of the rights available under XrML, see: eXten-

access to and use of digital content may be restricted to certain time periods, locations, devices (for example, computers, storage media, printers, and computer displays), and to certain users. Furthermore, the number of times content may be accessed or used can be restricted. At which quality, in which format and for what purpose the content may be accessed may also be defined. Finally, the access and use may be conditioned upon the payment of a flat or a pay–per–use fee.[1802]

Although it is beyond the scope of this article to describe RELs in detail, it is striking that most current RELs do not provide ample tools to express how and under which conditions content may be reused, altered, reformatted, modified or otherwise transformed for the integration — be it in part or as a whole — into other works. A dynamic DRM system would require an REL that would be able to manage transformative uses, overlapping innovation, and the creation of derivative works in a fine–grained way. Although there is a clear lack of dynamic REL implementations, some research initiatives have recently started to work in this area.[1803]

Furthermore, as was mentioned above, a dynamic DRM system that manages transformative reuses should be able to cope with the relationships among numerous rights holders. If some content is reused in another work and if this process is reiterated several times, the legal relationships between all the rights holders involved can become very complex. Similar complexity results from digital works that are based on a multiplicity of existing works (the "clip–art phenomenon"). In the area of movies, operas and multimedia works, the law has developed rather elaborate mechanisms to cope with such multiplicity of rights. A dynamic DRM system, and in particular its REL, should be able to express and manage complex relationships between rights holders as well. Here again, current DRM systems often lack adequate tools to deal with cumulative creativity if a large number of creators is involved. And again, at least some ongoing research is attempting to develop such RELs and DRM systems.[1804]

---

sible rights Markup Language (XrML) 2.0 Specification, Part IV: Content Extension Schema 7–25, available at: http://www.xrml.org/get_XrML.asp (Nov. 20, 2001); eXtensible rights Markup Language (XrML) 2.0 Specification, Part II: Core Schema 29–31, available at: http://www.xrml.org/get_XrML.asp (Nov. 20, 2001).

[1802] See: eXtensible rights Markup Language (XrML) 2.0 Specification, Part III: Standard Extension Schema 4–37, available at: http://www.xrml.org/get_XrML.asp (Nov. 20, 2001); Open Digital Rights Language (ODRL), *supra* note 1801, at 10–14, 35–38.

[1803] See: Kumazawa et al. (2001) (describing a rights expression language that uses a hierarchical structure to describe cumulative innovation); Kumazawa et al. (2000); Yasukawa (2003) (describing a DRM system that deals with cumulative innovation that is able to dynamically and interactively generate reuse license agreements that respond to the individual and changing preferences of creators of both existing and new content); Yasukawa (2002). For some comments on the Creative Commons project, see: *infra* text accompanying notes 1806–1808.

This is not to say that, in a dynamic DRM system, every transformative use should be controlled and subject to a license under the aegis of the DRM system. Having unfettered areas, or commons, in the information ecology is an essential prerequisite for maximizing innovation.[1805] But even approaches that attempt to preserve openness in our information ecology could benefit from dynamic DRM technologies, as the following subsection will illustrate.

DRM, Creative Commons, and Linux

One example of how DRM components can be used to preserve openness and alternative modes of creativity is the Creative Commons project.[1806] In December 2002, the project, directed by Lawrence Lessig and based at Stanford Law School's Center for Internet and Society, started its Licensing Project. It offers licenses that allow copyright owners to easily inform others that their works are free for copying, distribution, display, performance, modification, or reuse, or any combination or subset of the usages listed. Inspired in part by the open source software movement, Creative Commons intends to create a vibrant distributed collection of works of all sorts that are the base for creative reuses and cumulative innovation.

From an abstract perspective, Creative Commons is in the business of managing "rights" in a digital way: it enables copyright owners to grant users certain permissions to use their content in certain ways (such as to re–use their work in a derivative work), but to prohibit other uses (such as to use the work for commercial purposes or to distribute a derivate work under license terms other than Creative Commons' license terms). To achieve these goals, Creative Commons uses the World Wide Web Consortium's "Resource Description Framework" (RDF) and the "Dublin Core" metadata system to express the permissions granted by copyright owners in machine–readable metadata.[1807] In other words, Creative Commons is using a DRM rights expression language in order to preserve openness and enrich the "commons".[1808]

[1804] See: Kumazawa et al. (2001) (describing a rights expression language that "clarifies relation among each rights holder and relation among his/her offered terms and profit allocation to each holder"); Kumazawa et al. (2000).

[1805] See: Lessig (2001).

[1806] See: http://www.creativecommons.org.

[1807] See: http://creativecommons.org/learn/technology/metadata. For some criticism on this approach, see: Clark (2003). Meanwhile, Creative Commons metadata can be automatically included in weblogs and weblog RSS feeds by weblog authoring programs such as Movabletype and Userland's Manila; see: http://www.movabletype.org/docs/mt26.html#creative%20commons%20licenses; http://manila.userland.com/creativeCommonsRssManila. For an argument that this creates a DRM system, see: http://doc.weblogs.com/2003/04/13#theWhateverLicense.

[1808] Creative Commons emphasizes that it is not in the "digital rights management" business, but merely uses "digital rights description" or "digital rights expression" (DRE) technology; see: http://creativecommons.org/faq#faq_entry_3323; Lawrence Lessig, available at: http://cyberlaw.stanford.edu/lessig/blog/archives/2003_04.shtml#001067.

Another example of how DRM components may be used to preserve openness and alternative modes of creativity is the Linux kernel. This core component of the open source Linux operating system is distributed under the GNU General Public License (GPL).[1809] The Linux kernel allows kernel–level code to be added at run–time. Thereby, after Linux has booted, additional functionality, such as hardware device drivers, new system calls or support for another file system, can be loaded into the system without rebooting the system or recompiling the kernel. Typically, such "loadable modules" use and incorporate kernel functions and data structures and may therefore be a derivative work of the Linux kernel.[1810]

Section 2 b) of the GPL demands that all derivative works may only be distributed under the conditions set forth by the GPL. Thereby, the "viral"[1811] GPL prevents proprietary modules from being loaded into the Linux operating system. From an open source perspective, this provision of the GPL has an important purpose: it attempts to keep as much software components open and free from proprietary control as possible.[1812]

It objects to characterizations of its Licensing Project as a DRM project. This results from a different use of the term DRM. In the view of Creative Commons, the term "digital rights management" encompasses technologies that *enforce* certain policies, while DRE encompasses technologies that *express* them. This author agrees that the distinction between policy enforcement and policy expression is a very important one. The legal and policy implications of both sets of technologies are very different. Regularly, policy enforcement technologies raise much more concerns than mere policy expression technologies. Yet, as was described *supra* text accompanying note 1785, as opposed to Creative Commons, the author adopts a more neutral understanding of the term DRM which encompasses both policy enforcement and policy expression technologies. According to this terminology, "DRE" is just a subset of technologies that belong to the more general term "DRM". This is not to say that Creative Commons provides a full–fledged DRM system with access control, encryption and so on. However, as this subsection attempts to show, Creative Commons uses some DRM technologies such as rights expression languages and metadata. This illustrates that, properly understood, DRM is a neutral technology that does not *per se* violate the goals of Creative Commons. Of course, most of the current commercial DRM *implementations* run counter to the goals of Creative Commons. But this discrepancy is not inherent to DRM *technology*. For a related argument that open source software does not run counter copyright law, but rather depends on it, see: Radin (2002a): 13.

[1809] GNU General Public License, Version 2, available at: http://www.gnu.org/copyleft/gpl.html (June 1991).

[1810] Whether and to what extent loadable modules are in fact derivative works that are subject to § 2 of the GPL, is a difficult question that is beyond the scope of this article. No case law exists that directly addresses this question. As a general guideline, many commentators view modules that are statically linked to the kernel as derivative works, as opposed to dynamically linked modules. See: Jaeger, Metzger (2002): 43–45, 52–54; Asay (2002), 10–22; see also: E–mail from Linus Torvalds, available at: http://www.atnf.csiro.au/people/rgooch/linux/docs/licensing.txt (Oct. 19, 2001).

[1811] See: Behlendorf (1999): 167; see also: Radin (2002b): 1141.

[1812] However, this approach has some disadvantages as well. On the necessary tradeoff, see: Stallman (2002b). One alternative to the GPL that permits

Since September of 2001, the Linux system does not only rely on this legal allocation of rights, but also uses technology to enforce the desired openness of the system. In particular, the Linux kernel includes a mechanism that, before loading any module, checks whether the loadable module is GPL–compatible or not.[1813] If the module's license terms do not allow its distribution under the GPL, the mechanism reports a warning and flags the kernel as "tainted".[1814]

While a detailed technical description of this mechanism is beyond the scope of this article,[1815] it is important to realize that the Linux kernel uses technology to ensure that only software which adheres to the open source idea may use kernel functions. The Linux system uses a rudimentary rights expression language to express the license terms under which a module is distributed. The kernel reads this license string and either grants access, reports a warning or denies access to kernel components. This rights expression and enforcement mechanism is nothing less than a tiny DRM system.[1816] The Linux kernel's DRM system is another example of how DRM technology may be used to preserve openness and protect a "commons" for creativity.[1817]

Symmetric Rights Expression Languages

DRM has also been severely criticized for overriding various limitations to copyright law and for protecting content providers at the expense of legitimate interests of users and the public at large. Although this may be true for many current

the use of open source programs and libraries in proprietary programs is the "GNU Lesser General Public License" (LGPL), Version 2.1, available at: http://www.fsf.org/copyleft/lesser.html (Feb. 1999). For some information on the LGPL, see Nadan (2002): 360 note 51; Stallman (1999): 63; Jaeger, Metzger (2002): 50–54.

[1813] For a general overview, see: Dankwardt (2002).

[1814] Furthermore, the mechanism can also control that kernel symbols may only be used by modules which are licensed under the GPL; see: Dankwardt (2002); The Linux-Kernel Mailing List FAQ, at: http://www.tux.org/lkml/#s1-19 (last updated Sept. 29, 2002).

[1815] See: Dankwardt (2002); Insmod Manpage, at: http://lux.rm-rdf.com/man/man2html.cgi?insmod (last updated Jan. 30, 2002).

[1816] See also: posting of Alan Cox to linux-kernel@vger.kernel.org, at: http://lwn.net/2001/0906/a/ac-tainted.php3 (Sept. 5, 2001). Preserving openness was not the only, or even the primary reason for including the described mechanism into the Linux kernel. Rather, some of the kernel developers became tired of receiving bug reports from users who are running proprietary modules in their systems; see: LWN.net, *Kernel Development*, at: http://lwn.net/2001/0906/kernel.php3 (Sept. 6, 2001). Another example of a software system that uses DRM components to preserve openness is the "pragma License" in the Ada95 frontend to the GCC, GNAT; see: GNAT Reference Manual, at: http://gcc.gnu.org/onlinedocs/gcc-3.2/gnat_rm/Implementation-Defined-Pragmas.html.

[1817] In addition, in April 2003, Linus Torvalds, the creator of the Linux kernel, opined that no legal or political reason exists why a more extensive DRM system could not be built into the Linux operating system, see: Posting of Linus Torvalds to the Linux Kernel Mailing List, at: http://yro.slashdot.org/article.pl?sid=03/04/24/1312231 (Apr. 23, 2003).

commercial DRM implementations, it does not mean that the DRM concept is inherently hostile to fair use. Whether a DRM system respects fair use or not depends, in particular, on the design of the rights expression language. If fair use privileges and the other legitimate interests of information users cannot be expressed in the REL, such interests simply do not exist within the DRM system. Therefore, it is of utmost importance that RELs include semantics to express not only the interests of creators and rights holders (as all current RELs do), but also of information users (as no current REL does).[1818]

Recently, Deirdre Mulligan and Aaron Burstein have proposed changes to XrML that would create such a "symmetric" REL.[1819] If, for example, the content provider uses metadata to prevent uses which fall under the fair use defense or other copyright limitations, a symmetric REL would offer the means to express the user's request to engage in such use and communicate this to the DRM enforcement engine.[1820] Furthermore, a symmetric REL would include mechanisms to express the context in which DRM–protected content is used, so that the system may assess more accurately whether the user's request is a fair use or not.[1821] While expressing attributes such as locality and user intent in an REL might be a very complex issue, such expressiveness seems indispensable for creating a well–balanced REL. Mechanisms to distinguish between private and public uses would also be helpful, as copyright law often distinguishes along this line as well.[1822] Symmetric RELs should be able to mark data that is not covered by copyright protection (such as mere facts under U.S. copyright law or works after their copyright term has ended).[1823]

A symmetric REL could also involve various fair–use–friendly default settings. It could provide, for example, that users of a particular kind of work (such as electronic books) are always granted permission to use the work in certain ways (such as printing or private copying).[1824] Finally, it could include a default setting according to which pay–per–use models would not be employed and the tracking of individual usage patterns would be impermissible.[1825] Such approach might be even more promising in European *droit d'auteur* countries which, in contrast to the United States, limit their copyright protection not by a very broad and often fuzzy fair use doctrine, but by an enumerative list of discrete copyright limitations.[1826]

[1818] See: Mulligan, Burstein (2002): 4; Samuelson (2003): 42; Fox, LaMacchia (2003): 62–63.
[1819] See: Mulligan, Burstein (2002); see also: Bechtold (2002): 48–49.
[1820] See: Mulligan, Burstein (2002): 7.
[1821] See: Id.; see also: Felten (2003): 58.
[1822] See: Mulligan, Burnstein (2002): 10.
[1823] See: Id.: 11–12.
[1824] See: Id.: 8–9; see also: Fox, LaMacchia (2003): 63.
[1825] See: Mulligan, Burnstein (2002): 9.
[1826] See also: Burk, Cohen (2001): 70; Felten (2003): 58; Fox, LaMacchia (2003): 63; Erickson (2003): 38.

While a symmetric REL is not a silver–bullet solution to reconcile DRM systems with copyright limitations, it would at least enable DRM systems to approximate the scope and importance of copyright limitations in general, thereby enabling consumers to use and access content without having to seek approval from rights holders.[1827] DRM systems that employ a symmetric REL would more closely align with the existing balance set by copyright law and could overcome much of the criticism related to fair use.[1828]

Conclusion

In contrast to how it is sometimes described, DRM is not a synonym for absolute power of copyright owners over their creations. Rather, it provides an extremely flexible set of technologies that may be used for many different purposes. This is not to say that DRM will be able to cope with the whole range of copyright limitations and transformative uses in a manner of automated decision–making. It is just a critical remark about the current DRM discussions which do not take the full potential of DRM technology into account. Dynamic DRM systems may provide some tools to cope with cumulative innovation. DRM systems can also be used to preserve the commons in an open information environment. Finally, DRM systems may be built in which fair use privileges and other legitimate rights of information users can be managed and expressed. While current DRM implementations often fall short to fulfill such promises, this is just an indication that future DRM–related research and development should be focused on such issues. The potential of DRM for providing a balanced framework for the protection of both creators and users, i.e. a symmetric DRM, is far larger than usually acknowledged.

II.3 DRM Technology License Agreements and Fair Use

It has often been analyzed how DRM protects content by means of intertwining technology, anti–circumvention regulations, and usage contracts. However, it has been constantly overlooked that another means to protect digital content is DRM technology license agreements.[1829] This section will describe DRM technology license agreements and highlight their copyright implications.

[1827] But see: Felten (2003): 58–59, who argues that a DRM system trying to approximate the U.S. fair use doctrine is undesirable as such system would make too many errors leading to both undesired over– and underprotection of digital content. However, Felten's argument is much weaker in European *droit d'auteur* countries which do not have copyright limitations that are as vague as the U.S. fair use doctrine.

[1828] See also: Fox, LaMacchia (2003): 62–63 (aptly pointing out that the creation of a symmetric REL is only one step towards a fair–use–protecting DRM system). For a different approach to reconcile DRM with copyright limitations for private copying, see: Neubauer, Brandenburg, Siebenhaar (2002) (proposing a "light weight" DRM system that would allow users to transfer content to portable devices and transmit it to friends while discouraging them from engaging in mass-scale piracy).

[1829] So far, the relationship between DRM technology licenses, antitrust and copyright policy has only been analyzed thoroughly by Weinberg (2002) for a specific

Many DRM technologies are protected by a patent or kept as a trade secret. If a computer or consumer electronics manufacturer wants to enable his devices to process content that is protected by such DRM technology, it has to enter into a technology license agreement with the developer of the technology.[1830] Licensees of DRM technologies include manufacturers of consumer electronics, computers, storage media and other DRM–enabled devices or components as well as content providers. Licensors of DRM technologies are either the companies which have developed the DRM technology or specialized licensing authorities that administer the licensing process on behalf of these companies.[1831]

Although content providers are usually not licensors of DRM technology, due to a rather complex mix of interests, DRM technology license agreements indirectly serve their interests.[1832] This explains why various license agreements include copyright–related terms.[1833] DRM technology licenses attempt to prevent unauthorized copying. Various licenses restrict the quality or speed by which content is transmitted, making piracy less attractive as it either takes too long or leads to inferior copies.[1834] They also require that DRM–enabled devices obey the

license in the pay TV sector ("POD-Host Interface License Agreement") and by Bechtold (2002): 178–196, 405–406, for such licenses in general; see also: Marks, Turnbull (2000): 206.

[1830] Apart from Sony, there are no major content companies that also produce consumer electronics or vice versa.

[1831] Such licensing authorities include the DVD Copy Control Association, Inc. (http://www.dvdcca.org), the Digital Transmission Licensing Administrator (http://www.dtcp.com), the 4C Entity, LLC (http://www.4centity.com), and Digital Content Protection, LLC (http://www.digital-cp.com).

[1832] The short version of the story is that content providers will only release content in a DRM system if certain security requirements are met. Therefore, content providers are in the position to force DRM technology companies to alter their technology and the related license agreements according to the content providers' interests; for more information, see: Bechtold (2002): 180; Weinberg (2002): 286; *In re Implementation of Section 304 of Telecommunications Act of 1996*, 15 F.C.C.R. 18199, Par. 15, 27 (Sep. 18, 2000); see also: Marks, Turnbull (2000): 206.

[1833] For the following analysis, most of the publicly available DRM technology licenses were evaluated. The evaluated licenses include the CSS, CPRM/CPPM, DTCP and HDCP license agreements. For more information on the underlying technologies, *see infra* notes 1936–1939. In addition, the POD–Host Interface License Agreement ("PHILA") was evaluated. This license deals with a decryption technology ("Dynamic Feedback Arrangement Scrambling Technique", DFAST) that is used in U.S. pay TV decoders. For more information, see: Weinberg (2002): 287–288; Bechtold (2002): 184; *In re Implementation of Section 304 of Telecommunications Act of 1996*, Commercial Availability of Navigation Devices, 15 F.C.C. Rcd. 18199 (F.C.C. 2000). DFAST is also licensed under other licensing terms, see: *Consensus Cable MSO — Consumer Electronics Industry Agreement on "Plug & Play" Cable Compatibility and Related Issues*, available at: http://www.ncta.com/pdf_files/CE-NCTAagreement.pdf (Dec. 19, 2002).

[1834] See: § 2.3, Exhibit C, POD–Host Interface License Agreement, available at: http://www.opencable.com/downloads/PHILA_101702.pdf (Oct. 17, 2002); §§ 4.2.1 (ii), (iii), 5.1, 5.2.2, Exhibit C-1, and §§ 4.2.1 (ii), (iii), 6.1.2, Exhibit C-2, CPRM/CPPM License Agreement, Version 1.1f, available from: http://www.4centity.com/licensing/adopter/adopter_form.html.

usage rules of digital content that are defined by the content provider. If, for example, the content provider has embedded a digital watermark into his content prescribing that the content may only be copied once, all consumer devices that use the licensed DRM technology are contractually required to ensure through technology that a user can indeed make only one copy.[1835]

Although DRM technology license agreements raise many more questions,[1836] for the purposes of this article, it is sufficient to note that they may come into conflict with copyright law. DRM technology licenses enable content providers to make sure that all consumer devices that can access their DRM–protected content adhere to certain usage rules. Although they do not directly supersede copyright limitations, they can prevent device manufacturers from producing devices that would enable consumers to benefit from copyright limitations, as this would constitute a breach of the technology license.[1837] Thereby, DRM technology license agreements may contribute indirectly to the *de facto* undermining of copyright limitations.

The potential tension between DRM technology license agreements and copyright limitations has been very rarely addressed by legislatures or the administration. In Europe, the matter has not been tackled at all.[1838] In the United States, in its assessment of a DRM technology license in the pay TV sector,[1839] the Federal Communications Commission (FCC) rejected the claim that the license would preclude reasonable home recording of DRM–protected content.[1840] Although the FCC did not take action against the DRM technology license, this instance shows a possible method of reconciling technology licenses with copy-

[1835] See: § 2, Exhibit B, Part 1, Digital Transmission Protection License Agreement, at: http://www.dtcp.com/data/DTCP_Adopters_Agreement010730.PDF (July 30, 2001); § 3, Exhibit C, POD–Host Interface License Agreement, *supra* note 1834; §§ 4.1.4, 4.2.1 (i), Exhibit C-1, §§ 3.1.1 a), 3.2.2, § 4.2.1 (i), Exhibit C-2, §§ 3.1.1, 3.1.2, 4.2.1 (i), 4.2.2. (i) Exhibit C-3, CPRM/CPPM License Agreement, *supra* note 1834.

[1836] See: Bechtold (2003a); Bechtold (2002): 178–196, 377, 405–406.

[1837] See: Weinberg (2002): 292.

[1838] However, the possible tension between DRM technology licenses and other areas of public policy, in particular antitrust law, have long been recognized in Europe, see *infra* text accompanying notes 1891–1892.

[1839] For information on the "POD–Host Interface License Agreement", see *supra* note 1833.

[1840] *In re Implementation of Section 304 of Telecommunications Act of 1996*, *supra* note 1833, at Par. 28–29. That the FCC recognized the possible tension between DRM technology licenses and copyright limitations becomes evident in the separate statement of Commissioner Gloria Tristani: "[...] *our ruling in no way authorizes any attempt by providers of services to utilize this ruling to combine technology with copy protection in a manner that interferes with, or unreasonably restricts, a consumer's fair use of copy–protected material.* [...] *Today's declaration ensures the financial rewards of copy protection to content owners while protecting citizens from the dispossession of their right to fair use. Based on the record before us and controlling Supreme Court precedent, I believe we have struck the appropriate balance*", Id. at 18220. See also: Weinberg (2002): 289–292 (criticizing the FCC's failure to recognize the underlying public policy concerns).

right limitations: limiting the range of terms licensors can write into a DRM technology license.[1841]

II.4 DRM and Research

DRM–related anti–circumvention regulations may create chilling effects on scientific research and progress. In 2000, Princeton University Professor Edward Felten and several coauthors intended to present a research paper at a scientific conference that described weaknesses in several watermarking systems which the "Secure Digital Music Initiative" (SDMI) was considering to adopt at that time. The Recording Industry Association of America (RIAA) and SDMI threatened Professor Felten and his coauthors with a lawsuit because, as they claimed, the publication of the paper would violate the anti–circumvention provisions of the Digital Millennium Copyright Act (DMCA). As a result, the authors decided to withdraw the paper from the conference.[1842] In other instances, concerns about potential circumvention liabilities prompted researchers to withhold the results of their research or even not to engage in DRM–related security research at all.[1843]

To understand the potential tension between anti–circumvention provisions and security research, it is important to realize how security research works. Practical experiments and tests are indispensable for evaluating the features and security level of any real–world implementation of a security system. One of the standard approaches to evaluate a real–world security system is to attempt to break it. If a researcher succeeds in breaking it, he publishes his procedure and results, thereby enabling other members of the security research community to understand his attack and build more secure systems.[1844] By impeding such security research, the legal framework surrounding DRM could have detrimental impact on technological innovation in the area of security systems.

At least to some extent, the legislators on both sides of the Atlantic were aware of this tension between anti–circumvention regulations and scientific research. Yet, they may not have done enough to resolve it. The U.S. DMCA exempts certain acts of security testing, reverse engineering, and cryptography research from the anti–circumvention provisions. However, these exemptions are narrowly drawn and cover only a small subset of legitimate security research.[1845] In the European

[1841] See: Bechtold (2002): 405–406. This is not a totally novel approach, as the limitations on DRM technology licenses due to antitrust concerns demonstrate, see *infra* text accompanying notes 1891–1892.

[1842] The authors then sought a judicial declaration that their paper did not violate the DMCA. Later, this complaint was dismissed because SDMI and RIAA had withdrawn their objections to the publication of the paper; see: Samuelson (2001); Samuelson, Scotchmer (2002): 1647 note 333; Harper (2002); Imfeld (2003): 138.

[1843] See: Electronic Frontier Foundation (2003): 2–5; see also: Liu (2003).

[1844] See: Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 313–318; see also: Preston, Lofton (2002): 85–95.

[1845] See: Samuelson (2001): 2029; Samuelson (1999): 548–549; Committee on Intellectual Property Rights and the Emerging Information Infrastructure (2000): 318–321; see also: Preston, Lofton (2002): 119–125; Liu (2003).

Copyright Directive, the tension between anti–circumvention regulations and security research is only mentioned in a Recital.[1846]

Nevertheless, one should be cautious about condemning DRM and anti–circumvention regulations on these grounds. Whether anti–circumvention regulations actually impede security research depends on many factors related to the individual technology that was tested, the way the testing was done and publicized, the persons involved, the wording of the particular anti–circumvention regulation that is applied and so on.[1847] In some cases where an impediment of security research is claimed, such claims turn out to be unfounded.

Furthermore, the tension between anti–circumvention regulations and security research is not only a problem of the law, but also of technical security design. The more a security architecture adheres to the so–called Kerckhoff principle, the less strong this tension is.[1848] Unfortunately, this does not fully resolve the tension between anti–circumvention regulations and scientific research. There are many areas of computer security where the Kerckhoff principle does not apply, and quite often real–world implementations do not adhere to the Kerckhoff principle due to financial or technical constraints. As a result, security in most current DRM implementations does not adhere to the Kerckhoff principle, but is rather achieved by obscurity approaches, for example by using various code obfuscation technologies.[1849] Nevertheless, this demonstrates that striving for compliance with the Kerckhoff principle is not only a matter of good security systems design, but would also alleviate the tension between anti–circumvention regulations and security research.

In general, however, it is a troublesome development that various species in the ever–expanding world of intellectual property, including anti–circumvention regulations, increasingly come into conflict with the freedom of scientific research and thereby technological progress.[1850]

[1846] Recital 48 of the Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001, on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, Official Journal of the European Communities L 167 (June 22, 2001), 10, 14 (hereinafter: European Copyright Directive) (stating that circumvention prohibitions "should not hinder research into cryptography").

[1847] For an in–depth analysis of the DMCA's impact on encryption research, see: Liu (2003).

[1848] The Kerckhoff principle is widely accepted in cryptology research. It states that the security of an encryption system should not be based on the secrecy of the algorithm used, but only of particular keys employed. One of the consequences of the Kerckhoff principle is that unaffiliated security researchers may openly discuss the security features of the (publicly known) encryption algorithm without revealing any secrets. For more information on the Kerckhoff principle, see: Schneier (1996): 5; Anderson (2001): 240, 362; see also: State of New York v. Microsoft Corp., 224 F.Supp.2d 76, 238–239 (D.D.C. Nov. 1, 2002).

[1849] See: Bechtold (2002): 88–89. For more information on code obfuscation, see *infra* notes 1884–1885.

[1850] In the biotechnology area, concerns have been raised over the last few years that by issuing patents for biotechnological research tools and covering them with

III DRM, Property and Liability Rules

For several decades, copyright law has been grappling with the question of how to deal with private copying by consumers. With the emergence of cassette recorders and photocopying machines, it became evident that private copying was a mass-scale phenomenon that was very hard to control. For this and other reasons, many European legislators created a copyright exemption for private copying, but compensated rights holders indirectly by creating a levy system which imposes a levy on all blank media and copying devices being sold.[1851]

Today, 12 of the 15 member states of the European Union have put in place levy systems of different flavors.[1852] In Germany, which was the first country to create a statutory levy system in 1965, some of the levies are:[1853]

audio recording devices (except MP3 players)	€1,28	per device
audio recording media	€0,0614	per hour
MP3 players	€2,56	per player
video recording devices	€9,21	per device
video recording media	€0,087	per hour
CD burners	€6,50 – 7,00	per burner

These levies are collected by collecting societies which distribute the revenues (about 71 million € in 2000) among their members. In the United States, only the Audio Home Recording Act of 1992 includes a levy system for digital audio recording devices and blank storage media. There, the levy amounts to 2 or 3% of the price of the device or media.[1854] However, the Audio Home Recording

so–called "reach–through licenses", biological research that depends on these tools could be impeded; see: Goldstein (2001); Eisenberg (2001); see also: Ware (2002); Mueller (2001); Heller, Eisenberg (1998).

[1851] In Germany, compensating rights holders for the private copying exemption was one of the main reasons for introducing the levy system in 1965; see: Loewenheim in: Schricker (1999): § 53 notes 1–2, § 54 note 2. For a history of the levy system in European countries, see: Hugenholtz, Guibault, van Geffen (2003): 10–13.

[1852] See: Hugenholtz, Guibault, van Geffen (2003): 12 (listing Germany (1965), Austria (1980), Finland (1984), France (1985), Netherlands (1990), Spain (1992), Denmark (1992), Italy (1992), Belgium (1994), Greece (1994), Portugal (1998), and Sweden (1999)). Worldwide, at least 42 countries have a remuneration scheme for private copying, see: Id. 13.

[1853] See: § 54 of the German Copyright Act; see also: Kreile (1992). In addition, in February 2003, the arbitration board of the German Patent and Trademark Office (Deutsches Patent– und Markenamt) ruled that, for every PC sold in Germany, a levy of €12 should be paid, see: http://www.giantstepsmts.com/DRM%20Watch/germanpclevy.htm; Hugenholtz, Guibault, van Geffen (2003): 26. The PC manufacturing industry has strongly objected to the settlement proposal. It is expected that, ultimately, courts will have to decide whether PCs are subject to a levy under German copyright law or not. For some valid criticism of attempts to extend levy schemes to computers, see: Hugenholtz, Guibault, van Geffen (2003): 40–41.

[1854] 17 U.S.C. §§ 1003, 1004.

Act has a narrow scope. In particular, MP3 players are not covered by its levy system.[1855]

Levy systems curtail the rights of copyright and neighboring rights holders. With copyright, rights holders cannot only ensure to receive *remuneration* for the use of their works, but they can also *control* who uses their content in which ways and under what circumstances. In a levy system, rights holders lose this power to control, but retain the power to receive remuneration. In law–and–economic terms, levy systems turn copyright from a property rule to a liability rule.[1856] In this regard, levy systems are similar to compulsory licensing schemes: both approaches deprive rights holders of their ability to control who uses their content under what circumstances. What they are left with is the ability to receive remuneration for the use of their content.

With DRM systems, controlling private copying becomes technically feasible. This raises the question whether and to what extent existing levy systems can be justified in a DRM–suffused environment. On both sides of the Atlantic, the relationship between DRM and levy systems or related approaches is heavily discussed, albeit with sometimes opposing results.

In Europe, many DRM proponents argue that levy systems should be abandoned in favor of DRM systems. Both systems, they argue, cannot coexist: if a levy is imposed indirectly on consumers while, at the same time, they are required by DRM systems to pay for each private copy they make, consumers would end up being charged twice.[1857] Furthermore, DRM enables a more direct remuneration of the rights holders whose works are actually consumed. Compared to a levy system, DRM is, so the argument goes, more just, more precise and more efficient.[1858] According to this argument, levy systems should be abandoned, while DRM systems should be supported.[1859] This argument is supported by the European Copyright Directive of 2001 which seems to favor a gradual phasing–out of levies on digital media or equipment in favor of DRM systems.[1860]

[1855] See: Recording Industry Ass'n of America v. Diamond Multimedia Systems, Inc., 180 F.3d 1072 (9th Cir. 1999).

[1856] See: Calabresi, Melamed (1972).

[1857] See: Hugenholtz, Guibault, van Geffen (2003): 34.

[1858] See: Huppertz (2002): 108; Hart (2002): 60; Walker, Sharpe (2002): 260–261; see also: Hugenholtz, Guibault, van Geffen (2003): 32–47. This argument also raises the question what role collecting societies, which — among many other things — administer many levy systems, can still play in a DRM-suffused environment; see: Bechtold (2002): 11–13; see also: Jehoram (2001); Merges (1996); Kretschmer (2002); Hugenholtz, Guibault, van Geffen (2003): 47. See further: *Günnewig* (page 528); *Ulmer–Eilfort* (page 447) within this book.

[1859] An alternative solution would be to enact a broad levy system, but to disregard such content providers in the levy distribution process which use DRM systems to protect their content. The amount of the levy would create an upper bound up to which DRM technology companies could license their technologies to device manufacturers (as it would be cheaper for device manufacturers to use the levy system for content protection if the DRM technology license fee would be more expensive than the device levy).

By contrast, U.S. scholars have proposed to expand the liability rule regime considerably while condemning the DRM regime.[1861] While adequate remuneration for creators is an essential incentive for creativity, any über–protection of creators may harm innovation in regards to distribution technology and content itself. Empowering creators to control who uses their content under what circumstances, the argument goes, may be such an über–protection. Therefore, it may be a wise policy and economic decision to cut the power of rights holders back to a mere right to become remunerated — a compulsory licensing scheme or a levy system.[1862] The goal is, as Lawrence Lessig puts it, "compensation without control".[1863]

It is interesting to note that in Europe and the United States, opposite DRM policy proposals are articulated and discussed. In Europe, a move from the generalizing levy system to more individualized DRM solutions can be observed, while in the United States, academic circles argue to move from DRM to a levy system.

Although it is probably true that a regulatory system of perfect control would be a bad policy choice for intellectual property law, it is beyond the scope of this article to answer the question of what the optimal policy decision along the alleged axis between a levy or a compulsory licensing scheme and DRM

[1860] See: Article 5 (2) (b) of the European Copyright Directive, *supra* note 1846, at 10 (stating that member states may provide for limitations to the reproduction right "[...] *in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non–application of technological measures* [...]") and Recital 39 of the Directive (stating that in regards to the private copying limitation, member states "'[...] *should take due account of technological and economic developments, in particular with respect to digital private copying and remuneration schemes, when effective technological protection measures are available*"); see also: Recital 35. In Germany, Article 5 (2) (b) of the Copyright Directive is likely to be implemented as a new subparagraph of § 13 of the Urheberrechtswahrnehmungsgesetz, see Artikel 2 des Entwurfs eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft, Bundestags–Drucksache 15/837 vom 9. 4. 2003, S. 1, 22. For a comprehensive analysis of the relationship between DRM and levies under the European Copyright Directive, see: Hugenholtz, Guibault, van Geffen (2003).

[1861] See, e.g.: Netanel (2003) (proposing a statutory levy system for P2P software and services, computer hardware, CD burners, MP3 players, digital video recorders, and blank media while precluding content providers from employing DRM systems to block activities that are covered by the levy system); Sobel (2003) (proposing to impose a statutory license on the copying and redistribution of digital content, to embed digital watermarks and fingerprints into the content so that Internet service providers can monitor the content flow through their servers, and to obligate ISPs to pay a royalty charged by each work's copyright owner); Lunney (2001): 911–918. William Fisher makes a similar argument in chapter 6 of his forthcoming book "Promises to Keep — Technology, Law, and the Future of Entertainment". See also: Lessig (2001): 254–255.

[1862] See: Lessig (2001): 107–110, 199–202, 216–217, 254–255.

[1863] See: Id.: 201.

is. Rather, this subsection attempts to show that, in fact, no such axis exists. DRM is not the same as perfect control. Or, at least, it does not have to be. DRM is also not the opposite of a levy system, a compulsory licensing scheme or a liability rule. Properly understood, DRM technology is much more flexible than most of its critics acknowledge. Besides control technologies such as access control and encryption, DRM includes technologies to manage content flows, to describe content, users and devices, as well as to describe and prove the authenticity and integrity of content, users, metadata and devices.[1864] It is possible to design a DRM system that does not grant utmost control to rights holders, but only enables them to receive adequate remuneration.[1865] Indeed, even levy and compulsory licensing systems could be based on DRM technology.[1866]

Therefore, to ask whether a levy system or a DRM solution should be preferred is to ask the wrong question. Rather, it should be asked whether a copyright regime that is solely based on a property rule approach is preferable over a regime that includes well–placed elements which are based on a liability rule approach. The discussion along the alleged DRM — levy axis does not answer this question. Only after this question has been answered can one think about the appropriate technologies that should be used to achieve the desired incentive structure.

IV DRM and Privacy

While it is still unclear what role DRM should and will play in the intellectual property system, its relation to other areas of law is fuzzy as well. This applies particularly to privacy law. DRM systems use various mechanisms to identify and track users within the system. They have the potential to monitor what people privately read, listen to or watch.[1867] On the other hand, such usage information may be useful both to content providers and consumers: content providers can engage in price discrimination, which may lead to lower prices for some consumers.[1868] All consumers could also benefit from a better personalization and individualization of the service.

[1864] See *supra* note 1785.

[1865] Digital watermarks could be used to describe digital content, tamper–resistant hard– and software could be used to meter usage of the content which would be the basis for payment flows to the rights holders. Although such system would still manage rights in a digital way, no component would restrict access to any content. Rather, anybody would be free to use content as long as he would be willing to pay for it. In this sense, such a DRM system would distribute content as "free resources" as defined by Lessig (2001): 12, 20.

[1866] See: Netanel (2003): 38–39 (proposing to distribute the proceeds of suggested levy system to rights holders in proportion to the usage of their respective works, as measured by DRM technology); Sobel (2003): 12–13 (suggesting to use digital watermarks and fingerprints to support his proposed statutory licensing regime); Hugenholtz, Guibault, van Geffen (2003): 45 (proposing to embed metadata in recording equipment and media to indicate to a DRM system that a levy has been paid).

[1867] See: Bygrave, Koelman (2000); Cohen (1996); Bygrave (2002a); Bizer (2001).

In this muddy mixture of privacy, competition, consumer protection and business interests, a clear regulatory approach as to how to reconcile DRM with privacy laws does not exist yet.[1869] What is particularly unfortunate is that there is a clear lack of discussion about what role privacy–enhancing technologies (PETs) can and should play in DRM systems.[1870] Furthermore, it should be reminded that the acronym DRM does not stand for "digital copyright management", but for the management of *rights in general*.[1871] It is interesting to analyze how DRM systems can be adapted in order to manage and protect privacy rights.[1872]

The design of a DRM system shapes its privacy implications. This becomes particularly obvious with the design of metadata systems. It is an open question as to what the optimal granularity is with which digital objects should be identified by a metadata system. Should a text be only identifiable in its entirety or should each paragraph, sentence, word or even character be identifiable by the metadata systen?[1873] While there are many technical and efficiency reasons for preferring one approach over the other, it is important to realize that the

[1868] In general, price discrimination becomes particularly attractive if the fixed costs are high and the marginal costs are low. This applies, e.g., to digital content. DRM systems offer technologies that can clear two of the most important hurdles to price discrimination: identifying different users with different preferences and preventing arbitrage between such users; see: Bechtold (2002): 307–311. Whether price discrimination is beneficial from an economic perspective and should therefore be used in real–world DRM systems is a hard question; for some valid criticism against this conclusion, see: Boyle (2000); Cohen (2000): 1801–1806; Gordon (1998): 1381, 1386–1389; Bechtold (2002): 321–324.

[1869] While both the European Copyright Directive and the U.S. DMCA address the tension between DRM systems and privacy laws, they do not offer such an approach; see: Bygrave (2002a): 54–56; Bygrave, Koelman (2000): 106–120; Samuelson (1999): 552–554.

[1870] For an overview of the role PETs could play in DRM systems, see: Bechtold (2002): 138–142. For another, rather different and critical proposal, see: Feigenbaum, Freedman, Sander, Shostack (2001).

[1871] This insight was best expressed by Victor Shear, then CEO of InterTrust, in a Congressional hearing: "*Ultimately, the reality of sophisticated DRM technology is about far more than Napster, online entertainment and copyright law. It is about constructing a civil digital society in the Internet Age, where rules created for or by its citizens can be implemented and respected wherever and whenever their legitimate interests are in play*", Testimony Before the U.S. Senate Judiciary Committee on Online Entertainment and Copyright Law, Apr. 3, 2001, 2001 Westlaw 323735. Indeed, as DRM reveals, strong similarities between copyright and privacy exist in the digital age. In both cases, the law tries to allocate rights to individuals in order to solve conflicts of interests. In both cases, the subject of these rights is information in various forms.

[1872] See: Kenny, Korba (2002); Zittrain (2000).

[1873] See: Paskin (1999); Kroon (2000): 231; Bechtold (2002): 39. A related problem is whether information about the content should be embedded in the content itself or should be stored in a separate database. In the area of metadata systems, this led to a long–lasting battle between "intelligent" and "dumb" identifiers. Choosing an appropriate architecture along these lines has not only efficiency, but also privacy implications; see: Paskin (1999): 1209, 1213–1214; *Paskin* within this book on page 26; Hill (1999): 1232; Bechtold (2002): 38.

design of the metadata system has privacy implications as well. The more precisely an object can be identified, the better and more extensive usage data can be collected and processed. Determining the granularity of a metadata system determines its implications for privacy interests as well. Furthermore, rights expression languages could be designed to minimize expressions of personally identifying information.[1874] Consumers could be given control over the entities that process their data and consumption requests.[1875]

Although this article does not attempt to provide specific guidelines of how to implement a privacy–protecting DRM system, it attempts to show that the discussion about such issues could actually lead to a DRM design that truly respects and protects the various legitimate privacy interests of its users.[1876]

V DRM and Competition

Increasingly, DRM systems are used to protect hardware and software platforms.[1877] Such protection may harm competition, either in the platform market itself or in complementary markets. In analyzing these developments, issues such as antitrust, innovation, and security concerns as well as the free movement of goods have to be taken into account. As this section will demonstrate, anti–circumvention regulations are increasingly used in circumstances for which they were clearly not intended. Increasingly, DRM technologies and anti–circumvention regulations are not only used to control content against unauthorized copying, but also to control markets against undesired competition.

V.1 Competition in the Platform Market

More and more, manufacturers of hardware and software platforms use DRM components to prevent competitors from developing and marketing competing platforms. In particular, DRM technologies and anti–circumvention regulations are used to create proprietary interfaces to the platform, thereby foreclosing entry into the platform market.[1878] Three examples, from computer games and pay TV decoders to patented DRM components, may illustrate this point.

[1874] This could mean to limit the expressive functionality of rights expression languages so that they could not be used to express and gather personally identifying information; see: Mulligan, Burstein (2002): 12–13.

[1875] See: Id.: 13.

[1876] For interesting proposals to reconcile DRM with privacy interests on these grounds, see: Cohen (2003).

[1877] A technology platform is a good that a consumer can acquire to make use of complementary goods that depend on the platform. Desktop computers, video game consoles and operating systems are examples of such platforms. For an overview of the legal problems of such platforms, see: Lichtman (2000); Weiser (2002); Weiser (2001a); Weiser (2001b); Houweling (2002); Samuelson, Scotchmer (2002): 1611, 1615–1626.

[1878] See: Samuelson, Scotchmer (2002): 1645.

Reverse Engineering DRM–Protected Platforms

Developers of hard– or software platforms (such as personal computers, video game consoles or operating systems) have strong interests in preventing competitors from developing interoperable platforms, as this could reduce the developers' market share. By contrast, competitors have strong interests in being able to reverse engineer the dominant technology platform in order to develop a competing and interoperable platform. Whether and to what extent reverse engineering should be allowed and how this alters incentive structures for software developers is a question that has received considerable attention in the scholarly debate.[1879] As this subsection will show, protecting technology platforms with DRM components may alter the balance between copyright protection and reverse engineering limitations, which are enshrined in many countries' copyright laws. If a technology platform is protected by a DRM system, reverse engineering may not only violate traditional copyright law, but also anti–circumvention regulations. Thereby, the relationship between anti–circumvention regulations and reverse engineering activities becomes essential.

Two examples may illustrate this point. Blizzard Entertainment[1880] markets several highly successful computer games which can be played over the Internet in a multi–player mode. In order to play a Blizzard game in such a mode, each user has to connect to an Internet gaming server operated by Blizzard. Since 1998, a small software company has been analyzing the internal operation of Blizzard's gaming network in order to develop a software program called "bnetd" which emulates Blizzard's gaming server. With bnetd, users can form online gaming communities and play Blizzard's games without having to use Blizzard's online server. In the spring of 2002, Blizzard filed a lawsuit against the bnetd developers. Among other things, Blizzard claims that its gaming network is protected by various technological measures, and that the development of a competing gaming server is an infringement of the DMCA's anti–circumvention provisions. By contrast, the bnetd developers view their activity as lawful reverse engineering that is aimed at creating an interoperable, competing gaming server.[1881]

Another example of the tension between DRM–protected platforms and reverse engineering activities is the Sony Playstation. In 1999 and 2000, Sony filed two copyright– and patent–based lawsuits against two companies that had developed software programs which emulated Sony's video game console "Playstation". By using one of these programs, the user could play Playstation games on his personal computer without having to buy a Sony game console at all.[1882] These

[1879] See only: Samuelson, Scotchmer (2002).

[1880] Blizzard Entertainment is a division of Vivendi Universal Games, Inc.

[1881] For more information on the case, see: the EFF's Blizzard v. bnetd archive page, at: http://www.eff.org/IP/Emulation/Blizzard_v_bnetd (last updated Mar. 13, 2003); Miller (2002).

[1882] Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000); Sony Computer Entm't Am., Inc. v. Bleem, LLC, 214 F.3d 1002 (9th Cir. 2000); see also: Karas (2001): 48; Samuelson, Scotchmer (2002): 1611.

emulations were made possible by reverse engineering various technical components of Sony's Playstation.[1883]

Even if anti–circumvention regulations include an exemption for reverse engineering activities, this may still not enable competitors to develop a competing platform. Various DRM technologies exist — including "code obfuscation" technologies and similar approaches to create tamper–resistant software[1884] — which render attempts to reverse engineer either very costly or even impossible.[1885] Even if the law allows reverse engineering, this can remain a hollow promise in a DRM–protected technology platform if reverse engineering is simply impossible due to technical or financial reasons.[1886] Using DRM to protect technology platforms may therefore impede competition in the platform market.

Patenting DRM Components

Another example of how competition in the DRM platform market may be impeded involves patents on DRM components. In December 2001, Microsoft obtained approval for two U.S. patents that contain many of the basic elements of a DRM–enabled operating system.[1887] DRM veteran company Intertrust has been issued 26 U.S. DRM–related patents up to date.[1888] At the very least, patents on DRM components raise the general question of whether and to what extent standards should be subject to intellectual property rights.[1889] Like every patent on technology standards, DRM patents can also be used strategically. In the context of Microsoft's Palladium initiative, for example, critics have warned that Microsoft could use its patents over the Palladium design to thwart attempts of open source programmers to create a Linux version that could be executed on Palladium–enabled PC hardware.[1890]

[1883] See, e.g.: Sony v. Connectix, 203 F.3d 596, 599–601 (9th Cir. 2000). It is noteworthy that in both of these cases, the use of DRM components to protect the technology platform was not an issue before the court.

[1884] For an overview, see: Goto (2001): 145–146; see also: Bechtold (2002): 87–89.

[1885] Of course, this presupposes that technologies such as code obfuscation are effective means to protect against reverse engineering. For a theoretical rebuttal of the idea of code obfuscation, see: Barak et al. (2001).

[1886] For some policy proposals to address this problem, see: Samuelson, Scotchmer (2002): 1661–1662.

[1887] *Digital Rights Management Operating System*, U.S. Patent 6,330,670 (issued Dec. 11, 2001); *Loading and Identifying a Digital Rights Management Operating System*, U.S. Patent 6,327,652 (issued Dec. 4, 2001).

[1888] Since April 2001, a lawsuit is pending between Intertrust and Microsoft in which the validity, scope and ownership of various DRM-related patents is analyzed.

[1889] See, e.g.: Lemley (2002).

[1890] Indeed, in its Palladium FAQ, even Microsoft addresses this concern and gives the succinct answer: "*It is too early to speculate on how those issues might be addressed*", see: Microsoft Corp. (2003). For more information on Palladium, see *infra* text accompanying notes 1986—1999.

DRM Technology License Agreements and Competition

Finally, DRM technology license agreements may be used in anti–competitive ways as well. In the area of pay TV, European legislation has tried to deal with the potential tension between DRM technologies protected by intellectual property rights and a well–functioning competition. Standards developed by the "Digital Video Broadcasting Project" (DVB) allow several competing DRM systems (so–called "conditional access systems", CAS) to be included in one single Pay TV decoder.[1891] This architecture and related approaches enable competition to occur between different providers of DRM systems in the pay TV market. In order to protect this competition, the recently adopted European Access Directive prohibits DRM technology providers from using technology license agreements to thwart this competition, either by preventing interoperability between different DRM systems or by preventing the inclusion of a competing DRM system in the same decoder.[1892] This regulatory approach prevents DRM technology providers from using license agreements to impede competition in the DRM–protected platform market.

[1891] Describing the underlying technologies is beyond the scope of this article. For more information on SimulCrypt, MultiCrypt, the Common Interface, as well as Entitlement Management Messages (EMM) and Entitlement Control Messages (ECM), see: Bechtold (2002): 105 note 522; Llorens–Maluquer (1998): 560–563; European Commission (1999).

[1892] *See* Annex I, Part I, lit. (c) to Article 6 (1) of the Directive 2002/19/EC of the European Parliament and of the Council of March 7, 2002, on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities (Access Directive), Official Journal of the European Communities L 108 (Apr. 24, 2002), 7:

> "*when granting licences to manufacturers of consumer equipment, holders of industrial property rights to conditional access products and systems are to ensure that this is done on fair, reasonable and non–discriminatory terms. Taking into account technical and commercial factors, holders of rights are not to subject the granting of licences to conditions prohibiting, deterring or discouraging the inclusion in the same product of:*
>
> - *a common interface allowing connection with several other access systems, or*
> - *means specific to another access system, provided that the licensee complies with the relevant and reasonable conditions ensuring, as far as he is concerned, the security of transactions of conditional access system operators.*"

This provision supersedes the similar Article 4 (d) of the Directive 95/47/EC of the European Parliament and of the Council of October 24, 1995, on the Use of Standards for the Transmission of Television Signals (Transmission Standard Directive), Official Journal of the European Communities L 281 (Nov. 23, 1995), 51. The Transmission Standard Directive was repealed in 2002 by Article 26 of the Directive 2002/21/EC of the European Parliament and of the Council of March 7, 2002, on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), Official Journal of the European Communities L 108 (Apr. 24, 2002), 33.

V.2 Competition in Complementary Markets

DRM components are not only used to protect technology platforms from competition on a horizontal level. As the following four examples will illustrate, developers of technology platforms also use DRM components to control which complementary goods can use and access the platform.

DRM in the Sony Aibo Dog

For a few years now, Sony has been marketing a robot pet dog called "Aibo". Many programs controlling the Aibo dog are stored in a storage device (the "Sony Memory Stick") that can be inserted into the dog. This storage device is equipped with a DRM–like copy protection mechanism. Although Sony markets various programs that extend the basic functionality of Aibo, not all Aibo owners are satisfied with what Aibo is capable of. Therefore, one particularly enthusiastic owner — known as "AiboPet" — started to write new software programs that would teach Aibo new tricks and expand its functionality. One of his most successful program, for example, taught Aibo to dance to music. In order to write such programs, the programmer had to circumvent the copy protection technology built into the Aibo Memory Stick. In October of 2001, Sony decided to take action against this "infringement" and sent a cease–and–desist letter to the programmer, citing a violation of the anti-circumvention regulations of the DMCA.[1893]

What is difficult about the Sony Aibo case is differentiating between the important and the unimportant. The case is relatively unimportant in so far as it deals with the question of whether a company can protect its robot product with a DRM system. The case is also relatively unimportant in so far as Sony decided to actually take action against the hacking of its robot dog.[1894] Yet, the case is of importance because it exemplifies how DRM systems can be employed to control the use of and access to technology platforms. Essentially, Aibo is a platform on top of which software applications can be built and run. If such a platform is protected by a DRM system, the platform owner can control who is able to build applications on top of the platform. This can prevent unaffiliated software developers from developing applications for the platform.

DRM in Laser Printers

Another example of this power to control complementary markets involves laser and ink–jet printers. DRM can be used to protect business models that are

[1893] For further information on this case, see: Labrador, David (Jan. 21, 2002): Teaching Robot Dogs New Tricks. Available at: http://www.sciam.com/article.cfm?articleID=0005510C-EABD-1CD6-B4A8809EC588EEDF; Harmon, Amy (Nov. 5, 2001): Compressed Data — Put Off by Disco Dancing, Sony Tightens Leash on Its Robotic Dog. N.Y. Times, Nov. 5, 2001 at C4; No New Tricks for Robot Dog, Available at: http://www.chillingeffects.org/anticircumvention/notice.cgi?NoticeID=24 (original cease–and–desist letter sent by Sony).

[1894] Later, the company changed its attitude towards Aibo programmers and has even released a software development kit for Aibo.

based on charging subcompetitive prices for a particular product, but charging supracompetitive prices for complementary products. For a long time, printer manufacturers have been offering their printers at relatively low prices while charging high prices for toner cartridges.[1895] This strategy is advantageous to printer manufacturers as they can acquire a larger customer base due to the low price of the printers.[1896] In addition, it enables them to engage in price discrimination: high–volume printer users have to buy more toner cartridges and thereby pay a higher price for the product combination of printer and toner than low–volume users.[1897]

While this strategy may be beneficial to both manufacturers and consumers,[1898] it is also problematic as the manufacturer has an incentive to foreclose competition on the cartridge aftermarket[1899] and impede innovation by unaffiliated third parties.[1900] Indeed, over the last several years, printer manufacturers have increas-

[1895] In the United States, e.g., Lexmark offers discounts of up to $ 50 on its cartridges, see: Lexmark International, Inc. v. Static Control Components, Inc., No. 02-571-KSF, at 3 (E.D.Ky. 2003), at: http://www.eff.org/IP/DRM/DMCA/Lexmark_v_Static_Controls/20030303- finding-of-facts.pdf. This strategy can be observed in other areas as well: razors are given away to sell the blades, copying machines are sold cheaply to sell the service and replacement parts — a tactic which may lead to antitrust concerns, see: Eastman Kodak Co. v. Image Technical Services, Inc., 504 U.S. 451 (1992).

[1896] See: Varian (2001): 14; Shapiro, Varian (1999): 118–121, 142–143; see also: the complaint in Lexmark International, Inc. v. Static Control Components, Inc., 4, at: http://www.politechbot.com/docs/lexmark.complaint.010803.pdf (Dec. 30, 2002): "*Lexmark's strategy is based on a business model of building an installed base of printers that will then generate demand for Lexmark's printer supplies and services.*"

[1897] See: Pindyck, Rubinfeld (2001): 402; Varian (2001): 14, 16. For a general analysis of price discrimination in proprietary aftermarkets, see: Emch (2003). For an opposing analysis of creating customer lock–ins through proprietary aftermarkets, see: Borenstein, MacKieMason, Netz (2000). In order to prevent customers from having their low–price cartridges refilled by a third–party cartridge manufacturer, Lexmark attaches a shrink–wrap license to its low–price cartridge. According to this license agreement, customers are allowed to use the cartridge only once. When the cartridge is empty, they are required to return the cartridge to Lexmark. See: Lexmark International, Inc. v. Static Control Components, Inc., No. 02-571-KSF, at 3 (E.D.Ky. 2003), *supra* note 1895. Shrink–wrap licenses are often used to support price discrimination and prevent arbitrage. See e.g.: ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449–1450 (7th Cir. 1996).

[1898] See: Varian (2001): 14. For more information on the rather complex economics of laser printer toner cartridges, see: Emch (2002).

[1899] See: Varian (2001): 16; see also: Eastman Kodak Co. v. Image Technical Services, Inc., 504 U.S. 451 (1992). However, whether the foreclosure of aftermarkets leads to antitrust and competition policy concerns depends on the underlying theoretical economic framework. For an assessment of how the Kodak decision of the Supreme Court marks the transition from Chicago School to Post–Chicago School economics, see: Lande (1993); see also: Posner (2001): 236–237; Hovenkamp (1993); Klein (1993); Emch (2002/2003); Borenstein, MacKieMason, Netz (2000).

[1900] As Varian (2002) points out, embedding DRM technologies into ink–jet printers could impede innovative uses of the printers that were not envisioned by

ingly used DRM–related technologies to prevent third–party cartridge manufacturers from entering the cartridge aftermarket with low–priced cartridges. Today, companies such as Hewlett–Packard and Lexmark include sophisticated security chips in their printers to control the data flow between the printers and the toner cartridges. These security systems include challenge–response protocols, encryption systems, secure hashing algorithms, radio communication, custom–designed chips, and custom–designed communication protocols as well as periodic firmware updates, all of which are used to detect toner cartridges that are produced by third–party manufacturers.[1901] If such a toner cartridge is detected, the printer ceases operation.

In February 2003, in a case that could have significant impact on the whole remanufacturing industry, a U.S. district court in Kentucky issued a preliminary injunction against a company called Static Control Components (SSC).[1902] SCC produces microchips that can be installed in third–party toner cartridges. Equipped with these microchips, the toner cartridges can be used in Lexmark laser printers. Although the Lexmark printers try to detect unauthorized toner cartridges by using access control technologies, third–party toner cartridges that are equipped with the SSC microchip can be used in the printers as the microchip circumvents the access control that resides in the printers. As the availability of cheap toner cartridges from third–party vendors threatens Lexmark's business model, Lexmark wanted to force SSC to stop manufacturing its chips. In the preliminary injunction, the district court accepted Lexmark's line of argument and ruled that SSC's chips violated section 1201 (a) (2) of the DMCA as they circumvent an access control that is implemented in a software program located in the printer.[1903]

By using DRM technology and anti–circumvention regulations, Lexmark intended to protect a technology platform (the printer with the access control software running on it) from competitors in complementary markets (the toner

the printer manufacturer, such as using magnetic ink to squirt integrated circuits onto metalized plastic – a technology that could revolutionize integrated circuit production. For an analysis of the importance of enabling consumers to innovate on the basis of mass–market products, see: Hippel, Katz (2002); Thomke, Hippel (2002). This is an example of how increasing technological and intellectual property protection may lead to a concentration and homogenization of innovation; see *infra* text accompanying note 1923.

[1901] See: Static Control Components, Inc., Computer Chip Usage in Toner Cartridges and Impact on the Aftermarket: Past, Current and Future, available at: http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm (last modified Feb. 13, 2003); see also: Complaint in Lexmark International, Inc. v. Static Control Components, Inc., 6–8, *supra* note 1896.

[1902] See: Lexmark International, Inc. v. Static Control Components, Inc., No. 02-571-KSF (E.D.Ky. 2003), *supra* note 1895.

[1903] See Id.: 39–43. The court also opined that SSC's actions were not exempted from liability by the reverse–engineering clause of 17 U.S.C. § 1201 (f), see Id.: 47–48. In January 2003, Static Control Components proposed to the U.S. Copyright Office to create an exemption to the DMCA's anti–circumvention provisions so that Lexmark and other printer vendors could no longer use the DMCA to control the cartridge aftermarket, see: http://www.copyright.gov/1201/2003/petitions/static.pdf (Jan. 23, 2003).

cartridges market).[1904] Similar examples of this strategy include car manufacturers protecting software routines by DRM technology so as to prevent competition in the aftermarket for replacement tires, wiper blades or other automotive parts,[1905] Microsoft allowing software to be run on its Xbox game console only after the software has been signed by Microsoft,[1906] or cell phone manufacturers applying DRM technology to replacement batteries, headsets or car adapters.[1907]

[1904] While, in the U.S., this raises question of the applicability and scope of the anti–circumvention regulations of the DMCA, European legislation and administration attempt to address the problem in other ways. Firstly, according to news reports, the European Commission is considering an investigation of the European printer market from an antitrust perspective. Secondly, the recently adopted European Directive on Waste Electrical and Electronic Equipment (WEEE) includes a provision according to which printer manufacturers are forbidden to use DRM systems to prevent toner cartridges from being re–filled and re–used; see: Article 4 of the Directive 2002/96/EC of the European Parliament and of the Council of January 27, 2003, on Waste Electrical and Electronic Equipment (WEEE), Official Journal of the European Union L 37 (Feb. 13, 2003), 24; see also: Report of the European Parliament Delegation to the Conciliation Committee, Document A5-0438/2002 (Dec. 5, 2002), 11. Although this provision is based on recycling considerations, it could also open competition in the toner cartridge market.

[1905] For some information on the corresponding European legal framework, see: Article 4 (2) and Recital 26 of the Commission Regulation (EC) No. 1400/2002 of July 31, 2002, on the Application of Article 81 (3) of the Treaty to Categories of Vertical Agreements and Concerted Practices in the Motor Vehicle Sector, Official Journal of the European Communities L 203 (1.8. 2002), p. 30. For some information on the situation in the U.S., see the letter of automobile manufacturer and service industry groups to the U.S. Senate, at: http://www.asashop.org/legis/agreement.htm (Sept. 20, 2002); see also: http://www.asashop.org/legis/jointrelease.htm (26.9., 2002); The Motor Vehicle Owner's Right to Repair Act, H.R. 2735, 107th Cong. (2001) (not enacted).

[1906] The Microsoft Xbox is basically a normal PC with some security–related and some game–specific alterations. One of these alterations includes hardware–based mechanisms that allow only software to be run on the Xbox that has been issued a digital certificate by Microsoft; see: Bartholomew (2002); Lehner (2002); Green (2003); Huang (2002a). The Xbox Linux project is trying to create a version of the Linux operating system that could be run on the Xbox. Without any reverse engineering, this could only be achieved if Microsoft signed this particular version of Linux for use on the Xbox. Microsoft has never replied to the requests of the Xbox Linux project to issue such a certificate; see: *Microsoft Approval Sought for Xbox Linux Project* (Feb. 24, 2003), at: http://www.theregister.co.uk/content/54/29439.html; http://xbox-linux.sourceforge.net/articles.php?aid=20030047001211; http://xbox-linux.sourceforge.net/articles.php?aid=20030062171641. According to news reports, Microsoft sells the Xbox below costs and, at least in the beginning, lost as much as $ 110 on every box sold; see: Gaither, Chris: Microsoft Cuts Xbox Price. N.Y. Times, May 15, 2002, at C4; O'Brien (2001): 46. Therefore, Microsoft's attempt to enter the game console market can only be successful if consumers spend enough money in the complementary game aftermarket. As a result Microsoft has strong interests in preventing consumers from buying a heavily subsidized Xbox, installing a third–party operating system and using the Xbox asa normal personal computer. Despite the security measures taken by Microsoft,

DRM in Microsoft's Operating Systems

Another example illustrating how DRM may be used to control complementary markets involves DRM–enabled computer operating systems. DRM systems that are included in operating systems do not only increase the operating systems' security, they may also be used strategically. In particular, they may be used to impede competitors' development of software or hardware that is compatible with the operating system. By keeping details of application programming interfaces (APIs) or communication protocols of a DRM system secret or undocumented, by delaying the disclosure of such information and by assigning DRM encryption keys to hardware manufacturers, software programmers, and content providers on a discriminatory basis, the developer of an operating system may control who is able to create interoperable software applications and who can protect and distribute content in this system.

Therefore, it may seem surprising that the consent decrees, which brought the U.S. antitrust proceedings against Microsoft to an end in late 2002, include "security carve–out" provisions according to which Microsoft is not required

"*to document, disclose or license to third parties*:

a) *portions of APIs or Documentation or portions or layers of Communications Protocols the disclosure of which would compromise the security of a particular installation* [...] *of anti–piracy,* [...] *software licensing, digital rights management, encryption or authentication systems, including without limitation, keys, authorization tokens or enforcement criteria* [...]".[1908]

The consent decrees further state that Microsoft is allowed to condition any license of any of the technologies mentioned

"*on the requirement that the licensee* [...]

---

the Xbox Linux project succeeded in creating a full Linux version that could be executed on an Xbox with hardware modifications (using a so–called "mod chip") in October 2002. In March 2003, the project reportedly succeeded in getting Linux to run on the Xbox without hardware modifications; see: Backer, David (March 31, 2003): Hackers Cracks Xbox Challenge, at: http://news.com.com/2102-1043-997497.html; http://xbox-linux.sourceforge.net.

[1907] See: Anderson (2003a): 2. For an argument of how trusted computing architectures could exacerbate the problem, see *infra* note 2065. Another case that is similar to the Lexmark case involves remote control garage door opener systems. In 2002, a U.S. manufacturer of such systems brought a lawsuit against a manufacturer of remote controls. By claiming that these remote controls circumvented the garage door opener systems' access control technologies, the plaintiff attempted to prevent the competing manufacturer from entering the complementary remote control market. For more information, see: Chamberlain Group, Inc., v. Skylink Technologies, Inc., Amended Complaint, at: http://www.eff.org/IP/DMCA/20030114_chamerberlain_v_skylink_amd_complaint.pdf (Oct. 16, 2002), and Memorandum, available at: http://www.eff.org/IP/DMCA/20030113_ chamerlain_v_skylink_motion.pdf (Dec. 3, 2002).

[1908] See: U.S. v. Microsoft Corp., 2002 Westlaw 31654530, at 6, § III.J (D.D.C. Nov. 12, 2002); State of New York v. Microsoft Corp., 224 F.Supp.2d 76, 272, Appendix B, § III.J (D.D.C. Nov. 1, 2002).

b) has a reasonable business need for a planned or shipping product,
c) meets reasonable, objective standards established by Microsoft for certifying the authenticity and viability of its business,
d) agrees to submit, at its own expense, any computer program using such [technology] *to third–party verification, approved by Microsoft, to test for and ensure verification and compliance with Microsoft specifications for use of the* [technology] [...]".[1909]

There are legitimate reasons for such security carve–out provisions. An unconditional mandate to disclose information about Microsoft's DRM implementation could compromise its security as such information could be used to hack the DRM system.[1910] Nevertheless, the security carve–out provisions in question bear the danger that Microsoft could refuse to disclose or delay the disclosure of information about its DRM architecture on technically unjustified "security" issues.[1911] Although the court emphasized that the consent decrees strike a balance between the legitimate interests of Microsoft and its competitors by limiting the security carve–out to relatively narrow circumstances and that the provisions do not authorize Microsoft to discriminate against competitors,[1912] it is an open question whether this particular solution of the tension between security and competition will work in practice.

Region Coding, Competition and the Free Movement of Goods

The final example which illustrates how DRM technology can be used to control complementary markets involves technologies that separate markets geographically. Most DVD players and DVD discs include a so–called "regional code playback control". This system divides the world market into six distinct geographic regions. It is able to prevent, for example, European consumers from playing U.S. DVDs on a European DVD player.[1913] Similar systems can be found in Sony's Playstation game consoles[1914] and in various software applications.

[1909] See: Id.

[1910] See: U.S. v. Microsoft Corp., 231 F.Supp.2d 144, 193–195 (D.D.C. Nov. 1, 2002); State of New York v. Microsoft Corp., 231 F.Supp.2d 203, 251–252 (D.D.C. Nov. 1, 2002). Whether this statement is actually true depends on whether one believes that achieving security by secrecy or obscurity is a good engineering approach. Security by obscurity directly contradicts the widely–accepted Kerckhoff principle; see *supra* note 1848; see also: State of New York v. Microsoft Corp., 224 F.Supp.2d 76, 238–239 (D.D.C. Nov. 1, 2002).

[1911] See also: State of New York v. Microsoft Corp., 224 F.Supp.2d 76, 239 (D.D.C. Nov. 1, 2002). For a related problem in trusted computing architectures, see *infra* text accompanying note 2018.

[1912] See: U.S. v. Microsoft Corp., 231 F.Supp.2d 144, 193–195 (D.D.C. Nov. 1, 2002); State of New York v. Microsoft Corp., 224 F.Supp.2d 76, 239 (D.D.C. Nov. 1, 2002).

[1913] For more information, see: Bechtold (2002): 110–112.

[1914] See: Sony Computer Entm't Am., Inc. v. Gamemasters, Inc., 87 F.Supp. 2d 976, 981 (N.D.Cal. 1999). Whether the circumvention of the Playstation's regional code management control actually infringes anti–circumvention regulations is not an easy question. In July 2002, an Australian federal court ruled that the

Rights holders have various legitimate reasons for using regional code management systems.[1915] Nevertheless, regional code management systems in hardware[1916] or software[1917] platforms can also be used to exercise control over the complementary market in which digital content[1918] is processed on top of the platform. Both the European and the Australian competition authorities have investigated whether the regional code management system in DVD players is used to overcharge European and Australian customers for DVD discs compared to U.S. customers.[1919] Furthermore, regional code management systems can undermine the free movement of goods which intellectual property law protects by the exhaustion principle.[1920]

Conclusion

As the four examples given illustrate, DRM technologies and anti–circumvention regulations cannot only be used to fight piracy. Rather, by wrapping technology platforms in a DRM system, DRM can be used to control downstream markets and channel innovation. How DRM policy should deal with such cases is not an easy question. On the one hand, some protection for DRM platform developers may be desirable in order to provide sufficient incentives for the development of the platform.[1921] On the other hand, such incentive structures have to be carefully drafted and limited in order to not put too many stumbling blocks along the path to well–functioning competition and cumulative innovation.[1922] Highly protective intellectual property regimes may lead to an undesired concentration,

distribution of so–called "mod chips" which circumvent the Playstation's regional code management does not violate Australian anti–circumvention regulations, Kabushiki Kaihsa Sony Computer Entm't et al. v. Eddy Stevens, (2002) F.C.A. 906. For a related case in the U.K., see: Sony Computer Entm't, Inc. v. Paul Owen, 2002 Entertainment and Media Law Reports 34.

[1915] See: Marks, Turnbull (2000): 213; Answer of the European Commission to Written Questions E-1509/00 and E-1510/00, Official Journal of the European Communities C 53 E (Feb. 20, 2001), 158; Bechtold (2002): 110 note 557.

[1916] Such as DVD players.

[1917] Such as operating systems.

[1918] Such as video files or software applications.

[1919] See: Answer of the European Commission to Written Questions E-1509/00 and E-1510/00, *supra* note 1915; Answer of the European Commission to Written Question E-2371/00, Official Journal of the European Communities C 103 E (Apr. 3, 2001), 138; Letter of Cecilio Madero, DG Competition of the European Commission, to Lars Gaarden, at: http.//www.eurorights.org/dvd/E-1509-comments-answer.html (Mar. 14, 2001); Australian Competition & Consumer Commission, ACCC Consumer Express (Feb. 2002), available at: http://www.accc.gov.au/pubs/Publications/Journals/consumer_express/feb2002.htm.

[1920] In the context of DVDs, this is not a problem, however, as the world regions used by the regional code management system seem to be larger than the geographical areas in which intellectual property rights become exhausted. This would change, however, if the principle of international exhaustion would apply; see only: Chiappetta (2000).

[1921] See: Samuelson, Scotchmer (2002): 1621–1622.

[1922] See: Id.: 1625–1626.

commercialization, and homogenization of information production.[1923] Solving this tension between DRM protection by intellectual property rights and DRM competition leads to the general problem how intellectual property protection and competition policy interrelates and interacts.[1924] More particularly, it is troublesome that anti–circumvention regulations are increasingly used in circumstances for which they were clearly not intended.

VI DRM and Standardization

The more mature DRM technology becomes, the more efforts are made to standardize various DRM components. This section describes several legal and policy problems that emerge when DRM becomes standardized.

VI.1 Standardization by the Private Sector

DRM systems are subject to indirect network effects.[1925] The more content is available in a particular DRM system, the more consumers will buy equipment that is compatible with this system.[1926] Yet, if more consumers buy such equipment, more content will be made available for the DRM system, because demand increases. After passing a certain "tipping" point, this may lead to so–called "positive feedback" effects: while one DRM system becomes more and more dominant in the market, competing DRM systems are effectively driven out of the market.[1927] Network effects can lead to *de facto* standards, even monopolies in a market.[1928]

In a market with such structures, due to significant first–mover advantages, it may be rational for a company to invest heavily in the rapid acquisition of market share as early as possible.[1929] However, depending on various circumstances such as size and structure of the market, it may also be more effective to create

[1923] See: Benkler (2002).

[1924] See only: The documents of the hearings by the Federal Trade Commission and the U.S. Department of Justice on "Competition and Intellectual Property Law and Policy in the Knowledge–Based Economy" in 2002, http://www.ftc.gov/opp/intellect.

[1925] In a market shaped by positive network effects, a consumer's utility of a good increases with the number of other agents consuming the good, see: Katz, Shapiro (1985). With indirect network effects, the effect is mediated not by the good that is subject to the network effect, but by a complementary good; see: Shy (2001): 52. The existence, importance, and impact of network effects is controversial on a theoretical as well as an empirical level; see: Liebowitz, Margolis (1994): 149; Lemley, McGowan (1998); Bechtold (2002): 351–364.

[1926] This is comparable to the indirect network effects of operating systems: the more application programs are available for a particular operating system, the more consumers will buy this system; see: Shy (2001): 52. Indirect network effects also occur with computer hardware, video recorders and CD players.

[1927] See: Shapiro, Varian (1999): 175–179; Lemley, McGowan (1998): 496–497.

[1928] See: Katz, Shapiro (1994): 105.

[1929] See: Id.: 107; Lemley, McGowan (1998): 495, 504.

a private industry organization open to all which develops a common standard to which all market participants adhere. If the members of this organization have a significant market share their adoption of the standard may also produce the positive feedback effect described above.[1930] It is therefore understandable that, over the last few years, many working groups, industry organizations and standardization bodies have been created or became interested in standardizing DRM components. All these efforts attempt to contribute to a comprehensive DRM architecture that is seamlessly integrated into nearly all consumer electronics devices and computer equipment. They hope to create widely accepted DRM industry standards, because the single company or the group of companies that push the efforts have a significant market share, so that their adoption of a standard would create the positive feedback effect described above.

Examples of DRM Standards

The acronyms of DRM standardization bodies are as manifold as their number is staggering. The "Copy Protection Technical Working Group" (CPTWG), for example, played a major role in standardizing copy–protection and DRM components of the DVD disc. It is still one of the most important working groups in the DRM field.[1931] In June 2002, the "Broadcast Protection Discussion Group" (BPDG), which is a working group of the CPTWG, issued its final report recommending the inclusion of a "broadcast flag" into digital TV broadcasting in order to forestall unauthorized copying.[1932] The "Secure Digital Music Initiative" (SDMI), which was founded in 1999, started with fanfare, but failed to deliver any DRM standards that would be implemented in the market on a wide–scale basis.[1933]

Since 1995, the Dublin Core Metadata Initiative has been working on a standard for a rudimentary set of metadata.[1934] In early 2002, OASIS — a group responsible for crafting XML interoperability standards — announced the creation of a technical committee that would standardize a rights expression language for DRM systems.[1935] Intel, IBM, Matsushita and Toshiba (the so–called "4C" companies) have created the "Content Protection for Recordable Media" (CPRM)

[1930] See: Lemley, McGowan (1998): 516. Although network effects can lead to a standards monopoly, this is not inherently bad from an economic perspective. If, in a particular market, having a single standard is more efficient than having several competing standards, then this is desirable; Id.: 497. However, in such a market, it is not guaranteed that the "optimal" standard will be adopted. Network effects can lead to a lock–in into a "suboptimal" standard that neither consumers nor producers can escape due to high switching costs and collective action problems; see: Shy (2001): 4–5; Lemley, McGowan (1998): 497 (who also point out that this begs the question what an "optimal" standard actually is).

[1931] See: Marks, Turnbull (2000): 204–205, 208.

[1932] See: Broadcast Protection Discussion Subgroup, Final Report to the Copy Protection Technical Working Group, available at: http://www.cptwg.org/Assets/BPDG/BPDG%20Report.DOC (3.6. 2002).

[1933] For some information on SDMI, see: Marks, Turnbull (2000): 210–211; Levy (2000).

[1934] See: Paskin (1999): 1218–1219.

specification which is intended to protect content when recorded on physical media such as rewriteable DVDs or memory cards.[1936] The "Motion Picture Expert Group" (MPEG) has been dealing with DRM–related questions since MPEG-4. Further standards in the DRM field include the "Digital Transmission Content Protection" (DTCP),[1937] the "High–Bandwidth Digital Content Protection" (HDCP),[1938] the "Content Scramble System" (CSS),[1939] the "Copy Generation Management System" (CGMS),[1940] the envisaged "DVB Content Protection and Copy Management" (DVB CPCM),[1941] the DRM–related parts of the OpenCable specification,[1942] the still uncertain video watermark standard for DVD players,[1943] and various systems of regional code playback control.[1944]

More recently, two new standardization efforts have entered the arena: the Trusted Computing Platform Alliance (TCPA) and Microsoft's Palladium initiative. Both efforts attempt to implement a "trusted computing architecture".[1945] Such architecture uses components which ensure that a computing platform always behaves in the expected manner for the intended purpose. In particular,

[1935] See: http://www.oasis-open.org/committees/rights. Indeed, the standardization of a "general–purpose" REL may be the most important standardization effort in the DRM field which could have impact on areas far beyond traditional DRM, such as web services and the semantic web.

[1936] See: Taylor (2000): 193–195, 488–489; http://www.4centity.com/tech/cprm.

[1937] DTCP protects the transmission of digital content between different hardware components, e.g., between a computer and a digital video recorder. See: http://www.dtcp.com; Marks, Turnbull (2000): 208.

[1938] HDCP protects the transmission of digital content between a computer system and a connected monitor; see: http://www.digital-cp.com; Taylor (2000): 199–200, 490. In 2001, severe weaknesses in the security implementation of HDCP were demonstrated; see: Crosby et al. (2001).

[1939] CSS is an authentication and encryption system that was designed by Matsushita and Toshiba to prevent the making of digital copies of DVDs. In fall 1999, CSS was hacked by a software program named DeCSS. For more information on CSS, see: Taylor (2000): 481; Marks, Turnbull (2000): 205–206, 211–213; Universal City Studios, Inc. v. Reimerdes, 111 F.Supp. 2d, 294, 308–313 (S.D.N.Y. 2000).

[1940] See: Taylor (2000): 197.

[1941] See: Digital Video Broadcasting Forum, Call for Proposals for Content Protection & Copy Management Technologies, available at: http://www.dvb.org/dvb_technology/whitepaper-pdf-docs/cfp_cp_cm.pdf (July 5, 2001).

[1942] See: CableLabs, OpenCable POD Copy Protection System, available at: http://www.opencable.com/downloads/specs/OC-SP-PODCP-IF-I08-021126.pdf (Nov. 26, 2002).

[1943] In August 2002, the DVD Copy Control Association (DVDCCA) was unable to reach an agreement on the selection of a watermarking technology for copy and playback control in DVD players and drivers; see: Motion Picture Association of America, Content Protection Status Report III, available at: http://judiciary.senate.gov/special/mpaa110702.pdf (Nov. 7, 2002).

[1944] See *supra* text accompanying note 1913. For a detailed overview of DRM standards, see: Lyon (2002); Bechtold (2002): 101–126.

[1945] Anderson aptly points out that the goal of such architectures is not to be "trusted", but to be "trustworthy"; see: Anderson (2003a): 4.

the architecture provides evidence about the integrity and authenticity of the platform to both the platform's owner and to arbitrary third parties. Thereby, this architectural approach attempts to increase trust in the computing environment.[1946] If widely implemented, trusted computing architectures could alter the IT infrastructure landscape as we currently know it in considerable ways. They also raise new DRM–related problems, which will be described in the remainder of this subsection. As overview descriptions of TCPA and Palladium are still very rare, the article will first describe the underlying technologies in some detail.

Trusted Computing Platform Alliance (TCPA)

TCPA is an industry working group that was initially formed by Compaq, Hewlett–Packard, IBM, Intel, and Microsoft in 1999 and now boasts over 200 participating companies.[1947] Based on ideas developed in the mid 1990's,[1948] its goal is to create a standard for a trusted hardware computing platform. Although it is currently primarily focused on the personal computer architecture, the TCPA specification could, in the future, also be implemented on servers and mobile devices such as music players, cell phones or PDAs.[1949]

TCPA is a specification for computing platforms that creates a foundation of trust for software processes, based on a small amount of special hardware within such platforms.[1950] It enables three features that are of particular interest for DRM: it enables a secure attestation of the state of a platform, it can be used to create trusted platform identities, and it provides protected storage.

Platform State Attestation

TCPA attempts to increase trust in the computing environment. It starts from the assertion that it is impossible to rely on a software process to provide reliable information unless one can be certain that this process is working as expected.[1951] Therefore, TCPA provides a mechanism by which the state of all

[1946] See: Pearson (2003): 31, 41. For more information on the goals of trusted computing, see: Id.: 4–42.

[1947] For a list of the TCPA members, see: http://www.trustedcomputing.org/ tcpaasp4/members.asp. In April 2003, the formation of a new "Trusted Computing Group" (TCG) was announced. TCG is supposed to supersede the TCPA group, using the TCPA specifications as a starting point. For more information, see: http://www.trustedcomputinggroup.org. By creating a new standards body, various organizational changes and more formal structures could be introduced, such as becoming incorporated, using a RAND (reasonably and non-discriminatory) patent license policy, switching to the principle of majority rule, and introducing a logo program to signal compliance of specific implementations with TCG specifications.

[1948] See, e.g.: Arbaugh, Farber, Smith (1997). This was preceded by developments of secure systems in the military sector which started in the 1960's; see: Anderson (2001); *Kuhlmann, Gehring* within this book on page 178.

[1949] For more information on TCPA, see: http://www.trustedcomputing.org; Pearson (2003); TCPA (2002a); TCPA (2001): Par. 6.1; see also: Pfitzner (2003); Wintermute (2003).

[1950] See: Pearson (2003): 5.

[1951] See: Id.: 236.

software applications running under a particular operating system on a particular hardware can be attested to in a trustworthy manner. This mechanism performs a series of measurements that record summaries of software that has executed (or is executing) on the platform.

As a foundation for this mechanism, TCPA introduces two so–called "roots of trust" into the PC architecture:[1952] the "Core Root of Trust for Measuring Integrity Metrics" (CRTM) and the "Trusted Platform Module" (TPM).[1953] The TPM is a chip that is separate from the main processor of the PC, but is securely attached to the PC mainboard.[1954] It is a self–contained processing engine with special capabilities such as a random key number generator, a digital signature engine, a hash function, and asymmetric encryption.[1955] It can also be used to securely store arbitrary secrets.[1956] The TPM is required to be tamper–resistant:[1957] it has to resist all forms of software attacks and a specified set of hardware attacks.[1958] The CRTM, which does not have to be tamper–resistant, is typically implemented as part of the PC BIOS.[1959] It is the basis for a reliable measurement of platform integrity information.

Both the TPM and the CRTM are "roots of trust", i.e. the only components in the platform that are implicitly trusted.[1960] The main idea behind TCPA is to gradually expand trust from these roots to other components of the platform.[1961] In a typical PC booting process, this expansion of trust works as follows. If a PC starts its booting process, the CRTM inside the BIOS measures its own integrity and the integrity of the entire BIOS. It stores a condensed summary of these integrity metrics inside the TPM in a tamper–resistant "Platform Configuration Register" (PCR).[1962] Once the integrity metrics are stored in the

[1952] For clarity reasons, only a TCPA implementation on the PC architecture will be discussed in the following.

[1953] In fact, the TPM consists of the "Root of Trust for Storing Integrity Metrics" (RTS) and the "Root of Trust for Reporting Integrity Metrics" (RTR). However, these terms are rarely used; see: Pearson (2003): 63.

[1954] Often, but not necessarily, the TPM is soldered onto the motherboard. By contrast, IBM has implemented its TPM on a small daughter board that plugs directly into an LPC bus connector on the motherboard. The daughter board is equipped with several physical security features. This enables users to physically pull the TPM out of the motherboard, thereby fully disabling TCPA on their computers. See also: Pfitzner (2003): 13.

[1955] See: Pearson (2003): 30, 36, 180–201.

[1956] See *infra* text accompanying notes 1976–1985.

[1957] It is basically an enhanced smart card, see: Pearson (2003): 67.

[1958] See: Pearson (2003): 63, 68, 227. TCPA does not intend to secure the TPM against all possible hardware attacks, as such security is unachievable; see: Id.: 35. The system "*provides tamper evidence only. It provides no protection against physical threats such as simple power analysis, differential power analysis, external signals, or extreme temperature. Physical protection is assumed to be provided by the environment*", TCPA (2002b): 16.

[1959] See: Pearson (2003): 63–64.

[1960] See: Id.: 226–228, 235. For the question why these components should be implicitly trusted, see *infra* text accompanying notes 2031–2034.

[1961] See: Pearson (2003): 226.

PCR, they cannot be altered or deleted until the platform is rebooted.[1963] The CRTM then passes control to the BIOS, which checks the integrity of the operating system loader and stores these integrity metrics in another PCR. The BIOS then passes control to the operating system loader, which measures the integrity values of the operating system, stores this information in another PCR, and passes control to the operating system. Finally, the operating system measures the metrics of its components and of *any* software application that will be loaded onto the platform and stores this information in yet another PCR. If, subsequently, another software application is loaded, the operating system updates the integrity measurement information in this PCR.[1964]

The central idea behind this approach is that each component in the platform measures the next component in the chain and stores this value in such a way that it cannot later be modified by another component.[1965] This approach ensures that each binary code is measured and recorded before it is executed. As a result, rogue software cannot hide its presence in such a platform.[1966] Effectively, TCPA enables a "chain of trust" to be constructed from the roots of trust (the CRTM and TPM) to the applications executing on the operating system.[1967]

This mechanism to securely attest to the software state of a platform can be used for various purposes. Firstly, it can be used by local and remote entities to check the integrity of the platform. In a so–called "integrity challenge", the challenger compares the *actual* state of the platform (as reported by the trusted platform in its integrity metrics) with the *expected* state of the platform.[1968] Information about the expected state can be retrieved from so–called "Validation Entities" (VEs). VEs issue certificates for software applications which state that, if this application is executed on a trusted platform, the platform will be in a particular state.[1969] If the challenger compares this information with the integrity metrics as reported by the trusted platform, he can judge whether the software has been tampered with.[1970]

Secondly, the mechanism to attest a platform state can also be used to enable "secure booting". If, during the booting process of a PC, the TPM detects that the system does not boot as it should — because, for example, it boots additional software whose security is not certain — it reports this information to a non–TCPA software component that may then stop the booting process. Secure boot

[1962] For more information on PCRs, see: Id.: 67–68, 138–140.

[1963] See: Id.: 36.

[1964] See: Id.: 75, 235.

[1965] See: Id.: 87.

[1966] It is questionable, however, whether this also holds true in the context of data that is executed under scripting languages such as VBScript; see, e.g.: Vaughan–Nichols (2003): 18–19 (citing Ross Anderson).

[1967] See: Pearson (2003): 72, 225–238.

[1968] See: Id.: 76–77.

[1969] See: Id.: 235. More accurately, VEs are third parties responsible for certifying that, if a software application is executed, a particular integrity (i.e. hash) value is measured and reported on the platform; see: Id.: 243.

[1970] See: Id.: 244.

makes sure that a computer system is either booted into a secure software state or that it is not booted at all.[1971]

Trusted Identities

TCPA also enables the creation of trusted identities. Although each TCPA–enabled PC contains a unique "endorsement certificate", this is not used for identification purposes.[1972] Rather, users of a TCPA–enabled PC may create several pseudonymous identities by receiving certificates from so–called "Privacy Certification Authorities" (Privacy–CA).[1973] If a user possesses several such identities, they can only be correlated among each other by the Privacy–CA that issued the identities. No one else has enough information to correlate trusted platform identities.[1974]

As the user can choose between competing Privacy–CAs, the TCPA expects that he will be able to choose a Privacy–CA which does not correlate his various identities under any circumstance. Therefore, the TCPA argues that its architecture protects privacy interests to the largest extent possible.[1975]

Protected Storage

Finally, TCPA enables protected storage. The TPM is a secure portal to potentially unlimited amounts of protected storage.[1976] In the tamper–resistant TPM chip, a so–called "Storage Root Key" (SRK) is stored. The SRK[1977] is never revealed outside the TPM. It can be used to securely encrypt and decrypt arbitrary data, including content and encryption keys (so–called "TPM protected objects").[1978]

In regards to DRM, three features of protected storage are important to highlight: Firstly, a TPM protected object can be "sealed" to a particular software state on a platform. As a result, the object can only be accessed if the platform is in an agreeable state.[1979] This makes it possible to restrict the conditions

[1971] See: Id.: 90, 140. Yet, secure boot is not the normal operation of TCPA. Rather, a TCPA platform normally uses an "authenticated boot process", in which the platform could end up in any arbitrary state, but that state will be recorded and can be reported; see: Id.: 90.

[1972] But it is used in the creation of trusted identities, see *infra* text accompanying note 2059.

[1973] See: Id.: 80–84; see also: Arbaugh (2002): 78; Pfitzner (2003): 13. The TCPA specification also allows users to create various identities with different Privacy–CAs; see: Pearson (2003): 233.

[1974] See: Pearson (2003): 62, 78, 82.

[1975] See: Id.: 31–32, 82; but see *infra* text accompanying notes 2057–2064.

[1976] See: Id.: 38, 85, 145–146.

[1977] More precisely, the private key part of the asymmetric SRK key pair, see: Id.: 85.

[1978] See: Id.: 38. The TCPA specification distinguishes between "TPM protected data objects" and "TPM protected key objects", see: Id.: 145. The protected objects are not stored in the TPM itself; the TPM is not a memory device, but merely a portal to any storage medium, Id.: 58, 85. See also: Pfitzner (2003): 6–7.

[1979] This is done by storing the objects alongside target PCR values, which store summaries of the software state of a platform. The TPM reveals the protected

under which data can be used and accessed on a remote computer.[1980] In a DRM system, this feature could be used by content providers to make sure that their content may only be accessed by consumers if their devices are in a secure state.[1981]

Secondly, TCPA distinguishes between "migratable" and "non–migratable" objects. While the first kind of object can be moved to another platform, the second kind is cryptographically bound to a specific platform.[1982] Non–migratable objects are particularly important in the DRM field as they can be used to bind content to a particular computer.[1983] They are locked to this computer and can never be duplicated. If, in such a system, a hacker succeeded in copying content to another computer or device, this would be futile as the content could not be decrypted on the other computer.[1984]

Thirdly, in the TCPA architecture, no global secrets exist. Every trusted platform is equipped with distinct keys. If an attacker succeeds in hacking a platform, the overall security of the TCPA architecture is not compromised as other platforms are not affected by this attack.[1985] This increases the overall security of a DRM system that is built on top of TCPA.

---

object only if the current PCR values match the PCR values that are stored with the object; see: Pearson (2003): 48, 87, 153.

[1980] See: Id.: 47.

[1981] See: Id.: 87. See also: Id.: 237: "*Local components of the platform can therefore be designed to rely on the TPM's trustworthiness to protect themselves against potential threats from their own execution environment. This in turn will allow entities external to the platform to trust that an application's secret data can be protected to be only available when the* [trusted platform] *has been able to establish a given chain of trust from the start of its boot process up to the execution of the application itself. If a chain of trust is broken by integrity metrics that report unknown software, or software that does not cooperate in building the chain of trust further, the protected data* [...] *will not be accessible on the platform.*"

[1982] See: Id.: 47–48, 165–178. In the case of a non–migratable object, the private key that is necessary to decrypt the non–migratable object is only known to the TPM that created the private key and is never revealed outside of the TPM; see: Id.: 86, 149.

[1983] See: Id.: 86–87.

[1984] Non–migratable objects can, however, be *moved* to another platform with the cooperation of the platform manufacturer, see: Id.: 168–169. Binding content to a particular device by cryptographic tools is not a novel approach. Rather, both the CPRM and CPPM standards bind content to unique storage media as well; see: Bechtold (2002): 113.

[1985] Therefore, TCPA is "BORE"–resistant ("break once, run everywhere"); see: Pearson (2003): 58, 227. This is true for Microsoft Palladium as well, see: Microsoft Corp. (2003). However, two caveats must be made. Firstly, achieving BORE–resistance is the theoretical idea. Whether this actually works out in practice, is another question. Secondly, if trusted platform manufacturers include an optional TCPA mechanism that enables a remote upgrade of their platforms, there is a danger that all platforms of each manufacturer are equipped with one common private key to initiate the upgrade process; see: Pearson (2003): 187. This could increase the overall vulnerability of the TCPA security architecture.

Microsoft Palladium

Although TCPA requires some modifications to existing operating systems,[1986] the specification does not include any standards for these software layers.[1987] One future operating system that could build upon the TCPA hardware architecture is Microsoft Palladium. While it is a slight simplification,[1988] one can think of TCPA as a standard for a tamper–resistant hardware environment, while Palladium provides a tamper–resistant operating subsystem that builds on such a hardware environment.[1989] Initially named after the mythical statue that guarded Troy, Palladium is likely to be incorporated into future versions of Microsoft Windows. Perhaps when Microsoft was reminded that, after Odysseus and Diomedes had succeeded in stealing Palladium from the temple of Athene in Troy, the Greek were able to capture the city some 3000 years ago, Microsoft announced in January 2003 to rename its Palladium project to "Next–Generation Secure Computing Base" — clearly something that did not exist in the Ancient World. Nevertheless, this article will use the former name as it is still widely used and easier to grasp than the acronym NGSCB.

Although little detailed information about Palladium is publicly available at the time of this writing,[1990] some of the rough outlines of the system are already known. Palladium is based on the idea of system compartmentalization.[1991] Whereas one section of a computer's memory is not affected by Palladium, another section is turned into a trusted space. In this space, Palladium uses two

[1986] Indeed, without appropriate support by an operating system, TCPA would not enable a secure DRM, see: Arbaugh (2002).

[1987] See: Pearson (2003): 238.

[1988] The Palladium initiative does not only address software issues, but also includes hardware components. Currently, the TCPA specification does not support all the primitives that are needed for Palladium, and the privacy model of both architectures is different. Therefore, it used to be unclear whether Palladium will actually be built on top of TCPA; see: Peter Biddle, posting to cryptography@wasabisystems.com, available at: http://www.cl.cam.uk/~rja14/biddle.txt (Aug. 5, 2002). Meanwhile, however, Microsoft has announced to use a future version of TCPA as a hardware foundation for Palladium; see: Microsoft Corp. (2003). The forthcoming version 1.2 of the TCPA speficiation will include several features to allow Palladium to be built on top of TCPA. For an overview of some of the changes that are expected in version 1.2 of the TCPA specification, see: Grawrock (2002). Nevertheless, TCPA may be used in combination with any operating system that meets the requirements of the TCPA specification; see also: *Kuhlmann, Gehring* within this book on page 178.

[1989] In the Palladium nomenclature, the tamper–resistant hardware components on which the Palladium software components build are called "Security Support Components" (SSC), see: Microsoft Corp. (2003).

[1990] See: Microsoft Corp. (2002); Wintermute (2003); Schoen (2002). This article was finished in April 2003. Therefore, the more detailed technical description of Palladium which has been announced by Microsoft for May 2003 could not be considered.

[1991] System compartmentalization is a feature that distinguishes Palladium from TCPA in its current version 1.1b. For more information on system compartmentalization, see: England, Peinado (2002): 346.

components. The first component, called "Nexus" (formerly known as "Trusted Operating Root", TOR), is essentially the kernel of the Palladium–isolated software stack.[1992] It provides basic services to the second component, so–called "trusted agents" (also known as "Nexus Computing Agents", NCAs). These are trusted software applications that call the Nexus for security–related services and critical general services such as memory management. Together, both components provide protected storage, binding data to particular platforms,[1993] secure encryption services, migratable encrypted objects, state attestation, authenticated boot facilities, and trusted pseudonymous identities.[1994]

While these functionalities resemble many of the features offered by TCPA, Palladium provides some additional features that are not offered by TCPA in its current version.[1995] By using hardware–based "curtained" memory, Palladium ensures that each Palladium–aware application has its own execution memory space.[1996] Thereby, Palladium can securely isolate software applications from each other and prevent the modification of applications or the snooping of their memory space by other adversarial applications.[1997] Furthermore, Palladium creates a tamper–resistant communication path from the keyboard and mouse to software applications as well as from these applications to the computer display.[1998]

In general, Palladium makes it possible to isolate software applications and store data for them while ensuring that only software trusted by the data's owner has access to the data.[1999] These features could make Palladium very attractive to content providers who want to distribute their content in a DRM system.

DRM in a World of Trusted Computing

Although it is sometimes implied by opponents of trusted computing architectures, the foremost goals of such architectures do not have anything directly to do with DRM. Rather, trusted computing architectures could lead to a significant increase of the general IT security. The areas where such architectures could be useful are nearly innumerable.[2000]

[1992] See: Microsoft Corp. (2003).

[1993] See: Schoen (2002) (describing the binding to a particular hardware system in the Palladium architecture).

[1994] See: Microsoft Corp. (2002/2003).

[1995] However, it is expected that the forthcoming version 1.2 of the TCPA specification will include these features so that Palladium can use TCPA as a hardware foundation.

[1996] See: Microsoft Corp (2003). For the related idea of system compartmentalization, see *supra* text accompanying note 1991.

[1997] See also: England, Peinado (2002): 346, 351.

[1998] See: Microsoft Corp (2003).

[1999] See: Id.

[2000] See: Pearson (2003): 43–56, 251–276; see also: Safford (2002b); Pfitzner (2003): 10–11; but see: Anderson (2003a): 6–7 (doubting whether trusted computing will be valuable in the corporate and government sector).

Nonetheless, trusted computing architectures could be very attractive to DRM designers as they could serve as a firm foundation for a secure DRM system.[2001] On top of a trusted computing platform, a DRM system could use hardware–based tamper–resistant mechanisms for encryption, integrity and authenticity checking, policy enforcement and key revocation. By using curtained memory, trusted computing platforms could isolate applications from each other so that rogue software could not snoop or modify DRM audio or video player software.[2002] This is not to say that such a DRM system would be 100% secure. But it would probably be much more secure than current software–based DRM implementations.

However, whether trusted computing architectures will actually be used as a foundation for a secure DRM system is currently not certain by any means. Firstly, as was noted above, TCPA and Palladium do not provide utmost security against hardware attacks by the local owner of the trusted platform.[2003] At least initially, TCPA was focused on increasing security in the enterprise computing environment, where distrusting local platform owners is not the most important security concern. Therefore, even proponents of TCPA argue that TCPA is not particularly suited to DRM, which has to protect data against the local platform owner as well.[2004]

Secondly, if a DRM systems developer chose to use trusted computing architectures to securely attest the state of computing platforms, this could render the DRM system incredibly complex. As was described above, in a trusted system, any change to the BIOS, the operating system and any software application running on the system has to be reported in the integrity metrics storage.[2005] If a content provider wanted to use these metrics to decide whether a particular platform is in a secure state so that the protected content could be transmitted to the platform, he would have to be able to interpret the countless different integrity metrics resulting from the myriad hardware platforms, operating systems, software patches, and software applications running on the platform.[2006] The innumerable combinations of hardware and software components could pose a

---

For some of the motivations of IT companies to develop TCPA, see: *Kuhlmann, Gehring* within this book on page 178; Anderson (2003a): 8–9.

[2001] See: Microsoft Corp. (2003); Erickson (2003): 38–39; Anderson (2003a): 3; *Kuhlmann, Gehring* within this book on page 178. For an example of how DRM on top of TCPA might look like, see: Huang (2002): 103–104.

[2002] See: Microsoft Corp. (2003).

[2003] Concerning TCPA, see *supra* text accompanying note 1958. Concerning Palladium, see: Microsoft (2003) (stating that Palladium "*is not designed to provide defenses against hardware–based attacks that originate from someone in control of the local machine*").

[2004] See: Safford (2002a): 3. See also: TCG (2003), FAQ no. 22 ("*It is not TCG's intention to address DRM requirements. As a result, the specifications do not include provisions to prevent owner tampering*"); Pfitzner (2003): 16. However, this weakness may be reduced with the introduction of version 1.2 of the TCPA specification.

[2005] See *supra* text accompanying notes 1960–1964.

[2006] See: Safford (2002b): 5.

major stumbling block to the utilization of trusted computing platforms in the consumer sector.[2007] These problems do not exist in the enterprise sector where, usually, a more limited and homogeneous set of hardware and software components is used.[2008]

Whether consumer–oriented DRM, on which this article focuses, will use trusted computing platforms to increase its security, is therefore an open question.[2009] Furthermore, it is unclear at this time whether trusted computing will be implemented and how successful it will be in the marketplace. Therefore, one has to be careful at this time not to jump to erroneous conclusions about the implications of trusted computing in general and its relationship to DRM in particular. Despite these reservations, in the following, the article assumes that consumer–oriented DRM systems will use trusted computing platforms as their foundation. Therefore, in the remainder of this subsection, some of the DRM–related dangers arising from trusted computing architectures such as TCPA and Palladium will be discussed.[2010]

Dangers Related to Competition Policy and Institutional Arrangement
Trusted computing platforms could be used by companies developing the hard– and software components of the platform to thwart competition.[2011] As was described above,[2012] TCPA can be used to "seal" data to a particular software state on a platform. In a DRM system, this feature could be used by content providers to make sure that their content may only be accessed by consumers if their devices are in a secure state. However, it could also be used to seal data to a particular operating system, platform configuration, or software application.[2013] Software companies could develop proprietary file formats for their

[2007] Therefore, Microsoft's plan to use system compartmentalization in order to limit the trusted space to the really security–sensitive applications seems a promising approach to reduce complexity of the trusted platform operation.

[2008] But see: Anderson (2003a): 6–7 (doubting whether trusted computing will be valuable in the corporate and government sector).

[2009] See also: Id.: 7 (doubting whether the increased security provided by trusted computing will actually lead to viable business models).

[2010] This article does not address dangers or advantages of TCPA and Palladium that are not related to DRM. For a document of strong opposition against TCPA and Palladium, see: Anderson (2003); for some valid criticism of Anderson's paper, see: Safford (2002a); Pfitzner (2003): 21–22.

[2011] In November 2002, the German government noted that the introduction of TCPA and/or Palladium might increase entry barriers for competing software developers, in particular for open–source developers; see: Antwort des Parlamentarischen Staatssekretärs Gerd Andres vom 26. 11. 2002 auf die Frage der Abgeordneten Dr. Martina Krogmann, Bundestags–Drucksache 15/116 vom 29. 11. 2002, S. 18, 19. The European Commission has expressed similar concerns, see: John Lettice, European Antitrust Chief Concerned over MS Palladium?, available at http://www.theregister.co.uk/content/4/25988.html (July 2, 2002). See also: Kleine Anfrage der CDU/CSU-Fraktion "Auswirkungen des 'Trusted Platform Module' und der Software 'Palladium'", Bundestags–Drucksache 15/660 vom 17. 3. 2003, S. 1 ff.

[2012] See *supra* note 1979–1981.

[2013] See: Pearson (2003): 87.

applications, preventing competitors from building possibly superior applications that can read this file format and thereby interoperate.[2014] As the costs of converting files would be significantly increased,[2015] this could deter customers from switching to competing applications, operating systems and even hardware platforms in the first place.[2016] Content providers could make sure that their content is only accessible with a particular proprietary player. In general, sealed storage could hamper competition in the hardware, operating system and the software application markets. Trusted computing could prove a powerful tool to create customer lock–in and artificially increase switching costs.[2017]

Therefore, the future DRM policy debate will deal with questions such as: Should the owner of commercial data (or the developer of a word processing software) be able to dictate one particular software environment that must exist in a platform before the data (or the files written with the word processor) can be accessed? Should he be allowed to dismiss other software environments that have comparable, fully acceptable security properties? If not, what tools should technology and the law provide to assess and compare the acceptability of software environments? Should the law prescribe that rights holders and software companies may not deny competing software environments access to their content or software if these environments have certain acceptable properties? Should the law create an interoperability requirement between different software and hardware environments (including non–trusted–computing environments)? Is there a need for a "trusted computing misuse" regulation?[2018]

Trusted computing architectures are likely to incorporate some kind of signing, certification or evaluation procedure. While the TCPA architecture itself does not require any software code or device driver to be signed to run,[2019] two caveats have to be made. Firstly, as was described above,[2020] TCPA uses "Validation

[2014] Arbaugh (2002): 78; Anderson (2002): 8–10.

[2015] As Anderson (2003a): 10, points out, such conversion might even be impossible for the owner of the files. Even if he would authorize such conversion, he could still not convert them as long as the developers of the trusted hardware and software components would not provide him with appropriate conversion tools or authorizations.

[2016] See: Id.: 10–11.

[2017] See: Id.: 9–11.

[2018] These questions relate to the problem discussed above how and by whom "security" should be defined in the security carve–out provisions in the Microsoft antitrust consent decrees; see *supra* text accompanying note 1911.

[2019] Pearson (2003): 36. TCPA does not include any central certification agency that decides whether a particular software component can be used in the TCPA framework. It also does not include any central licensing agency that decides whether a particular platform is TCPA–compliant or not. Rather, TCPA provides certain conformance requirements that establish the security requirements of TCPA implementations. These requirements are used by third–party certification authorities to vouch for the correct design and implementation of TCPA standards in a particular platform; see: Id. 208. Basically, TCPA merely provides trustworthy integrity metrics which can be used by the two parties engaged in the transaction to determine if the other platform is trusted for the intended transaction; see: TCPA (2002c): 3.

Entities" to issue certificates for software applications which state that, if the application is executed on a trusted platform, the platform will be in a particular state.[2021] Secondly, even if TCPA itself does not use signing authorities in a strict sense, an operating system that builds on top of TCPA could still condition the execution of software applications upon prior evaluation and signing procedures.[2022]

Although the details are still unclear, the Palladium environment is likely to incorporate some kind of signing or certification procedure for software applications as well.[2023] Such certification procedure could also start from application and content providers. A content provider could, for example, state that its content may only be accessed by certain software applications that have been certified as complying with certain security requirements, or that it may only be accessed if the overall platform is in a secure state.[2024] Such procedures would rely on an underlying certification infrastructure that provides such certificates.

Although it is still unclear how important signing and certification architectures will be in a real–world implementation of trusted computing architectures, some risks of such architectures in general should be highlighted. Any trusted platform architecture that uses signing or certification procedures in order to control which application can be executed on the platform runs the danger of using this control strategically. As such architecture may prevent a user from running an "unapproved" application, it may limit the choice of applications a user actually has, as the providers of the certification infrastructure could decide which application would be certified and which not.[2025] Such architecture could also endanger open source software. If, for open source software to be run on a trusted platform, a certificate has to be obtained, the software would have to be re–certified each time after it has been altered and extended by an open source programmer. This re–certification may be costly, take time and be an overly bureaucratic procedure.[2026] As open source programmers probably will not have the resources to finance such re–certification, they may decide not to work on

[2020] See *supra* note 1969.

[2021] However, it is important to note that anyone can be a validation entity in TCPA. Validation entities need no approval or certification from TCPA to operate. TCPA merely states the format of the certificates which validation entities issue; see also *infra* text accompanying notes 2038–2039.

[2022] See: Pearson (2003): 36.

[2023] See: Microsoft Corp. (2003).

[2024] For an argument that, within Palladium, the locus of trust resides at application and content providers, see: Anderson (2003a): 5.

[2025] See: Arbaugh (2002): 78. One example of this strategy is Microsoft's denial to issue a certificate for a Linux version that could be run on the Xbox game console. It is important to note, however, that Microsoft might have legitimate reasons not to issue such a certificate; *see supra* note 1906 and the accompanying text.

[2026] See: Anderson (2003): Par. 18; *Kuhlmann, Gehring* within this book on page 178; see also: Arbaugh (2002): 78. In the context of TCPA, the "certificate" which an open source programmer would have to obtain would be a certificate by a validation entity that enables third parties to challenge the integrity of a trusted platform on which the open source program is running.

the software program at all. The idea of cumulative innovation, which lies at the heart of the open source movement, could be thwarted by the financial hurdles created by trusted computing certification architectures.[2027]

Furthermore, signing or certification procedures could hamper attempts by competitors to reverse engineer software developed by the trusted platform developer.[2028] If a company succeeded in reverse engineering such software in order to create an interoperable program, its program would still need a certification to be run on the platform. If the certification authority would be affiliated with the platform developer, it might deny the certificate for strategic reasons.[2029]

To put it succinctly: certification architectures in trusted platform infrastructures can be used in many anti–competitive ways. While all these predictions may sound alarming, they have to be qualified in two respects. Firstly, these dangers are not unique to trusted computing platforms. Indeed, they are just another example of how DRM systems can be used to control competition in the platform or in complementary markets.[2030] What is new about trusted computing platforms is that they increase security significantly. Compared to a purely software–based DRM system, a trusted computing platform makes it much harder to break the security architecture. Trusted computing, in other words, does not enable market participants to thwart competition, but it increases their ability to do so.

Secondly, and more importantly, it is unclear at the moment whether these dangers will ultimately materialize. This depends, in particular, on the institutional arrangement surrounding trusted computing architectures. Consider, as an example, the TCPA specification. The architectural idea of TCPA is that, in order to enable trust in a computing platform, a root of trust[2031] has to exist in this platform. From this root of trust, a chain of trust across the layers of hard– and software can then be established. This, of course, only raises the question of why anyone should have confidence in this root of trust from which the chain of trust originates.

TCPA states that, in order to have confidence in the root of trust in a computing platform, two conditions must be met. Firstly, the standard to which the root of trust adheres has to be trustworthy itself. This means that the TCPA standards have to function exactly as they claim to function. TCPA attempts to gain this trust by delivering its standards as public documents which are open for review by both consumers and the scientific community.[2032]

[2027] For an important caveat to this statement in the context of TCPA, see *infra* text accompanying notes 2037–2039.

[2028] For an analysis of the importance of reverse engineering, see: Samuelson, Scotchmer (2002).

[2029] In the end, certification architectures can therefore have similar effects as code obfuscation technologies; see *supra* note 1884.

[2030] See *supra* section V of this article.

[2031] Which, in the TCPA specification, are the CRTM and the TPM.

[2032] See: Pearson (2003): 225. Similarly, Microsoft has announced to publish the source code of the Palladium Nexus in its Shared Source Initiative, see: the interview with John Manferdelli, available at: http://www.microsoft.com/presspass/features/2002/jul02/07-01palladium.asp (Jul. 1, 2002).

Even if the TCPA specification is considered trustworthy, the root of trust can only be trusted if, secondly, it is certain that the root of trust is fully compliant with the TCPA specification. Therefore, TCPA requires five certificates by four different logical entities that certify that a particular platform is in fact a genuine trusted platform that fully complies with the TCPA specification.[2033]

From an abstract perspective, what TCPA ultimately does is that it changes the targets in which computer users and third parties have to trust. They do not have to trust in any of the components of computing platforms any more. Rather, they have to trust in certain institutions which vouch for the security of particular computing platforms. The TCPA architecture then transfers this *trust in entities* to *trust in components*.[2034] If TCPA succeeds, it will reduce the areas in which computer users have to trust to a few well–defined institutions and documents.

In such an approach, which is common to all trusted computing architectures, it becomes of utmost importance how these institutions are designed. One possible institutional arrangement would be to use a centralized agency that provides all certifications. Another institutional arrangement would be to allow competition to occur among different agencies that provide certification services.[2035] If well–functioning competition between different certification agencies existed, many of the problems raised above would be solved by market forces.[2036] Consider, for example, the potential tension between open source software and TCPA that was

[2033] These entities are the "Trusted Platform Module Entity" (TPME) (vouching that the TPM is genuine, i.e. that it contains a genuine "endorsement key"), the "Conformance Entity" (CE) (issuing two certificates which vouch that the design of a particular class of platform meets the requirements of the TCPA specification), the "Platform Entity" (PE) (vouching that a specific platform is an instance of a class of platforms that meets the TCPA specification), and the "Privacy–Certification Authority" (Privacy–CA) (vouching that a particular identity belongs to a trusted platform). In addition, "Validation Entities" (VE) are used to vouch for the expected metrics for platform components such as software applications; see Pearson (2003): 59–62, 125–131, 205–212, 226–234; *Kuhlmann, Gehring* within this book on page 178.

[2034] See: Pearson (2003): 234.

[2035] Microsoft claims to use the second institutional arrangement in Palladium; see: Microsoft Corp. (2002) (stating that "[a]*nyone can certify 'Palladium' hardware or software, and it is expected that many companies and organizations will offer this service. Allowing multiple parties to independently evaluate and certify 'Palladium'–capable systems means that users will be able to obtain verification of the system's operation from organizations that they trust. In addition, this will form the basis for a strong business incentive to preserve and enhance privacy and security*"). TCPA enables competition among certification institutions as well. A third institutional arrangement would be to enable a fully decentralized system in which certificates are issues on a peer–to–peer basis. For an abstract analysis of how such different architectures of the certification infrastructure influences legal and policy values, see: Bechtold (2003b): 1268–1285.

[2036] This is not to say that, in a trusted computing infrastructure, all competition–related problems could easily be solved by market forces. Even in an otherwise competitive market, without government intervention, many of the concerns

described above.[2037] Although the financial and bureaucratic hurdles of certification and recertification could severely impede the development of open source software, this holds true only if a monopolistic or oligopolistic certification infrastructure would exist. At least theoretically, however, TCPA allows every software developer to become his own certification authority.[2038] Open source developers do not necessarily depend on any third–party certification infrastructure, but could build their own infrastructure. As long as users and other developers would trust this open source certification infrastructure, it would work without any problems in TCPA.[2039]

Using the invisible hand of competition in the certification infrastructure to solve policy problems of trusted computing architectures assumes, however, that such competition will actually work. Whether this is a vaild assumption depends on many factors, including the existence of network effects, interoperability requirements and the particular design of the infrastructure. Although network effects could lead to a monopolization in the certification market, two caveats should be made. Firstly, interoperability and interconnection requirements between different certification services could decrease the adversary impacts of network effects.[2040] Secondly, even if a particular certification service provider became dominant in the trusted computing certification market due to network effects, this would still not hinder users to use competing certification services as well, at least as long as the user's trusted platform would concurrently accept certificates from different certification authorities. As long as the trusted platform owners are able to use various certification services concurrently, network effects would therefore not foreclose entry into the certification market.[2041]

related to switching costs and consumer lock–ins (see *supra* text accompanying notes 2012–2017) are likely to continue to exist. These problems could only be solved by interoperability and interconnection requirements; see also: Bechtold (2003b): 1273–1281.

[2037] See *supra* text accompanying note 2026.

[2038] Or, more precisely, his own validation entity. Therefore, it is possible that no commercial third–party validation entity would be needed in a future TCPA environment, as all developers of software (open source *and* proprietary) would act as their own validation entity.

[2039] See also: Arbaugh (2002): 78. Therefore, in the context of TCPA, the sticking point is not whether proprietary validation infrastructures will impede the development of open source software, but, firstly, whether the open source community will succeed in creating its own validation entities and, secondly, whether users and other developers will trust these validation entities.

[2040] For an abstract analysis of the relationship between network effects and interoperability/interconnection requirements, see: Bechtold (2003b): 1273–1281. For some general literature of network effects, see *supra* note 1925.

[2041] This, in turn, does not only depend on the assumption that users will be able to use various certification services concurrently, but also that they will actually do so. Unfortunately, it is highly questionable whether one can expect ordinary trusted platform users to deviate from the standard settings about certification authorities in their platforms. Both a theoretical analysis and practical examples seem to argue against this notion. On the theoretical side, steep learning curves, high transactions costs, information asymmetries (as in the "market for

In general, it is important to ensure that the certification infrastructure of trusted computing architectures is designed in a way that certification agencies do not act strategically, that independent agencies exist, and that they issue certificates on a non–discriminatory basis. In order to really have confidence in a trusted computing infrastructure, a neutral certification infrastructure, on which the trusted computing infrastructure builds, has to exist.

Until now, the companies developing TCPA and Palladium have not been actively involved in discussing the impacts of trusted computing on competition. As with earlier DRM technologies, they seem to take the view that they are mere developers of technology that should not openly engage in policy discussions. While it is highly questionable whether this is a good strategy,[2042] all the more it is important to start such discussions in legal and policy circles.[2043]

Dangers Related to Copyright Law

Although DRM systems which are based on trusted computing architectures may come into conflict with copyright law, these conflicts are hardly novel or restricted to trusted computing. In most cases, they are general problems that may occur in any DRM system.[2044] Three examples may illustrate this point. Firstly, as was described above, trusted computing architectures enable content to be cryptographically bound to a particular platform, even to a particular platform configuration.[2045] If copyright limitations allow a consumer to copy content to another device without the rights holder's permission, the trusted platform could nevertheless prevent such copying as the sealed content could not be decrypted on the other device. Trusted computing platforms may there-

lemons", see: Bechtold (2002): 339–344), as well as bounded rationality and willpower (see: Korobkin (2003); Jolls, Sunstein, Thaler (1998): 1477–1479) all seem to imply that users do not make informed decisions about which certification authorities to use. On the empirical side, in the context of the Platform for Privacy Preferences (P3P), it seems that most users rarely customize their browers' privacy settings; see: Cranor (2002): 257–259; Garfinkel (1998): 44, 46. See also: Schwartz (2000): 754 (comparing the P3P example to the "blinking twelve" problem with video recorders and stressing the importance of good interface design in this context); Bechtold (2003b): 1277 note 159 (describing a similar problem in the context of local Internet browser settings on certification authorities for the Secure Socket Layer (SSL) encryption); Mackay (1991) (describing an empirical study of software customization in a Unix environment); but see: Page et al. (1996) (describing an empirical study in which 92% of the participants customized their word processing software in some way). If it is indeed unrealistic to expect users to customize the settings in their trusted platform according to their actual preferences, a well–functioning competition between different certification authorities might be unrealistic as well. Ultimately, this is just an application of the general problem what the implications of standard settings in distributed computing environments are.

[2042] See also: Landesbeauftragter für den Datenschutz Mecklenburg–Vorpommern (2003); *Kuhlmann, Gehring* within this book on page 178.

[2043] See also: *Kuhlmann, Gehring* within this book on page 178.

[2044] For a general analysis of the tension between DRM and copyright law, see: Bechtold (2002/2003a).

[2045] See *supra* text accompanying notes 1979–1984, 1993.

fore come into conflict with traditional copyright law.[2046] However, this is not a feature that is unique to trusted computing platforms. The CPRM/CPPM standards[2047] are able to bind content to particular devices as well.[2048] Furthermore, even software–based DRM systems are able to prevent content from being copied to other devices.

Secondly, Microsoft Palladium offers a tamper–resistant communication path between different system components in a PC.[2049] Furthermore, by using "curtained" memory, it can securely isolate software applications from each other and prevent any snooping by adversarial applications.[2050] However, such ideas are not absolutely novel either. DRM standards such as HDCP[2051] and DTCP,[2052] for example, protect communication paths between different system components and between different devices as well.

Finally, the combination of trusted computing architectures and anti–circumvention regulations may impede security testing and research. As was described above, in a trusted computing architecture, users only have to trust in certain institutions which vouch for the security of particular computing platforms. Trusted computing architectures then transfer this trust in entities to trust in components.[2053] While this may sound very promising at first glance, the dangers of this approach have to be considered as well. It may become hard for independent security research to assess the security of trusted platform architectures. Not only might their various technological protection measures impede security research, but breaking some of the protection measures in order to engage in security research could also violate anti–circumvention regulations. Ultimately, trusted platforms could represent a move from a security paradigm according to which security can only be guaranteed if it has been proven by independent security research to a paradigm according to which security can be guaranteed by the security architecture itself. While this move from *security by proof to security by trust*[2054] may be troublesome, the underlying impediment of independent security research is not novel either. Rather, it is just an application of the general tension between DRM technology, anti–circumvention regulations and security research.[2055]

In general, trusted computing platforms do not create qualitatively new challenges to copyright law. What is novel about trusted computing is that it provides much higher security and thereby makes the circumvention of the security

[2046] See: Arbaugh (2002): 79, who proposes a modification of the TCPA specification that would enable individuals themselves to authorize various devices under their control to view purchased content; see also: Huang (2002): 104.
[2047] For more information, see *supra* text accompanying note 1936.
[2048] See *supra* note 1984.
[2049] See *supra* text accompanying note 1998.
[2050] See *supra* text accompanying notes 1996–1997.
[2051] See *supra* note 1938.
[2052] See *supra* note 1937.
[2053] See *supra* text accompanying note 2034.
[2054] The author is indebted to Volker Grassmuck for this insight.
[2055] See *supra* section II.4: *DRM and Research*.

system much more difficult than ordinary DRM systems.[2056] Therefore, the potential tension between DRM systems, which are based on trusted computing architectures, and copyright law becomes much stronger.

Dangers Related to Privacy Laws

Finally, DRM systems based on trusted computing architectures may come into conflict with legitimate privacy interests. As was described above, TCPA includes an extensive infrastructure of Privacy Certification Authorities intended to protect the user's privacy.[2057] However, doubts have been raised whether, from a technical perspective, the system is actually as privacy–protecting as TCPA claims it to be. One issue of concern is, for example, that the public key of the endorsement key pair, which uniquely identifies a particular trusted platform,[2058] is used in the creation of trusted identities[2059] — making it easier for Privacy–CAs to correlate several trusted identities and identify individual users.[2060] Furthermore, for performance and financial reasons, the TCPA specification allows platform manufacturers to generate endorsement keys outside a TPM and then inject them into an individual platform.[2061] Although the TCPA specification mandates that injected keys must be as secure and as private as those generated inside the TPM,[2062] the risk remains that external copies of the endorsement key exist.[2063] In general, the privacy design of TCPA heavily relies on the trustworthiness of Privacy–CAs and hardware manufacturers. As with the competition–related concerns, the implications of trusted computing for privacy protection heavily depend on the architecture of the underlying privacy certification infrastructure.[2064] As was described above, TCPA's privacy model builds upon the assumption that competition between different Privacy–CAs will enable users to choose a Privacy–CA which fits their individual preferences. Unfortunately, only a real–world implementation of trusted computing architectures will show whether they will adequately protect the privacy interests of their

[2056] Another novelty is the attempt to create a pervasive security infrastructure; see *infra* text accompanying note 2065.

[2057] See *supra* text accompanying notes 1972–1976.

[2058] See *supra* text accompanying note 1972.

[2059] See: Wintermute (2003): Par. 2.6.5, see also: Arbaugh (2002): 79; Pfitzner (2003): 11–14; Pearson (2003): 124, 128.

[2060] See: Pfitzner (2003): 11–12; Landesbeauftragter für den Datenschutz Mecklenburg–Vorpommern (2003): 4. As Arbaugh (2002): 79, points out, this problem could only be solved if a method existed that would be able to verify the compliance of a particular trusted platform with the TCPA specification without releasing the compliant device's identity information; see also: Safford (2002a): 5.

[2061] See: Pearson (2003): 124.

[2062] See: Id.: 124, 126.

[2063] See: Pfitzner (2003): 11.

[2064] See: Konferenz der Datenschutzbeauftragten, available at: http://www.datenschutz.mvnet.de/beschlue/ent65.html; Landesbeauftragter für den Datenschutz Mecklenburg–Vorpommern (2003) (both documents are statements of German data protection authorities on the implications of TCPA and Palladium for privacy).

users. In some usage contexts, competition among different Privacy–CAs with different levels of privacy protection might solve the privacy–related problems of TCPA. In other contexts, however, the necessary reliance upon external entities that purport to protect the user's privacy might be unacceptable.

The Peril of Pervasiveness

Many of the potential dangers described above are not unique to trusted computing. They have emerged in other contexts before. What is novel about trusted computing is that it provides much higher security and therefore increases the tension between technology and public policy values considerably. What is novel as well is the goal of trusted computing to create a security infrastructure that becomes as wide–spread as possible. Ideally, this infrastructure would not only cover personal computers, but would also extend to other computing devices such as PDAs, cell phones and mobile devices.

Trusted computing aims at creating a pervasive infrastructure. With trusted computing, any tension between technology and public policy, which might have existed before in small, well–defined subsections of the computing environment, could now become projected onto the entire computing infrastructure that surrounds us. While the tension between technology and public policy used to be restricted to isolated incidents, trusted computing could make this tension omnipresent.[2065] Pervasive technology standards which nobody can evade have to be subject to close scrutiny.

Nevertheless, as the discussion of trusted computing architectures shows, many of the potential problems raised by such architectures can be solved by a clever design of the technical architecture or the institutional arrangements surrounding the architecture. Fortunately, as trusted computing architectures are still in the development stage, there may be a realistic chance to influence such architectures so that they become a neutral infrastructure which enables competition, respects copyright limitations, and protects privacy interests.

VI.2 Standardization by the Legislature or the Administration

DRM technology does not only become standardized by market participants. Increasingly, legislators are thinking about mandating the implementation of various DRM components into consumer devices. They are pushed towards adopting such laws by powerful lobbying groups from the content industries (in particular the movie industry), while most computer and device manufacturers fiercely oppose such attempts. As is often the case in the DRM debate, both sides argue with extreme scenarios. Without any mandated DRM solution, the proponents argue, cultural production as we currently know it could come to an end. The

[2065] See also: Stallman (2002a): 115. The attempt of platform developers to control complementary aftermarkets (see *supra* section V.2 *Competition in Complementary Markets*) may illustrate this point. In a world of trusted computing, security primitives are available to platform developers at very low costs. This could make it rather straightforward for all sorts of vendors to control complementary aftermarkets. See: Anderson (2003a): 3.

opponents argue that a mandated DRM solution would mean the end of the general purpose computer which could have severe impacts on innovation and growth in the technology sector.[2066]

Traditionally, attempts by the legislators to mandate particular DRM systems have been rare, albeit not unknown. In the United States, the Audio Home Recording Act of 1992 requires consumer DAT players to be equipped with the "Serial Copy Management System" (SCMS).[2067] The Digital Millennium Copyright Act of 1998 requires analog consumer video recorders and cameras to be equipped with copy protection mechanisms developed by Macrovision.[2068] European Directives have been mandating, for competition policy reasons, a particular scrambling algorithm to be implemented into digital pay TV systems since 1995.[2069]

Nevertheless, in general, it has been a worldwide accepted policy that legislators should refrain from interfering in the DRM development process by mandating a particular system. Both the U.S. Digital Millennium Copyright Act and the European Copyright Directive of 2001 provide in so–called "no–mandate clauses" that device manufacturers are not required by law to include any DRM system into their products.[2070]

Yet, over the last two years, new proposals for legislative DRM mandates have emerged. For example, in the United States, in the fall of 2001, a bill called "Consumer Broadband and Digital Television Promotion Act" (CBDTPA)[2071] was proposed that would empower the FCC to issue a rule mandating the implementation of particular DRM standards into a broad range of digital devices. In August 2002, the FCC issued a Notice of Proposed Rulemaking aimed at mandating the recognition by digital TV consumer equipment of a "broadcast flag" developed by the "Broadcast Protection Discussion Subgroup" (BPDG) of the CPTWG.[2072] In December 2002, the U.S. cable and consumer electronics industries reached an agreement for a national digital cable TV standard. If the

[2066] See: Grassmuck (2002): 36–37; see also: Marks, Turnbull (2000): 203–205.

[2067] 17 U.S.C. § 1002 (a). Similar lobbying attempts to mandate SCMS in European DAT players failed. For some background, including the history of the Athens Agreement, see: Bechtold (2002): 244–245.

[2068] 17 U.S.C. § 1201 (k).

[2069] See: Annex VI No. 1 to the Directive 2002/22/EC of the European Parliament and of the Council of March 7, 2002, on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive), Official Journal of the European Communities L 208 (Apr. 24, 2002), 51. This provision supersedes Article 4 (a) of the Transmission Standard Directive, *supra* note 1892. See also: Bechtold (2002): 241–243.

[2070] See: 17 U.S.C. § 1201 (c) (3); Recital 48 of the European Copyright Directive, *supra* note 1852, at 14.

[2071] S. 2048, 107th Congress (2002). The bill was first proposed as the "Security Systems Standards and Certification Act" (SSSCA) and is sometimes referred to as the "Hollings bill", after Senator Fritz Hollings who introduced the bill into Congress.

[2072] See: *In the Matter of Digital Broadcast Copy Protection*, 17 F.C.C.R. 16027 (F.C.C. 2002). For more information on the BPDG, see *supra* note 1932.

agreement is approved by the FCC, every digital television set in the United States would be required to be equipped with the "High–Bandwidth Digital Content Protection" (HDCP).[2073]

At first sight, mandating DRM standards seems a promising approach for a market characterized by network effects. One common DRM architecture could be introduced into the market in a relatively short period of time, and standard wars between incompatible standards could be avoided.

However, history argues against legislative DRM mandates. Given the modest success of earlier attempts to mandate DRM technologies by law, it seems not very likely that a general mandate to implement DRM components into nearly all consumer equipment will be enacted in the near future.[2074] Considering the failure in Europe to even mandate the use of SCMS in consumer DAT players,[2075] such a scenario seems particularly unlikely in Europe. Furthermore, all recent efforts to mandate DRM technology on a broad scale have met with fierce opposition from various groups such as the computer and consumer electronics industry[2076] and consumer advocacy groups. However, industry–specific attempts to mandate DRM technology into particular families of devices (such as pay TV decoders or mobile players) may prove much more successful in receiving the necessary support for a legislative adoption.

It is not only history that makes broad legislative or administrative DRM mandates unlikely. Forcing the inclusion of DRM technology components into the general PC hardware could mean the end of the general purpose computer as we know it: the PC owner would lose his "freedom to tinker" with his own hardware, as Edward Felten calls it.[2077] The eradication of the general–purpose PC could have an unforeseeable negative impact on innovation and commercial development in the computer industry.

While these are valid concerns, technological mandates create other kinds of problems as well. One should not forget that DRM benefits primarily content providers. Therefore, it seems only a second–best solution to create a statutory DRM mandate, as this would assign the costs of DRM implementation not to content providers, but to technology vendors. Furthermore, legislative standardization runs the risk of freezing outdated or inherently insecure tech-

[2073] See: *Consensus Cable MSO — Consumer Electronics Industry Agreement on "Plug & Play" Cable Compatibility and Related Issues*, *supra* note 1833. See also: Taub, Eric A.: *Pact Lifts an Obstacle to HDTV Transition*, N.Y. Times, Jan. 2, 2003, at G7. For more information on HDCP, see *supra* note 1938.

[2074] See also: Netanel (2003): 10–11; Samuelson (2003).

[2075] See *supra* note 2067.

[2076] See only: Technology and Record Company Policy Principles, available at: http://www.bsa.org/usa/policyres/7_principles.pdf (Jan. 2003) (in which the U.S. record industry joins the ranks of DRM mandate opponents); http://alliancefordigitalprogress.org.

[2077] See: http://www.freedom-to-tinker.com. See also: Stallman (2002a): 115; and *supra* note 2066.

nologies.[2078] It may impede competition between the old standardized DRM technology and newly emerging technologies and thereby hold up technological innovation.

VII Conclusion

This article started with two goals. Firstly, it attempted to show that, in the future, we might be confronted with new kinds of policy problems that are underrepresented in the current DRM debates. The tension between DRM and copyright law is only a small part of the overall DRM policy debate. The article highlighted several issues that stem from other areas of law and public policy, in particular from competition–related concerns.

Secondly, the article argued against fundamentalist viewpoints in the DRM policy debate. While the author shares many of the concerns raised against DRM, this article attempted to show that in many cases, DRM technology and its surrounding framework are much more flexible than commonly assumed. Unfortunately, over the last few years, the DRM debate has developed into a discussion about extremes. Depending on the point of view, digital rights management is perceived as either heaven or hell on earth. Some DRM opponents consider the potential threats of DRM as so dangerous that they condemn the idea of digital rights management altogether.[2079] However, to argue that DRM will inevitably lead to an Orwellian world of perfect private control suffers from a general problem cyberlaw has to deal with: although a world of perfect control would indeed be highly undesirable, it is often unclear whether such perfection will ever occur in the real world.[2080] Particularly in an area such as DRM, where technology seems capable to reflect many of the objections raised against the technology, unconditional opposition to the technology seems inappropriate at this time.

Naturally, framing the DRM debate as a debate about extremes has its own reasons. The most important reason may be that it is easier to talk about clear–cut extremes — DRM as paradise for creators versus DRM as hell for consumers — than to grapple with the muddy middle ground in between. However, debating about DRM in terms of extremes disguises the insight that such middle ground may exist and be preferable. The difficulties to conceptualize balanced DRM regimes as well as the staggering complexity of innovation policy in general should not deter technologists, lawyers, legal scholars, economists and policy makers from attempting to crystallize this middle ground.

Currently, no one knows whether a balanced DRM system that protects interests of users and the society at large is ultimately feasible both from a technological and a business perspective. The potentials of DRM to create a balanced and

[2078] See: *Biddle, England, Peianado, Willmann* within this book: 356–357 (arguing against a statutory watermarking mandate due to various technical inadequacies of digital watermarks).

[2079] For a general analysis of such slippery slope arguments, see: Volokh (2003).

[2080] For the same argument in a different context, see: Bechtold (2002a): 242.

just information ecology are still largely unexplored. As all technology, DRM is malleable, and one should not miss the opportunity to engage in a value–centered design process that shapes DRM appropriately.

BIBLIOGRAPHY

— **A** —

Anderson (2001):
Anderson, Ross J. (2001): Security Engineering — A Guide to Building Dependable Distributed Systems. New York.

Anderson (2002):
Anderson, Ross J. (2002): Security in Open versus Closed Systems — The Dance of Boltzmann, Coase and Moore. Available at: http://www.ftp.cl.cam.uk/ftp/users/rja14/toulouse.pdf.

Anderson (2003a):
Anderson, Ross J. (2003): Cryptography and Competition Policy — Issues with "Trusted Computing". Available at: http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tcpa.pdf (May 2003).

Anderson (2003b):
Anderson, Ross J. (2003): TCPA/Palladium Frequently Asked Questions. Version 1.0. Available at: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (last modified Apr. 2003).

Arbaugh (2002):
Arbaugh, Bill (2002): Improving the TCPA Specification. 35 (8) IEEE Computer 77.

Arbaugh, Farber, Smith (1997):
Arbaugh, Bill/ Farber, Dave/ Smith, Jonathan (1997): A Secure and Reliable Bootstrap Architecture. In: Proceedings of the IEEE Symposium on Security and Privacy 1997. Los Alamitos. p. 65.

Asay (2002):
Asay, Matt (Apr. 2002): A Funny Thing Happened on the Way to the Market: Linux, the General Public License, and a New Model for Software Innovation. Available at: http://www.linuxdevices.com/files/misc/asay-paper.pdf.

— **B** —

Barak et al. (2001):
Barak, Boaz/ Goldreich, Oded/ Impagliazzo, Russel/ Rudich, Steven/ Sahai, Amit/ Vadhan, Salil/ Yang, Ke (2001): On the (Im)possibility of Obfuscating Programs. In: Joe Kilian (ed.): Advances in Cryptology — CRYPTO 2001. Berlin. p. 1.

Bartholomew (2002):
Bartholomew, Paul (July 14, 2002): Understanding the Xbox Boot Process/Flash Structures. Available at: http://xbox-linux.sourceforge.net/articles.php?aid=2002194020413.

Bechtold (2002):
Bechtold, Stefan (2002): Vom Urheber– zum Informationsrecht — Implikationen des Digital Rights Management. Munich.

Bechtold (2002b):
Bechtold, Stefan (2002): The Problems of Perfection. Review of Cass Sunstein, Republic.com. 3 European Business Organization Law Review 237.

Bechtold (2003a):
Bechtold, Stefan (2003): Digital Rights Management in the United States and Europe. Unpublished draft.

Bechtold (2003b):
Bechtold, Stefan (Forthcoming 2003): Governance in Namespaces. 36 Loyola of Los Angeles Law Review 1239.

Behlendorf (1999):
Behlendorf, Brian (1999): Open Source as a Business Strategy. In: DiBona, Chris; Ockman, Sam & Stone, Mark (eds.), Open Sources — Voices From the Open Source Revolution. Sebastopol. p. 149.

Benkler (2002):
Benkler, Yochai (2002): Intellectual Property and the Organization of Information Production. 22 International Review of Law and Economics 81.

Bizer (2001):
Bizer, Johann (2001): Datenschutzgerechte Gestaltung des technischen Urheberschutzes. 25 Datenschutz und Datensicherheit 12.

Borenstein, MacKieMason, Netz (2000):
Borenstein, Severin/ MacKieMason, Jeffrey K./ Netz, Janet S. (2000): Exercising Market Power in Proprietary Aftermarkets. 9 (2) Journal of Economics & Management Strategy 157.

Boyle (2000):
Boyle, James (2000): Cruel, Mean, or Lavish? Economic Analysis, Price Discrimination and Digital Intellectual Property. 53 Vanderbilt Law Review 2007.

Burk (2003):
Burk, Dan L. (forthcoming 2003): Anti-Circumvention Misuse, 48 UCLA Law Review. Draft available at http://paper.ssrn.com/abstract=320961 (2002).

Burk, Cohen (2001):
Burk, Dan L./ Cohen, Julie E. (2001): Fair Use Infrastructure for Rights Management Systems, 15 Harvard Journal of Law & Technology 41.

Bygrave (2002):
Bygrave, Lee A. (2002): The Technologisation of Copyright: Implications for Privacy and Related Interests. 24 European Intellectual Property Review 51.

Bygrave, Koelman (2000):
Bygrave, Lee A./ Koelman, Kamiel J. (2000): Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems. In: Hugenholtz, P. Bernt (ed.), Copyright and Electronic Commerce. London. p. 59.

— C —

Calabresi, Melamed (1972):
Calabresi, Guido & Melamed, A. Douglas (1972): Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. 85 Harvarv Law Review 1089.

Chiappetta (2000):
Chiappetta, Vincent (2000): The Desirability of Agreeing to Disagree: The WTO, TRIPS, International IPR Exhaustion and a Few Other Things. 21 Michigan Journal of International Law 333.

Clark (2003):
Clark, Kendall G. (2003): Creative Comments: On the Uses and Abuses of Markup. Available at http://www.xml.com/pub/a/2003/01/15/creative.html (Jan. 15, 2003).

Cohen (1996):
Cohen, Julie E. (1996): A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace. 28 Connecticut Law Review 981.

Cohen (1998):
Cohen, Julie E. (1998): Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management". 97 Michigan Law Review 462.

Cohen (2000):
Cohen, Julie E. (2000): Copyright and the Perfect Curve. 53 Vanderbilt Law Review 1799.

Cohen (2003):
Cohen, Julie E. (Forthcoming 2003): DRM and Privacy. 18 Berkeley Technology Law Journal. Draft available at https://www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.pdf (Feb. 10, 2003).

Cranor (2002):
Cranor, Lorrie F. (2002): Web Privacy with P3P. Sebastopol.

Crosby et al. (2001):
Crosby, Scott/ Goldberg, Ian/ Johnson, Robert/ Song, Dawn/ Wagner, David (2001): A Cryptanalysis of the High-Bandwidth Digital Content Protection System. In: Sander, Tomas (ed.): Security and Privacy in Digital Rights Management. Berlin. p. 192.

— **D** —

Dankwardt (2002):
Dankwardt, Kevin (2002): Are Non–GPL Loadable Linux Drivers Really Not a Problem? Available at http://www.linuxdevices.com/articles/AT5041108431.html (last modified Sept. 30, 2002).

Datenschutzbeauftragte des Bundes und der Länder:
TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden. Entschlieung der 65. Konferenz der Datenschutzbeauftragten am 27./28. März 2003 in Dresden. Available at http://www.datenschutz.mvnet.de/beschlue/ent65.html (March 27/28, 2003).

— **E** —

Eisenberg (2001):
Eisenberg, Rebecca S. (2001): Bargaining Over the Transfer of Proprietary Research Tools: Is This Market Failing or Emerging? In: Dreyfuss, Rochelle C.; Zimmermann, Diane L. & First, Harry (eds.), Expanding the Boundaries of Intellectual Property: Innovation Policy for the Knowledge Society. Oxford. p. 223.

Electronic Frontier Foundation (2003):
Electronic Frontier Foundation (2003): Unintended Consequences: Four Years under the DMCA. Available at http://www.eff.org/IP/DRM/DMCA/20030103_dmca_consequences.pdf (Jan. 9, 2003).

Elkin–Koren, Netanel (2002):
Elkin–Koren, Niva & Netanel, Neil W. (eds.) (2002): The Commodification of Information. The Hague.

Emch (2002):
Emch, Eric R. (March 2002): Does Opportunism Explain Markups in Laser Printer Toner and Memory? No and Yes. Evidence on Pricing in Laser Printer Aftermarkets. Available at http://papers.ssrn.com/abstract=311840.

Emch (2003):
Emch, Eric R. (2003): Price Discrimination via Proprietary Aftermarkets. 2 (1) Contributions to Economic Analysis & Policy 4. Available at: http://www.bepress.com/bejeap/contributions/vol2/iss1/art4.

England, Peinado (2002):
England, Paul/ Peinado, Marcus (2002): Authenticated Operation of Open Computing Devices. In: Lynn Batten & Jennifer Seberry (eds.), Information Security and Privacy — 7th Australasian Conference (ACISP 2002). Berlin. p. 346.

Erickson (2003):
Erickson, John S. (April 2003): Fair Use, DRM, and Trusted Computing. 46 (4) Communications of the ACM 34.

European Commission (1999):
European Commission (Nov. 9, 1999): The Development of the Market for Digital Television in the European Union. COM (1999) 540.

— **F** —

Feigenbaum, Freedman, Sander, Shostack (2001):
Feigenbaum, Joan/ Freedman, Michael J./ Sander, Tomas/ Shostack, Adam (2001): Privacy Engineering for Digital Rights Management Systems. In: Sander, Tomas (ed.), Security and Privacy in Digital Rights Management. Berlin. p. 76

Felten (2003):
Felten, Edward (April 2003): A Skeptical View of DRM and Fair Use. 46 (4) Communications of the ACM 57.

Foged (2002):
Foged, Terese (2002): U.S. v. EU Anti-Circumvention Legislation: Preserving the Public's Privileges in the Digital Age. 24 European Intellectual Property Review Review 525.

Fox, LaMacchia (2003):
Fox, Barbara L./ LaMacchia, Brian A. (April 2003): Encouraging Recognition of Fair Uses in DRM Systems. 46 (4) Communications of the ACM 61.

— **G** —

Galline, Scotchmer (2002):
Galline, Nancy & Scotchmer, Suzanne (2002): Intellectual Property: When is it the Best Incentive Mechanism? In: Adam Jaffe et al. (eds.), Innovation Policy and the Economy, Volume 2. Cambridge. p. 51.

Garfinkel (1998):
Garfinkel, Simson L. (November/December 1998): The Web's Unelected Government. Technology Review 38.

Gimbel (1998):
Gimbel, Mark (1998): Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law. 50 Stanford Law Review 1671.

Goldstein (2001):
Goldstein, Jorge A. (Summer 2001): Patenting the Tools of Drug Discovery. Drug Discovery World 9.

Gordon (1998):
Gordon, Wendy J. (1998): Intellectual Property as Price Discrimination: Implications for Contract. 73 Chicago–Kent Law Review 1367.

Gordon (2002a):
Gordon, Wendy J. (2002): Excuse and Justification in the Law of Fair Use: Commodification and Market Perspectives. In: Elkin–Koren, Niva & Netanel, Neil W. (eds.), The Commodification of Information. The Hague. p. 149.

Gordon (2002b):
Gordon, Wendy J. (2002): Market Failure and Intellectual Property: A Response to Professor Lunney. 82 Boston University Law Review 1031.

Goto (2001):
Goto, Hideaki (2001): Evulation of Tamper-Resistant Software Deviating from Structured Programming Rules. In Varadharajan, Vijav & Mu, Yi (eds.), Information Security and Privacy — 6th Australasian Conference (ACISP 2001). Berlin. p. 145.

Grassmuck (2002):
Grassmuck, Volker (2002): Das Ende des Allzweck-Computers steht bevor. In: FifF-Kommunkation 4/2002. p. 24.

Grawrock (2002):
Grawrock, David (Sept. 2002): TCPA 1.2 Specification. Available at http://www.intel.com/idf/us/fall2002/presentations/SFC173PS.pdf.

Green (2003):
Green, Andy (Feb. 21, 2003): The Xbox Is a PC. Available at http://xbox-linux.sourceforge.net/articles.php?aid=20030051051044.

Guibault (2002):
Guibault, Lucie (2002): Copyright Limitations and Contracts — An Analysis of the Contractual Overridability of Limitations on Copyright. London.

— **H** —

Harper (2002):
Harper, Tieffa (2002): Much Ado About the First Amendment — Does the Digital Millennium Copyright Act Impede the Right to Scientific Expression? 12 DePaul-LCA Journal of Art & Entertainment Law 3.

Hart (2002):
Hart, Michael (2002): The Copyright in the Information Society Directive — An Overview. 24 European Intellectual Property Review 58.

Heller, Eisenberg (1998):
Heller, Michael A./ Eisenberg, Rebecca S. (1998): Can Patents Deter Innovation? Anticommons in Biomedical Research. 280 Science 698.

Hill (1999):
Hill, Keith (1999): A Perspective: The Role of Identifiers in Managing and Protecting Intellectual Property in the Digital Age. 87 Proceedings of the IEEE 1228.

Hippel, Katz (2002):
Hippel, Eric von/ Katz, Ralph (2002): Shifting Innovation to Users via Toolkits. 48 Management Science 821.

Houweling (2002):
Houweling, Molly S. van (2002): Cultivating Open Information Platforms: A Land Trust Model. 1 Journal on Telecommunications and High Technology Law 309.

Hovenkamp (1993):
Hovenkamp, Herbert (1993): Market Power in Aftermarkets: Antitrust Policy and the Kodak Case. 40 UCLA Law Review 1447.

Huang (2002a):
Huang, Andrew (May 26, 2002): Keeping Secrets in Hardware: the Microsoft XBox Case Study. Available at ftp://publications.ai.mit.edu/ai-publications/2002/AIM-2002-008.pdf.

Huang (2002b):
Huang, Andrew (2002): The Trusted PC: Skin-Deep Security. 35 (10) IEEE Computer 103–104.

Hugenholtz, Guibault, van Geffen (2003):
Hugenholtz, P. Bernt/ Guibault, Lucie/ van Geffen, Sjoerd (March 2003): The Future of Levies in a Digital Environment. Available at http://www.ivir.nl/publications/other/DRM%20Levies%20Final%20Report.pdf.

Huppertz (2002):
Huppertz, Marie-Thérèse (2002): The Pivotal Role of Digital Rights Management Systems in the Digital World. Computer und Recht international. p. 105.

— **I** —

Imfeld (2003):
Imfeld, Cassandra (2003): Playing Fair With Fair Use? The Digital Millennium Copyright Act's Impact on Encryption Researchers and Academians. 8 Communication Law and Policy 111.

— **J** —

Jaeger, Metzger (2002):
Jaeger, Till/ Metzger, Axel (2002): Open Source Software — Rechtliche Rahmenbedingungen der Freien Software. Munich.

Jehoram (2001):
Jehoram, Herman C. (2001): The Future of Copyright Collecting Societies. 23 European Intellectual Property Review 134.

Jolls, Sunnstein, Thaler (1998):
Jolls, Christine/ Sunnstein, Cass R./ Thaler, Richard (1998): A Behavioral Approach to Law and Economics. 50 Stanford Law Review 1471.

— **K** —

Karas (2001):
Karas, Stan (2001): Sony Computer Entertainment, Inc. v. Connectix Corp. 16 Berkeley Technology Law Journal 33.

Katz, Shapiro (1985):
Katz, Michael L./ Shapiro, Carl (1985): Network Externalities, Competition, and Compatibility. 75 American Economic Review 424.

Katz, Shapiro (1994):
Katz, Michael L./ Shapiro, Carl (1994): Systems Competition and Network Effects. 8 (2) Journal of Economic Perspectives 93.

Kelsey, Schneier (1998):
Kelsey, John & Schneier, Bruce (1998): Electronic Commerce and the Street Performer Protocol. Proceedings of the 3rd USENIX Workshop on Electronic Commerce. Available at http://www.usenix.org/publications/library/proceedings/ec98/full_papers/schneier/schneier.pdf.

Kenny, Korba (2002):
Kenny, Steve & Korba, Larry (2002): Applying Digital Rights Management Systems to Privacy Rights Management. 21 Computers & Security 648.

Kitch (1977):
Kitch, Edmund W. (1977): The Nature and Function of the Patent System. 20 Journal of Law and Economics 265.

Kitch (2000):
Kitch, Edmund W. (2000): Elementary and Persistent Errors in the Economic Analysis of Intellectual Property. 53 Vanderbilt Law Review 1727.

Klein (1993):
Klein, Benjamin (1993): Market Power in Antitrust: Economic Analysis after Kodak. 3 Supreme Court Economic Review 43.

Koelman, Helberger (2000):
Koelman, Kamiel J./ Helberger, Natali (2000): Protection of Technological Measures. In: Hugenholtz, P. Bernt (ed.) (2000): Copyright and Electronic Commerce. London. p. 165.

Korobkin (2003):
Korobkin, Russell (2003): Bounded Rationality and Unconscionability: A Behavioral Theory of Policing Form Contracts. University of Chicago Law Review, forthcoming 2003. Draft available at http://papers.ssrn.com/abstract=367172.

Kreile (1992):
Kreile, Reinhold (1992): Collection and Distribution of the Statutory Remuneration for Private Copying with Respect to Recorders and Blank Cassettes in Germany. 23 International Review of Industrial Property & Copyright Law 449.

Kretschmer (2002):
Kretschmer, Martin (2002): The Failure of Property Rules in Collective Administration: Rethinking Copyright Societies as Regulatory Instruments. 24 European Intellectual Property Review 126.

Kroon (2000):
Kroon, Annemique M. E. de (2000): Protection of Copyright Management Information. In: Hugenholtz, P. Bernt (ed.), Copyright and Electronic Commerce — Legal Aspects of Electronic Copyright Management. London. p. 229.

Kumazawa et al. (2000):
Kumazawa, Masayuki/ Kamada, Hironori/ Yamada, Atsushi/ Hoshino, Hiroshi/ Kambayashi, Yahiko/ Mohania, Mukesh (2000): Relationship among Copyright Holders for Use and Reuse of Digital Content. In: Proceedings of the Fifth ACM Conference on Digital Libraries (DL 2000). New York. p. 254.

Kumazawa et al. (2001):
Kumazawa, Masayuki/ Yamada, Atsushi/ Hoshino, Hiroshi/ Kambayashi, Yahiko/ Mohania, Muksh (2001): Representation of Reuse Mechanisms for Digital Work with Multiple Right-Holders. In: Proceedings of the 2001 Symposium on Applications and the Internet — Workshops. SAINT 2001 Workshops. p. 145.

— L —

Lande (1993):
Lande, Robert H. (1993): Chicago Takes It on the Chin: Imperfect Information Could Play a Crucial Role in the Post-Kodak World. 62 Antitrust Law Journal 193.

Landesbeauftragter für den Datenschutz Mecklenburg–Vorpommern (2003):
Landesbeauftragter für den Datenschutz Mecklenburg–Vorpommern (March 31, 2003): TCPA, Palladium und DRM. Available at:
http://www.datenschutz.mvnet.de/informat/tcpa/tcpa.pdf.

Lehner (2002):
Lehner, Franz (Dec. 8, 2002): Xbox Security Concept. Available at:
http://xbox-linux.sourceforge.net/articles.php?aid=2002341141734.

Lemley (1997):
Lemley, Mark A. (1997): The Economics of Improvement in Intellectual Property Law. 75 Texas Law Review 989.

Lemley (2002):
Lemley, Mark A. (2002): Intellectual Property Rights and Standard Setting Organizations. 90 California Law Review 1889.

Lemley, McGowan (1998):
Lemley, Mark A./ McGowan, David (1998): Legal Implications of Network Economic Effects. 86 California Law Review 479.

Lessig (1999):
Lessig, Lawrence (1999): Code and Other Laws of Cyberspace. New York.

Lessig (2001):
Lessig, Lawrence (2001): The Future of Ideas — The Fate of the Commons in a Connected World. New York.

Levy (2000):
Levy, Nichelle Nicholes (2000): Method to Their Madness: The Secure Digital Music Initiative, a Law and Economics Perspective. 5 Virginia Journal of Law and Technology 12.

Lichtman (2000):
Lichtman, Douglas (2000): Property Rights in Emerging Platform Technologies. 29 Journal of Legal Studies 615.

Liebowitz, Margolis (1994):
Liebowitz, Stan J./ Margolis, Stephen E. (1994): Network Externality: An Uncommon Tragedy. 8 (2) Journal of Economic Perspectives 133.

Liu (2003):
Liu, Joseph P. (2003): The DMCA and the Regulation of Scientific Research. 17 Berkeley Technology Law Journal (forthcoming 2003). Draft available at http://www2.bc.edu/%7Eliujr/scholarship/encryption.doc (last updated Mar. 20, 2003).

Llorens–Maluquer (1998):
Llorens–Maluquer, Carles (1998): European Responses to Bottlenecks in Digital Pay-TV: Impacts on Pluralism and Competition Policy. 16 Cardozo Arts & Entertainment Law Journal 557.

Lunney (2001):
Lunney, Glynn S. (2001): The Death of Copyright — Digital Technology, Private Copying, and the Digital Millennium Copyright Act. 87 Virginia Law Review 813.

Lyon (2002):
Lyon, Gordon E. (Oct. 2002): A Quick-Reference List of Organizations and Standards for Digital Rights Management. National Institute of Standards and Technology Special Publication 500–241. Available at http://www.itl.nist.gov/div895/docs/NIST241assm.9oct.pdf.

— **M** —

Mackay (1991):
Mackay, Wendy E. (1991): Triggers and Barriers to Customizing Software. In: Scott P. Robertson (ed.), Reaching Though Technology — Proceedings of the 8th Conference on Human Factors and Computing Systems 1991. New York. p. 153.

Marks, Turnbull (2000):
Marks, Dean S./ Turnbull, Bruce H. (2000): Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses. 22 European Intellectual Property Review 198.

Merges (1996):
Merges, Robert P. (1996): Contracting Into Liability Rules — Intellectual Property Rights and Collective Rights Organizations. 84 California Law Review 1293.

Merges, Nelson (1990):
Merges, Robert P./ Nelson, Richard R. (1990): On the Complex Economics of Patent Scope. 90 Columbia Law Review 839.

Microsoft Corp. (2002):
Microsoft Corp. (Aug. 2002): Microsoft "Palladium": A Business Overview. Available at: http://www.microsoft.com/presspass/features /2002/jul02/0724palladiumwp.asp.

Microsoft Corp. (2003):
Microsoft Corp. (Feb. 2003): Microsoft Next–Generation Secure Computing Base — Technical FAQ. Available at: http://www.microsoft.com/technet/treeview /default.asp?url=/technet/security/news/NGSCB.asp.

Miller (2002):
Miller, Ernest (Feb. 28, 2002): Analysis of BNETD and Blizzard. Available at: http://research.yale.edu/lawmeme
/modules.php?name=News&file=article&sid=149.

Mueller (2001):
Mueller, Janice M. (2001): No "Dilettante Affair": Rethinking the Experimental Use Exception to Patent Infringement for Biomedial Research Tools. 76 Washington Law Review 1.

Mulligan, Burstein (2002):
Mulligan, Deirdre K./ Burstein, Aaron (2002): Implementing Copyright Limitations in Rights Expression Languages. Available at: http://crypto.stanford.edu/DRM2002/mulligan_burstein_acm_drm_2002.doc.
To appear in: Feigenbaum, John (ed.): Security and Piracy in Digital Rights Management. Berlin. Forthcoming 2003.

— **N** —

Nadan (2002):
Nadan, Christian H. (2002): Open Source Licensing: Virus or Virtue? 10 Texas Intellectual Property Law Journal 349.

National Research Council (2000):
National Research Council (2000): The Digital Dilemma. Intellectual Property in the Information Age. Washington.

Netanel (2003):
Netanel, Neil W. (Mar. 2003): Impose a Noncommercial Use Levy to Allow Free P2P File Sharing. Draft available at: http://www.utexas.edu/law/faculty/nnetanel/Levies_chapter.pdf.

Neubauer, Brandenburg, Siebenhaar (2002):
Neubauer, Christian/ Brandenburg, Karlheinz/ Siebenhaar, Frank (October 2002): Technical Aspects of Digital Rights Management Systems. Presented at the 113th Convention of the Audio Engineering Society.

— **O** —

O'Brien (2001):
O'Brien, Jeffrey (Nov. 2001): The Making of the Xbox. Wired 9.11. p. 142.

— **P** —

Page et al. (1996):
Page, Stanley R./ Johnsgard, Todd J./ Albert, Uhl/ Allen, C. Dennis (1996): User Customization of a Word Processor. In: Tauber, Michael J. (ed.) (1996): Proceedings of the Conference on Human Factors in Computing Systems 1996. New York. p. 340.

Paskin (1999):
Paskin, Norman (1999): Toward Unique Identifiers. 87 Proceedings of the IEEE 1208.

Pearson (2003):
Pearson, Siani (ed.) (2003): Trusted Computing Platforms — TCPA Technology in Context. Upper Saddle River.

Pfitzner (2003):
Pfitzner, Roy (Apr. 2003): TCPA, Palladium und DRM — Technische Analyse und Aspekte des Datenschutzes. Version 1.2. Available at: http://www.lda.brandenburg.de/material/tcpa.pdf.

Pindyck, Rubinfeld (2001):
Pindyck, Robert S./ Rubinfeld, Daniel L. (2001): Microeconomics. 5th edition. Upper Saddle River.

Posner (2001):
Posner, Richard A. (2001): Antitrust Law. 2nd edition. Chicago.

Preston, Lofton (2002):
Preston, Ethan/ Lofton, John (2002): Computer Security Publications: Information Economics, Shifting Liability and the First Amendment. 24 Whittier Law Review 71.

— **R** —

Radin (2002a):
Radin, Margaret J. (2002): Incomplete Commodification in the Computerized World. In: Elkin-Koren, Niva/ Netanel, Neil W. (eds.) (2002): The Commodification of Information. The Hague. p. 3.

Radin (2002b):
Radin, Margaret J. (2002): Online Standardization and the Integration of Text and Machine. 70 Fordham Law Review 1125 (2002).

Rosenblatt, Trippe, Mooney (2002):
Rosenblatt, Bill/ Trippe, William/ Mooney, Stephen (2002): Digital Rights Management — Business and Technology. New York.

Safford (2002a):
Safford, David (Oct. 2002): Clarifying Misinformation TCPA. Available at: http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf.

Safford (2002b):
Safford, David (Oct. 2002): The Need for TCPA. Available at http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf.

Samuelson (1999):
Samuelson, Pamela (1999): Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised. 14 Berkeley Technology Law Journal 504.

Samuelson (2001):
Samuelson, Pamela (2001): Anticircumvention Rules: Threat to Science. 293 Science 2028.

Samuelson (2003):
Samuelson, Pamela (April 2003): DRM {and, or, vs.} the Law. 46 (4) Communications of the ACM 41.

Samuelson, Scotchmer (2002):
Samuelson, Pamela/ Scotchmer, Suzanne (2002): The Law and Economics of Reverse Engineering. 111 Yale Law Journal 1575.

Sander (2002):
Sander, Tomas (2002): Golden Times for Digital Rights Management? In: Syverson, Paul F. (ed.) (2002): Financial Cryptography 2001. Berlin. p. 64.

Schneier (1996):
Schneier, Bruce (1996): Applied Cryptography. 2nd edition. New York.

Schoen (2002):
Schoen, Seth (Jul. 5, 2002): Palladium Summary. Available at: http://vitanuova.loyalty.org/2002-07-05.html.

Schricker (1999):
Schricker, Gerhard (ed.) (1999): Urheberrecht. Kommentar. 2nd edition. Munich.

Schwartz (2000):
Schwartz, Paul M. (2000): Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices. Wisconsin Law Review 743.

Shapiro, Varian (1998):
Shapiro, Carl & Varian, Hal R. (1998): Information Rules. A Strategic Guide to the Network Economy. Boston.

Shy (2001):
Shy, Oz (2001): The Economics of Network Industries. Cambridge.

Sobel (2003):
Sobel, Lionel S. (forthcoming 2003): DRM As an Enabler of Business Models: ISPs as Digital Retailers. 18 Berkeley Technology Law Journal. Draft available at: https://www.law.berkeley.edu/institutes/bclt/drm/papers/sobel-drm-btlj2003.pdf.

Stallman (1999):
Stallman, Richard M. (1999): The GNU Operating System and the Free Software Movement. In: DiBona, Chris/ Ockman, Sam/ Stone, Mark (eds.) (1999): Open Sources — Voices From the Open Source Revolution. Sebastopol. p. 53.

Stallman (2002a):
Stallman, Richard M. (2002): Can You Trust Your Computer? In: Gay, Joshua (ed.) (2002): Free Software, Free Society: Selected Essays of Richard M. Stallman. Boston. p. 115.

Stallman (2002b):
Stallman, Richard M. (2002): Why You Shouldn't Use the Library GPL for Your Next Library. Available at: http://www.fsf.org/philosophy/why-not-lgpl.html (last modified Oct. 24, 2002).

— **T** —

Taylor (2000):
Taylor, Jim (2000): DVD Demystified. 2nd edition. New York.

Thomke, Hippel (2002):
Thomke, Stefan & Hippel, Eric von (April 2002): Customers as Innovators — A New Way to Create Value. Harvard Business Review 74.

Trusted Computing Group (2003):
Trusted Computing Group (2003): Frequently Asked Questions. Available at http://www.trustedcomputinggroup.org/about/faq.

Trusted Computing Platform Alliance (2001):
Trusted Computing Platform Alliance (Sep. 9, 2001): TCPA PC Specific Implementation Specification. Version 1.00. Available at: http://www.trustedcomputing.org/docs/TCPA_PCSpecificSpecification_v100.pdf.

Trusted Computing Platform Alliance (2002a):
Trusted Computing Platform Alliance (Feb. 22, 2002): Main Specification. Version 1.1b. Available at:
http://www.trustedcomputing.org/docs/main%20v1_1b.pdf.

Trusted Computing Platform Alliance (2002b):
Trusted Computing Platform Alliance (Jul. 1, 2002): Trusted Platform Module Protection Profile. Version 1.9.7. Available at: http://www.trustedcomputing.org/docs/TCPA_TPM_PP_1_9_7.pdf.

Trusted Computing Platform Alliance (2002c):
Trusted Computing Platform Alliance (Oct. 16, 2002): TCPA Specification/TPM Q&A. Available at:
http://www.trustedcomputing.org/docs/TPM_QA_1016021.pdf.

— **V** —

Varian (2001):
Varian, Hal R. (Dec. 16, 2001): Economics of Information Technology. Available at: http://www.sims.berkeley.edu/~hal/Papers/maltioli.pdf.

Varian (2002):
Varian, Hal R. (2002): New Chips Can Keep a Tight Rein on Consumers. New York Times, July 4, 2002, at page C2.

Vaughan–Nichols (2003):
Vaughan–Nichols, Steven J. (March 2003): How Trustworthy Is Trusted Computing? IEEE Computer 18.

Volokh (2003):
Volokh, Eugene (2003): The Mechanisms of the Slippery Slope. 116 Harvard Law Review 1026.

— **W** —

Walker, Sharpe (2002):
Walker, Jacqui/ Sharpe, Andrew (2002): Digital Rights Management. 18 Computer Law & Security Report 259.

Ware (2002):
Ware, Donald R. (2002): Research Tool Patents: Judicial Remedies. 30 APILA Quarterly Journal 267.

Weinberg (2002):
Weinberg, Jonathan (2002): Digital TV, Copy Control, and Public Policy. 20 Cardozo Arts & Entertainment Law Journal 277.

Weiser (2001a):
Weiser, Philip J. (2001): Networks Unplugged: Towards a Model of Compatibility Regulation Between Information Platforms. Available at http://www.arxiv.org/html/cs/0109070.

Weiser (2001b):
Weiser, Philip J. (2001): Internet Governance, Standard Setting, and Self-Regulation. 28 Northern Kentucky Law Review 822.

Weiser (2002):
Weiser, Philip J. (2002): Law and Information Platforms. 1 Journal on Telecommunications and High Technology Law 1.

Wintermute (2003):
Wintermute (Jan. 25, 2003): TCPA and Palladium Technical Analysis. Version 1.06. Available at: http://wintermute.homelinux.org/miscelanea/TCPA%20Security.txt.

— **Y** —

Yasukawa (2002):
Yasukawa, Michiko (2002): A Method for Making Dynamic License Agreements in Reuse of Web Contents. 43 (SIG 2) IPSJ Transactions on Databases 179 (in Japanese).

Yasukawa (2003):
Yasukawa, Michiko (2003): A Dynamic License Agreement System for Reuse of Web Contents. In: Meersman, Robert/ Aberer, Karl/ Dillon, Tharam S. (eds.) (2003): Semantic Issues in E-Commerce Systems. IFIP TC2/WG2.6 Ninth Working Conference on Database Semantics. Boston. p. 35.

— Z —

Zittrain (2000):
Zittrain, Jonathan (2000): What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication. 52 Stanford Law Review 1201.