Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 5

Separation of Ownership and the Authorization to Use Personal Computers: Unintended Effects of EU and U.S. Law on IT Security

Lukas Feiler

2010

TTLF Working Papers

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

Sponsors

This project was co-sponsored by the Stanford-Vienna Transatlantic Technology Law Forum (Stanford Law School/University of Vienna School of Law), the Stanford Center for E-Commerce, the Forum on Contemporary Europe at the Freeman Spogli Institute for International Studies at Stanford University, as well as supported by the University of Vienna Research Grant 2010.

About the Author

Lukas Feiler is Vice Director at the European Center for E-Commerce and Internet Law, Vienna, and is working remotely as a software developer and system administrator for Empowered Media, New York. He earned his law degree from the University of Vienna School of Law in 2008 and a Systems Security Certified Practitioner (SSCP) certification from (ISC)² in 2009. He also studied U.S. cyberspace and intellectual property law at Santa Clara University. Previous activities include a traineeship with the European Commission, DG Information Society & Media, Unit A.3 "Internet; Network and Information Security" in Brussels (2009), an internship at Wolf Theiss Attorneys at Law, Vienna (2006), several software developer positions with software companies (2000-2006), and a teaching position for TCP/IP networking and web application development at the SAE Institute Vienna (2002-2006). He is the co-author of the book "On the Way to the Surveillance State? New ICT Surveillance Measures" (2009, in German) and lead developer of the open source project Query2XML, which was accepted for inclusion in the official PHP Extension and Application Repository. He has been a TTLF Fellow since August 2009 and an FCE Research Affiliate since November 2009.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project

Suggested Citation

This TTLF Working Paper should be cited as:
Lukas Feiler, Separation of Ownership and the Authorization to Use Personal Computers: Unintended Effects of EU and U.S. Law on IT Security, TTLF Working Paper No. 5, http://www.law.stanford.edu/program/centers/ttlf/papers/feiler_wp5.pdf.

Copyright

Abstract

It used to be that owners of personal computers typically had full and exclusive authorization to use their computers. This was primarily due to the open architecture introduced with the IBM Personal Computer in the 1980s and proliferated in the 1990s. Recent developments bear evidence of an increasing disconnection between the concept of ownership and that of authorization to use a personal computer (including mobile devices such as notebooks, sub-notebooks, cell phones, smartphones, and PDAs): interference with the closed architecture employed by Apple's iPhone is claimed to constitute a violation under 17 U.S.C. § 1201; the EULA for Windows 7 supposedly grants Microsoft the right to disable a user's operating system if the user is deemed to be in violation of the license terms; the Google Chrome Terms of Service supposedly grant Google the right to install new versions of its product without notice; on July 17, 2009, Amazon remotely deleted certain titles, including Animal Farm and Nineteen Eighty-Four from its customers' ebook devices without consent or notice. This paper analyzes the extent to which EU and U.S. contract law and (para-)copyright law disconnect the concepts of ownership and authorization and how that affects the security of personal computers.

Table of Contents

1. Introduction

It used to be that owners of personal computers typically had full and exclusive authorization to use their computers. The open architecture introduced with the IBM Personal Computer in the 1980s (and proliferated in the 1990s) made it technically possible for the owner to install and uninstall any and all programs or even install an entirely different operating system.

However, this congruence of the concepts of ownership and authorization is not a legal necessity. Authorization to use a computer system is a legal right that may be restricted or

transferred to other parties than the owner by means of statutory law or a contract. This paper will analyze the extent to which EU and U.S. contract law and (para-)copyright[1] law result in the de-authorization of the owner or the authorization of third parties to use the owner's personal computer, which for the purpose of this paper shall also include mobile devices such as notebooks, sub-notebooks, cell phones, smartphones, and PDAs.

The following examples trigger scrutiny of the extent to which EU and U.S. law disconnects the concepts of ownership and authorization to use personal computers:

Regarding its iPhone, Apple claimed that the circumvention of the SIM-lock or a "jail break"[2] constituted a breach of contract and/or a violation of 17 U.S.C. § 1201(a) as it involves the circumvention of a technological measure that effectively controls access to a work protected under 17 U.S.C. When Apple released their version 1.1.1 update for the iPhone on September 27, 2007 users who had previously unlocked their iPhone or had performed a "jail break" discovered that the installation of the update disabled ("bricked") their iPhones entirely.[3] In 2007, Microsoft updated installations of Windows XP and Windows Vista even if the owner of a personal computer had deliberately disabled the auto-update feature.[4] In 2005, Sony BMG distributed music CDs that, when inserted into a computer's CD drive, installed spyware and a rootkit that created vulnerabilities that could

---

[1] Paracopyright refers to legal protections related to but going above and beyond traditional copyright. *Cf.* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.18[B] (2002).

[2] The term "jail break" refers to the act of unlocking the iPhone's file system to allow the execution of programs not authorized by Apple. *See, e.g.,* Timothy J. Maun, *iHack, Therefore iBrick: Cellular Contract Law, the Apple iPhone, and Apple's Extraordinary Remedy for Breach*, 2008 WIS. L. REV. 747, 751.

[3] *See* Katie Hafner, *Altered iPhones Freeze Up*, N.Y. Times, Sept. 29, 2007, at C1, *available at* http://www.nytimes.com/2007/09/29/technology/29iphone.html.

[4] *See* J. Nicholas Hoover, Microsoft Updates Windows Without User Permission, Apologizes (Sept. 13, 2007), http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=201806263. *See also* Bruce Schneier, Microsoft Updates Both XP and Vista Without User Permission or Notification (Sept. 17, 2007), http://www.schneier.com/blog/archives/2007/09/microsoft_updat.html.

be exploited by other malware.[5] The Microsoft License Terms for Windows 7 provide that if Microsoft deems the licensee to be in violation of the license terms, the licensee "may not be able to use or continue to use the software,"[6] supposedly granting Microsoft the authority to remotely disable a user's operating system. On July 17, 2009, Amazon remotely deleted certain titles, including Animal Farm and Nineteen Eighty-Four, from its customers' "Kindle" ebook devices without consent or prior notice.[7]

The disconnection of the concepts of ownership and of authorization to use personal computers occurs in two distinct ways: by de-authorizing owners to use their personal computers and by granting third parties authority over a personal computer, the former addressed in chapter 2 and the latter in chapter 3. Chapter 4 will then assess the effects of this disconnection on the security of personal computers.[8]

2. De-Authorizing Owners

The acquisition of ownership of a personal computer, in principle, transfers full and exclusive authorization to use that computer in any way or form to the new owner. The discussion below describes various statutory and corresponding contractual means that

---

[5] Mark Russinovich, Sony, Rootkits and Digital Rights Management Gone Too Far (Oct. 31, 2005), http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx. J. Alex Halderman & Edward W. Felten, Lessons from the Sony CD DRM Episode (Feb. 14, 2006), http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf.

[6] Microsoft Software License Terms for Windows 7, http://www.microsoft.com/about/legal/useterms/default.aspx (last visited Oct. 20, 2009).

[7] Brad Stone, *Amazon Erases Orwell Books From Kindle*, N.Y. Times, July 18, 2009, at B1, *available at* http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html.

[8] The idea that a disconnection between ownership and authorization would undermine security was first articulated by information security expert Bruce Schneier. *See* Bruce Schneier, *Everyone Wants to "Own" Your PC* (May 4, 2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70802, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 161-3 (2008).

effectively result in de-authorizing the owner from certain uses of his computer (or parts of it).

2.1. Statutory Prohibitions of the Circumvention of Technological Protection Measures

Digital technologies, most notably the Internet, have not only drastically expanded the possibilities for copyright holders to distribute their works but have also created new ways for mass copyright infringement.[9] Technological protection measures were thought to be the "silver bullet" against copyright infringement committed by digital means.[10] As no technological protection measure can be 100% "secure," at least for a long-term period, copyright holders successfully lobbied for a prohibition of the circumvention of technological protection measures.[11]

2.1.1. Statutory Prohibitions

2.1.1.1. International Background

Art. 11 of the WIPO Copyright Treaty (WCT)[12] obligated all contracting parties to provide adequate legal protection and effective legal remedies against the "circumvention of effective technological measures that are used by authors in connection with the exercise

---

[9] *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES 81 et seq. (1999)

[10] *See, e.g.*, LAWRENCE LESSIG, FREE CULTURE 157 (2004).

[11] However, as Hal Varian has argued, it seems that stronger DRM helps system vendors more than the content industry, because the computer industry has fewer competitors in this space (Microsoft, Sony, and Apple being the only serious suppliers for DRM platforms). *See* Hal Varian, Keynote Address to the Third Digital Rights Management Conference, Berlin, Germany (Jan. 13, 2005). *Cf.* Neil Weinstock Netanel, *Digital Rights Management: Temptations of the Walled Garden: Digital Rights Management and Mobile Phone Carriers*, 6 J. ON TELECOMM. & HIGH TECH. L. 77, 77 (2007).

[12] WIPO Copyright Treaty, adopted 20 December 1996, WIPO Doc. CRNR/DC/94; approved on behalf of the European Community with regard to matters within its competence by Council Decision 2000/278, 2000 O.J. (L 89) 6 (EC).

of their rights under the WCT or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."[13]

2.1.1.2. 17 U.S.C. § 1201

The Digital Millennium Copyright Act (DMCA)[14] was enacted on Oct. 28, 1998, *inter alia*, to implement the WCT. The DMCA specifically introduced 17 U.S.C. § 1201 to implement art. 11 WCT.

§ 1201 contains three principal prohibitions regarding the circumvention of technological protection measures:[15]

- § 1201(a)(1) prohibits the circumvention of a technological measure that effectively controls access to a work protected under Title 17 (hereinafter referred to as an "access control measure"). § 1201(a)(3)(A) states that to "circumvent a technological measure" means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."
- § 1201(a)(2) states that no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that: (A) is primarily designed or produced for the purpose of circumventing an access control measure; (B) has only limited

---

[13] For an analysis of art. 11 WCT, which is outside the scope of this paper *see, e.g.*, Jane C. Ginsburg, *Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience*, Columbia Public Law Research Paper No. 5-93 (2005), http://ssrn.com/abstract=785945.

[14] Codified in 17 U.S.C. §§ 1201-1205 (2009).

[15] Prior to the DMCA, some courts held that it was lawful to sell products which enabled consumers to circumvent technological protection measures, because consumers had a right under 17 U.S.C. § 117 to make a backup or archival copy of a program. *See e.g., Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988).

commercially significant purpose or use other than to circumvent an access control measure; or (C) is marketed for use in circumventing an access control measure.

- § 1201(b) contains the same prohibition as § 1201(a)(2) but refers to "a technological measure that effectively protects a right of a copyright owner under Title 17" (hereinafter referred to as a "copy control measure"), instead of referring to an access control measure.

§ 1201 introduced a rather complex regulatory scheme from which two important distinctions arise. First, it differentiates between the act of circumvention itself (§ 1201(a)(1)) and the trafficking in circumvention technology (§ 1201(a)(2) and § 1201(b)).

Second, it distinguishes between access control measures and copy control measures: the prohibition on circumvention only applies to access control measures (§ 1201(a)(1)), while the prohibition on trafficking circumvention technology applies to both (§ 1201(a)(2) and § 1201(b)).

Access control measures (§ 1201(a)) are of primary interest here as they limit the ability to lawfully access one's own personal computer or parts thereof. For this reason, this chapter will focus on § 1201(a).[16]

The first issue to be addressed is how to distinguish between access control measures and copy control measures. Access control measures are defined in § 1201(a)(3)(B) as any technological measure, that "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." However, this statutory definition does not clarify the meaning of the term "access." At this point, it should be noted that, in the field of computer and

[16] For a discussion on whether (para-)copyright law grants copyright owners an "access-right" *see* Thomas Heide, *Copyright in the EU and U.S.: What "Access-Right"?*, 48 J. COPYRIGHT SOC'Y U.S.A. 363 (2001).

information security, it is universally understood that "access controls" do not only determine *whether* but also *what kind of access* is being granted to a subject.[17]

In *Lexmark Int'l, Inc. v Static Control Components, Inc.*, the District Court stated that the term "access" should be given its ordinary customary meaning, which is the "ability to enter, to obtain, or to make use of."[18] It held that an authentication protocol[19] implemented in the plaintiff's printer software in order to authenticate printer cartridges manufactured by the plaintiff constituted an access control measure because the authentication protocol controlled the ability to make use of the printer firmware by preventing the printer from functioning. On appeal, the 6th Circuit disagreed, while applying the same definition of "access."[20] It held that § 1201(a) does not naturally apply when the "work protected under this title" is otherwise accessible. As the object code of the printer software was accessible

---

[17] *See, e.g.*, NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUBLICATION 800-12 – AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK 195 (1995), http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (specifically stating with regard to "logical access control" that "[i]t may also be important to control the *kind of access* that is afforded"). *See also* NAT'L INST. OF STANDARDS AND TECH., FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 200 - MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS 2 (2006), http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (stating with regard to access control that "[o]rganizations must limit information system access to authorized users […] and to the *types of transactions and functions* that authorized users are permitted to exercise" (emphasis added)); *see also* INT'L ORG. FOR STANDARDIZATION, ISO/IEC 27000:2009 INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY, Clause 2.1 (2009) (stating that the term access control "means to ensure that access to assets […] is authorized and restricted based on business and security requirements"); James S. Tiller, *Access Control*, in OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 93, 95 (Harold F. Tipton & Kevin Henry eds., 2007).

[18] *Lexmark Int'l, Inc. v Static Control Components, Inc.*, 253 F. Supp. 2d 943, 967 (E.D. Ky. 2003), vacated and remanded, 387 F.3d 522 (6th Cir. 2004).

[19] The Lexmark printers used an SHA-1 based Message Authentication Code which prevents replay attacks and is based on a secret key. For an explanation of Message Authentication Codes *see* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 455 et seq. (2d ed. 1996).

[20] *Lexmark Int'l, Inc. v Static Control Components, Inc.*, 387 F.3d 522, 546 (6th Cir. 2004).

by directly reading the printer memory—without the benefit of the authentication sequence—the authentication sequence did not restrict "access" to the protected work, rendering § 1201(a) inapplicable. The court therefore effectively imposed the requirement that access control measures must (at least) control the "ability to obtain a copy of the work." A measure that only limits the ability to modify or execute a program would therefore fall outside this definition.[21]

This is in line with other widely noted cases, such as *RealNetworks, Inc. v. Streambox, Inc.* The court held that a "secret handshake" between the plaintiff's RealServer and RealPlayer software constituted an "access control" under § 1201(a), while a "Copy Switch" used by RealServer software to signal that RealPlayer software should disable the copy functionality of a particular media stream, was considered a "copy control measure" under § 1201(b).[22] In *Universal City Studios, Inc. v. Corley*, the 2nd Circuit held that "CSS," the encryption technology used by motion picture studios on DVDs to prevent the unauthorized viewing and copying of motion pictures is an "access control measure."[23]

The second issue to be addressed is that of "effective" control. Both § 1201(a) and (b) only cover "effective" measures. As § 1201(a)(3)(B) as well as (b)(2)(b) refer to "the ordinary course" of the measure's operation, a rather low standard has been adopted by most courts.[24]

---

[21] In the field of computer security, on the other hand, measures that only determine whether a file can be executed or written to are also considered "access controls." *Cf.* SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 131 (3d ed. 2003).

[22] *RealNetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

[23] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). For the trial court decision *see Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

[24] *See e.g.*, *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000) (holding that whether the measure is a "strong means of protection" or not is irrelevant). *See also I.M.S. Inquiry Mgmt. Sys. v Berkshire Info. Sys.* 307 F. Supp. 2d 521 (S.D.N.Y. 2004) (holding that password protection constitutes an effective technological protection measure. However, the defendant's motion to dismiss was granted on grounds that accessing the plaintiff's computer system through unauthorized use of a password issued to a

The last issue to be discussed with regard to the scope of § 1201(a) is that of "circumvention." Section 1201(a)(3)(A) states that to "circumvent a technological measure" means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, *without the authority of the copyright owner*" (emphasis added). Somebody who has *the authority to circumvent* would therefore not violation § 1201(a)(1).

Some commentators suggest that *authority to access* the work is sufficient to evade a violation of § 1201(a)(1).[25] In *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, the Federal Circuit seems to have gone in that direction. At issue was the software embedded in the garage door systems manufactured by the plaintiff, specifically, whether the plaintiff's software was protected by copyright and an access control measure. The court examined whether use of a remote control manufactured by the defendant, in the plaintiff's garage door system, would constitute a circumvention under § 1201(a)(1) and make the defendant liable under § 1201(a)(2) for trafficking in circumvention technology. The court sided with the defendant, holding that the plaintiff's customers did not violate § 1201(a)(1) since the Copyright Act authorized them *to use* the copy of the plaintiff's copyrighted software embedded in the garage door systems that they purchased. The court effectively read "authority of the copyright owner" as "authority *to use the protected work*" as opposed to "authority *to circumvent the access control*." By trafficking in alternative remote controls the defendant therefore did not violate § 1201(a)(2).[26]

---

party other than the defendant did not constitute a "circumvention" targeted by § 1201(a)). *But cf. Agfa Monotype Corp. v. Adobe Sys.*, 404 F. Supp. 2d 1030 (N.D. Ill. 2005) (holding that embedded "bits" which encode permissions do not by themselves constitute an "effective" technological protection measure).

[25] *See* Markus Fallenböck, *On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions* 19 (2002), http://www.ijclp.net/files/ijclp_web-doc_4-7-2003.pdf (framing it as a question of whether "access" refers only to the initial access, or also to all subsequent acts of gaining access). *See also* JESSICA LITMAN, DIGITAL COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET 151 (2001).

[26] *Chamberlain Group, Inc. v. Skylink Tech., Inc.*, 381 F.3d 1178, 1204 (Fed. Cir. 2004).

However, the plain language of § 1201(a)(3)(A) clearly states that authority has to be granted with regard to circumvention, i.e. the activities described in said subsection (descramble, decrypt, otherwise avoid, bypass, remove, deactivate, or impair a technological measure). Accordingly, in *Universal City Studios, Inc. v. Corley*, the 2nd Circuit ruled that it was irrelevant whether an individual who buys a DVD has the authority *to view* the DVD. Section 1201(a)(3)(A) would only exempt from liability those users who have the authority *to decrypt* an encrypted DVD but not those who merely have the authority *to view* a DVD.[27]

2.1.1.3. The EU Computer Programs Directive and the EU Copyright Directive

EU law[28] provides three distinct statutory schemes for technological protection measures: the EU Computer Programs Directive (hereinafter referred to EUCPD),[29] the EU Copyright Directive (hereinafter referred to as EUCD),[30] and the EU Conditional Access Directive.[31] The latter is not of interest here as it concerns access to a service and therefore has no direct impact on a user's authority to use his or her personal computer.

---

[27] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 444 (2d Cir. 2001).

[28] All 27 Member States having deposited their ratification instruments in Rome, the Treaty of Lisbon will enter into force on Dec. 1, 2009. Art. 1 of the Treaty on European Union as amended by the Treaty of Lisbon provides that "[t]he Union shall replace and succeed the European Community." In anticipation of this succession, this paper generally refers to the EU where previously referred to the EC.

[29] Parliament and Council Directive 2009/24, 2009 O.J. (L 111) 16-22 (EC). This Directive is a re-codification of Council Directive 91/250, 1991 O.J. (L 122) 42-46 (EEC), taking into account the amendments performed by Council Directive 93/98, 1993 O.J. (L 290) 9-13 (EEC). *See* Recital 1 Parliament and Council Directive 2009/24.

[30] Parliament and Council Directive 2001/29, 2001 O.J. (L 167) 10-19 (EC).

[31] Parliament and Council Directive 98/84, 1998 O.J. (L 320) 54-57 (EC).

While the EUCPD applies only to technological protection measures that protect computer programs, the EUCD applies to the measures that protect all other copyrighted works.[32]

At first blush, it would seem that only the EUCPD, which deals exclusively with software protection measures, is significant to the issue of authority to use one's personal computer. However, as will be described below, the de-authorizing effect of a technological protection measure can be equally significant even if the work protected is not a computer program. Due to its broader scope, the EUCD shall be discussed first.

Similar to 17 U.S.C. § 1201, art. 6 EUCD provides a distinction between the act of circumvention itself (art. 6(1) EUCD) and trafficking in circumvention technology (art. 6(2) EUCD).

Art. 6(1) EUCD obligates EU Member States to provide adequate legal protection against the circumvention of any "effective technological measures," which is carried out with knowledge, or reasonable grounds for knowing, that such objective is being pursued.

This wording goes beyond 17 U.S.C. § 1201(a)(1)(A) in the sense that it requires that the person performing the circumvention does so knowingly or at least negligently ("with reasonable grounds to know").[33]

The term "technological measures," as it is used in art. 6(1) EUCD, is defined in art. 6(3) sentence 1 EUCD as any technology, device or component that, in "the normal course of its operation," is designed to "prevent or restrict acts, in respect of works or other subjectmatter, which are not authorised by the rightholder of any copyright or any right

---

[32] Recital 50 EUCD provides that the EUCD "should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive" (referring to Council Directive 91/250, now Parliament and Council Directive 2009/24).

[33] *Cf.* Markus Fallenböck, *On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions* 39 (2002), http://www.ijclp.net/files/ijclp_web-doc_4-7-2003.pdf.

related to copyright as provided for by law or the sui generis right" provided for in Chapter III of the EU Database Directive.[34]

According to art. 6(3) sentence 2 EUCD, a technical measure shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through "application of an *access control* or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a *copy control* mechanism, which achieves the protection objective" (emphasis added).

This wording indicates that art. 6(1) EUCD prohibits the circumvention of both access control measures and copy control measures. The circumvention prohibition of art. 6(1) EUCD is therefore, at least in this regard, broader than that of 17 U.S.C. § 1201 which only prohibits the circumvention of access control measures but not of copy control measures.[35] As art. 6(1) EUCD covers both types of measures, their distinction, which is important under 17 U.S.C. § 1201, is almost irrelevant here.

Art. 6(2) EUCD prohibits the trafficking of circumvention technology. It states that Member States shall provide adequate legal protection against "the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services" which fulfill any of the following three conditions: (a) they are promoted, advertised or marketed for the purpose of circumvention of any effective technological measures; (b) they have only a limited commercially significant purpose or use other than to circumvent; or (c) they are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating circumvention. The substance and even the wording of art. 6(2) EUCD is almost identical to that of 17 U.S.C. § 1201(a)(2) (regarding access control measures) and 17 U.S.C. § 1201(b) (regarding copy control measures).

---

[34] Parliament and Council Directive 96/9, 1996 O.J. (L 77) 20-28 (EC).

[35] *See* chapter 2.1.1.2 *supra.*

I shall now consider the EUCPD which, according to Recital 50 EUCD, applies exclusively to "technological measures used in connection with computer programs." Art. 7(1)(c) EUCPD provides that Member States shall provide appropriate remedies against the acts of "putting into circulation, or the possession for commercial purposes of, any means" whereby the sole intended purpose is "to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program."

Art. 7(1)(c) EUCPD is far more narrow than art. 6 EUCD or 17 U.S.C. § 1201. First, it only prohibits "acts of putting into circulation" and "the possession for commercial purposes." The act of circumvention itself is therefore *not* prohibited.

Second, a plain reading of art. 7(1)(c) EUCPD only prohibits putting "means" into circulation, or possessing "means." Unlike art. 6(2) EUCD or 17 U.S.C. § 1201, providing services for the purpose of facilitating circumvention is not prohibited.

Third, it only covers "means" where the "sole intended purpose of which is to facilitate the unauthorised removal or circumvention" of a technical protection measure. In contrast to art. 6(2) EUCD and 17 U.S.C. § 1201, art. 7(1)(c) EUCPD does not cover technology that has only limited commercially significant purpose or use other than to circumvent[36] or that is promoted, advertised or marketed for the purpose of circumvention.[37]

Finally, art. 7(1)(c) EUCPD only protects "technical devices which may have been applied to protect a computer program." The term "device" implies a limitation of scope to physical (i.e. hardware-based) protection measures. However, the German, French and Spanish language versions all use the equivalent of the term "means" ("Mittel" in German, "moyen" in French, and "medio" in Spanish). Under the principle of uniform interpretation,[38] the different language versions must be given a uniform interpretation. As

---

[36] *Cf.* art. 6(2)(b) EUCD and 17 U.S.C. § 1201(a)(2)(B) and (b)(1)(B).

[37] *Cf.* art. 6(2)(a) EUCD and 17 U.S.C. § 1201(a)(2)(C) and (b)(1)(C).

[38] See Case 30/77, Régina v. Bouchereau, 1977 E.C.R. 1999.

there is a divergence between the versions, art. 7(1)(c) EUCPD must be interpreted by reference to the purpose and general scheme of the EUCPD as a whole. As the EUCPD is concerned with software, it seems logical that this provision captures not only hardware-based but also software-based measures protecting software.

2.1.2. Statutory Exemptions

2.1.2.1. 17 U.S.C. § 1201

Before examining the exemptions contained in § 1201 itself, the relationship between § 1201 and the fair use doctrine (incorporated in 17 U.S.C. § 107) needs to be examined. Section 1201(c)(1) provides that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."[39] Courts are split regarding the interpretation of this clause.

In *Universal City Studios, Inc. v. Corley*, the 2nd Circuit rejected the defendant's assertion that § 1201(c)(1) should be read to allow the circumvention of technology protecting copyrighted material when "fair use" exempts the infringing use of the material at issue from copyright liability. The court held that § 1201(c)(1) merely clarifies that § 1201 is only concerned with the question of circumvention (or the trafficking of circumvention technologies), and not the question of whether material obtained in a manner made illegal by § 1201 can be legitimately used by reason of fair use.[40]

On the other hand, in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.* the Federal Circuit rejected a reading of § 1201 that would grant a copyright holder unlimited rights to hold circumventors liable for merely accessing a work, even if that access involved only rights that the Copyright Act exempts for the public.[41] Such a reading would be contrary to

---

[39] *Inter alia*, this refers to the exclusive rights of a copyright holder under § 106 of the Copyright Act and defenses against copyright infringement such as fair use (§ 107 of the Copyright Act).

[40] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001).

[41] *Chamberlain Group, Inc. v. Skylink Tech., Inc.*, 381 F.3d 1178, 1200 (Fed. Cir. 2004). *See also Storage Tech. Corp. v. Custom Hardware Engineering & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed. Cir., 2005).

§ 1201(c)(1), and the court thereby interpreted § 1201 as only prohibiting "forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners."[42] The court further stated that the DMCA cannot allow the plaintiff "to retract the most fundamental right that the Copyright Act grants consumers: the right to use the copy of Chamberlain's embedded software that they purchased."[43]

The opposing conclusions drawn by the courts from § 1201(c)(1) is indeed remarkable[44] and leaves users with a significant legal risk should they decide to rely on a fair use defense.

§ 1201 itself creates two types of possible exemptions: the ones codified in § 1201(d) to (j) and those created by the Librarian of Congress in accordance with § 1201(a)(1)(B) and (C). We shall first examine the former.

§ 1201 codifies various exemptions to the prohibitions of § 1201: Exemption for nonprofit libraries, archives, and educational institutions (§ 1201(d));[45] law enforcement, intelligence, and other government activities (§ 1201(e));[46] reverse engineering (§ 1201(f)),[47] encryption research (§ 1201(g)),[48] exceptions regarding minors (§ 1201(h)),[49]

---

[42] *Chamberlain Group, Inc. v. Skylink Tech., Inc.*, 381 F.3d 1178, 1202 (Fed. Cir. 2004). For a similar case *see Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed. Cir. 2005).

[43] *Chamberlain Group, Inc. v. Skylink Tech., Inc.*, 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[44] From a perspective of statutory interpretation, it also seems noteworthy that the *Chamberlain* court and the *Corley* court cited two different but consecutive pages of the legislative history, yet drawing contrary conclusions. *See* H.R. REP. NO. 105-551, pt. 2, at 25, 26 (1998).

[45] § 1201(d) only provides an exemption for § 1201(a)(1).

[46] § 1201(e) provides exemptions for § 1201(a)(1), (2) and § 1201(b).

[47] § 1201(f) provides exemptions for § 1201(a)(1), (2) and § 1201(b).

[48] § 1201(g) provides an exemption for § 1201(a)(1) and a narrow exemption for § 1201(a)(2).

[49] § 1201(h) provides an exemption for § 1201(a)(1) and (2).

protection of personally identifying information (§ 1201(i));[50] and security testing (§ 1201(j)).[51] Regarding the issue of computer security and the authority to use one's own personal computer, only § 1201(f), (g), (i), and (j) are of relevance.[52]

§ 1201(f) provides exemptions for reverse engineering[53] that is performed for the purpose of obtaining interoperability information: According to § 1201(f)(1), it does not constitute a violation of § 1201(a)(1) to circumvent an access control measure that has been applied to a computer program if a right to use the program has been lawfully obtained and the circumvention is performed for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability between an independently created computer program[54] and other programs. Section 1201(f)(2) and (3) provide similar exemptions regarding § 1201(a)(2) and (b). However, § 1201(f) clearly only targets people that aim to develop interoperable software.[55] It does not allow access control measures to be circumvented for the purpose of installing (as opposed to

---

[50] § 1201(i) only provides an exemption for § 1201(a)(1).

[51] § 1201(j) provides an exemption for § 1201(a)(1) and (2).

[52] For an extensive description of these exemptions *see* Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium,"* 23 COLUM.-VLA J.L. & ARTS 137, 148-52 (1999).

[53] Reverse engineering can be defined as the process of discovering technological information about computer hard- or software by examining it. *Cf.* ELDAD EILAM, REVERSING: SECRETS OF REVERSE ENGINEERING 3 et seq. (2005).

[54] *See* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.04[B][1] (2002).

[55] *See Davidson & Assoc. v. Internet Gateway*, 334 F. Supp. 2d 1164, 1185 (E.D. Mo. 2004) (holding that a § 1201(f) defense was not available because the defendants did not try to independently create an interoperable computer program but a program that was intended as a functional alternative), *aff'd sub nom. Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005). *Cf.* Jane C. Ginsburg, The Pros and Cons of Strengthening Intellectual Property Protection: Technological Protection Measures and Section 1201 of the US Copyright Act 11 (Feb. 1, 2007), http://ssrn.com/abstract=960724.

developing) interoperable software. Section 1201(f) therefore has minimal effect on the authority to use one's own personal computer.[56]

§ 1201(g) provides an exemption from § 1201(a)(1) and (a)(2)[57] for encryption research, which § 1201(g)(1)(A) defines as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works," if these activities are conducted to "advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products." Although important in the field of cryptography, this exemption also has little effect with regard to the authority to use one's own personal computer.

§ 1201(i) creates an exemption from § 1201(a)(1)—but not from (a)(2) or (b)—if the circumvention is performed for the purpose of protecting personally identifying information (PII). A natural person may circumvent an access control measure if it (or the work it protects) contains the "capability of collecting or disseminating personally identifying information reflecting the online activities"[58] of the person who seeks to circumvent the measure. According to § 1201(i)(1)(B), for the exemption to apply, it is further required that the measure (or the work it protects) collects or disseminates the PII without providing conspicuous notice of such collection or dissemination, *and* without providing the capability to prevent or restrict such collection or dissemination. This drastically narrows the applicability of § 1201(i).[59] If the user so much as receives a conspicuous notice of the data collection or dissemination, the exemption does not apply. Furthermore, the exemption does not apply to PII in general but only to PII that reflects "online activities." Protected software that collects information about offline activities (e.g.

---

[56] For further discussion of § 1201(f) *see* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.04[B] (2002).

[57] The exemption from § 1201(a)(2) only applies regarding "another person with whom [the researcher] is working collaboratively" (§ 1201(g)(4)(B)). It is therefore a very limited one.

[58] § 1201(i)(1)(A).

[59] *See* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.05[B][1] (2002).

writing a document using a locally installed word processor instead of Google Docs) falls outside the scope of § 1201(i).

§ 1201(j) provides an exemption from § 1201(a)(1) and (2) for "security testing." This term is defined in § 1201(j)(1) as accessing a computer, computer system, or computer network, "solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network." It is important to recognize that this definition very much centers on the term "vulnerability" (which is used synonymously with "security flaw"). However, vulnerability is only one of many elements that can be addressed when mitigating security risks to a computer, computer system, or computer network. Other elements are: the asset, safeguards, vulnerabilities, threats, and threat agents. § 1201(j) allows an owner of a computer system to circumvent an access control measure in an effort to mitigate his security risk by "testing, investigating, or correcting [a] vulnerability." However, § 1201(j) does not provide an exemption for other risk mitigation strategies such as reducing the asset (e.g. testing, investigating, or correcting the amount of information stored by a protected work; *cf.* § 1201(i) above) or adding safeguards (e.g. encrypting information resources protected by the access control measure).

Furthermore, as the term "security testing" itself indicates, the primary purpose of § 1201(j) is not to allow the improvement of the security of the personal computer on which the access control measure is installed. § 1201(j)(3) states that one of the factors to be considered in determining if a person qualifies for the § 1201(j) exemption is whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer system, or shared directly with the developer of the computer system.[60]

---

[60] The second factor to be considered is of limited importance in this context: whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under Title 17 or a violation of applicable law other than § 1201, including a violation of privacy or breach of security (§ 1201(j)(3)(B)).

In addition to the exemptions codified in § 1201(d) to (j), subsections § 1201(a)(1)(B) and (C) provide a more general exemption and an associated rulemaking procedure. The prohibition of § 1201(a)(1) shall not apply[61] to persons who are users of "a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under Title 17." Identification of those "classes of works" is left up to the Librarian of Congress pursuant to § 1201(a)(1)(B): every three years, he shall make the determination in a rulemaking proceeding. Under § 1201(a)(1)(C), the Librarian shall examine the following factors in conducting the rulemaking: (i) the availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and (v) other factors the Librarian considers appropriate.

As of writing, the 2006 publication of the Librarian of Congress' determination is still in force.[62] It was extended by the Librarian on an interim basis on Oct. 27 2009[63] and provides six classes of copyrighted works of which only the last two are relevant:[64]

---

[61] A very strong argument can be made that creating an exemption from § 1201(a)(1) while not doing so for § 1201(a)(2) gives users the right but not the means to perform a circumvention, leaving those who lack technical expertise effectively checkmated. *See* David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673 (2000).

[62] 71 Fed. Reg. 68472-80 (Nov. 27, 2006). Prior determinations were published as 68 Fed. Reg. 62011-18 (Oct. 31, 2003) and 65 Fed. Reg. 64556-574 (Oct. 27, 2000). For a content analysis of the first two proceedings, conducted in 2000 and 2003, *see* Bill D. Herman & Oscar Gandy, *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121 (2006), *available at* http://ssrn.com/abstract=844544. For a review of the Librarian of Congress's 2006 exemption process *see* John Haubenreich, *The iPhone and the DMCA: Locking the Hands of Consumers*, 61 VAND. L. REV. 1507, 1518 et seq. (2008).

[63] 74 Fed. Reg. 55138-9 (Oct. 27, 2009).

- Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network (37 C.F.R. § 201.40(b)(5) (2009)).

- Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities (37 C.F.R. § 201.40(b)(6) (2009)).

The first class affords owners of a cell phone full authority to use the phone irrespective of any access controls but does so only for the limited purpose of connecting to a different carrier's network (referred to hereafter as the "SIM lock exemption").[65] A cell phone, acquired from a specific carrier usually ships with firmware that is programmed to only accept SIM cards from that carrier. By asserting that the firmware is a copyrighted work that is protected by access control measures, at least one carrier had previously successfully argued that "breaking" a SIM lock would constitute a violation under

---

[64] The other classes deal with audiovisual works when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors (37 C.F.R. § 201.40(b)(1) (2009)); computer programs and video games distributed in formats that have become obsolete, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive (37 C.F.R. § 201.40(b)(2) (2009)); computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete (37 C.F.R. § 201.40(b)(3) (2009)); and literary works distributed in ebook format when all existing ebook editions of the work contain access controls that prevent the enabling either of the book's read–aloud function or of screen readers (37 C.F.R. § 201.40(b)(4) (2009)).

[65] In particular, this exemption does not cover so-called "jail breaking" (i.e. gaining access to the file system) of an iPhone.

§ 1201(a).[66] The first court applying the new exemption held that unlocking cell phones for the purpose of selling them for a profit was not "for the sole purpose of lawfully connecting to a wireless telephone communication network" and therefore outside of the exemption's scope.[67]

The second class to be discussed here concerns sound recordings and audiovisual works distributed on a CD that contains access control measures that "create or exploit security flaws or vulnerabilities" given that the circumvention is accomplished solely for the purpose of "good faith testing, investigating, or correcting such security flaws or vulnerabilities" (hereinafter referred to as the "Sony BMG exemption"). This class was created in response to a digital rights management system contained on music CDs distributed by Sony BMG Music Entertainment.[68] Upon insertion into a computer's CD drive, a spyware and a rootkit were installed.[69] It might have been argued that § 1201(j) already provides an exemption for such cases but in his recommendation to the Librarian of Congress, the Register of Copyrights stated that "it is not clear whether that provision

---

[66] *See TracFone Wireless, Inc. v. Sol Wireless Group, Inc.*, No. 05-23279-CIV (S.D. Fla., Feb. 28, 2006), available at http://www.copyright.gov/1201/2006/hearings/granick.pdf, 50 et seq.

[67] *TracFone Wireless, Inc. v. Dixon*, 475 F. Supp. 2d 1236, 1238 (M.D. Fla. 2007). For a discussion of the effects of the SIM lock exemption on iPhone users, *see* Mark Defeo, *Unlocking the iPhone: How Antitrust Law Can Save Consumers from the Inadequacies of Copyright Law* 49 B.C. L. REV. 1037, 1065 et seq. (2008).

[68] *See* 71 Fed. Reg. 68477 (Nov. 27, 2006) for the detailed rationale for 37 C.F.R. § 201.40(b)(6).

[69] This "automatic" installation required Microsoft Windows' AutoRun feature to be turned on, which it is by default. For a detailed technical description see Mark Russinovich, Sony, Rootkits and Digital Rights Management Gone Too Far (Oct. 31, 2005), http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx. *See also* J. Alex Halderman & Edward W. Felten, Lessons from the Sony CD DRM Episode (2006), http://www.cse.umich.edu/~jhalderm/pub/papers/rootkit-sec06.pdf. In response Sony BMG published a program to uninstall the software. However, the uninstaller itself created new risks. *See* Mark Russinovich, More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home (Nov. 4, 2005), http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx.

extends to such conduct."[70] The ambiguity is demonstrated in the fact that Mark Russinovich, who first publicized the details about the Sony BMG "DRM," was actually not the first to discover it: Edward Felten and J. Alex Halderman discovered the rootkit a month prior to Russinovich but feared a lawsuit under § 1201 if they disclosed it without the record label's authorization.[71]

The final issue to discuss with regard to statutory exemptions is whether they are capable of contractual derogation. Claims under contract law are of course subject to the preemption doctrine. Congress' power to preempt state law directly stems from the Supremacy Clause of the U.S. Constitution.[72] 17 U.S.C. § 301 provides for an express preemption regarding "all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 […]." But § 301 is not applicable in the context of § 1201 as the latter does not deal with any of the exclusive rights in copyrighted works enumerated in § 106.[73]

However, claims under contract law might be subject to a form of implied preemption if § 1201 is found to be "so pervasive as to make reasonable the inference that Congress left no room for the States to supplement it"[74] (field preemptions).[75]

---

[70] *See* 71 Fed. Reg. 68477 (Nov. 27, 2006).

[71] *See* Transcript of the Public Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems For Access Control Technologies, Mar. 31 2006, 8 et seq., http://www.copyright.gov/1201/2006/hearings/index.html. *See also* Anne Broache & Declan McCullagh, *Seeking changes to the DMCA*, CNET News.com, Apr. 3, 2006, http://www.zdnetasia.com/news/business/0,39044229,39347541,00.htm.

[72] U.S. Const. art. VI, § 2 states "This Constitution, and the Laws of the United States which shall be made in Pursuance thereof […] shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the contrary notwithstanding."

[73] *Cf.* Kevin McReynolds, *SDMCA Laws: Preemption and Constitutional Issues*. 12 UCLA ENT. L. REV. 63, 81 (2004).

[74] *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947).

It remains to be seen how courts will deal with efforts of "contracting around" the statutory exemptions of § 1201. In particular, contract claims might find support in the requirement that the circumvention must "not constitute […] a violation of applicable law." This requirement (or similar forms thereof) are contained in the security testing exemption (§ 1201(j)(2)), the exemption for the protection of personally identifying information (§ 1201(i)(1)(C)), the encryption research exemption (§ 1201(g)(2)(C)), the reverse engineering exemption (§ 1201(f)(3)), and the SIM lock exemption (37 C.F.R. § 201.40(b)(5)).[76]

2.1.2.2. The EU Computer Programs Directive and the EU Copyright Directive

In stark contrast to 17 U.S.C. § 1201, the EUCD only provides for one statutory exemption, and none are available through the EUCPD[77].

Recital 48 EUCD states that the legal protection of technological protection measures "should not hinder research into cryptography." If a circumvention is performed for the purpose of cryptography research, the prohibitions of art. 6 EUCD therefore do not apply. However, it should be noted that cryptography is traditionally defined as "the art and science of keeping messages secure"[78] as opposed to the art and science of breaking encrypted messages (referred to as cryptanalysis).[79]

---

[75] The second form of implied preemption, referred to as "conflict preemption" (*see Florida Lime & Avocado Growers, Inc. v. Paul*, 373 U.S. 132, 142-43 (1963) (holding that State law is preempted where compliance with both federal and state regulations is a physical impossibility)) seems a rather remote possibility. For a more extensive discussion on § 1201 and the issue of preemtion *see* Kevin McReynolds, *SDMCA Laws: Preemption and Constitutional Issues*. 12 UCLA ENT. L. REV. 63 (2004).

[76] *See* Timothy J. Maun, *iHack, Therefore iBrick: Cellular Contract Law, the Apple iPhone, and Apple's Extraordinary Remedy for Breach*, 2008 WIS. L. REV. 747, 791.

[77] *See* THOMAS DREIER & BERNT HUGENHOLTZ, CONCISE EUROPEAN COPYRIGHT LAW 235 (2006).

[78] BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 1 (2d ed. 1996).

[79] Cryptography and cryptanalysis are collectively referred to as cryptology; *see id.*

Furthermore, regarding the prohibition of circumventions performed for the purpose of making noninfringing uses, the EUCD implements a remarkable approach.[80] Art. 6(4) EUCD provides that only in the absence of voluntary measures taken by rightholders[81] shall Member States take appropriate actions to ensure that noninfringing[82] uses are possible.[83] This provision constitutes a very strong interference of law as it not only prohibits all circumventions by default (whether or not performed to make noninfringing uses), but also leaves much latitude and discretion to Member States for regulating technical protection measures with respect to the uses they must permit.[84] The consequence of insufficient voluntary measures must be emphasized: it does *not* give a user permission to circumvent, but rather, it triggers a Member State's obligation to compel rightholders to

---

[80] This issue has been subject of much debate between the European Commission, the Council, and the European Parliament. *See* Communication from the Commission to the European Parliament pursuant to the second subparagraph of Article 251 (2) of the EC Treaty concerning the common position of the Council on the adoption of a Directive of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information Society, SEC(2000) 1734 final (Oct. 20, 2000). *See also* Markus Fallenböck, *On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions* 42 et seq. (2002), http://www.ijclp.net/files/ijclp_web-doc_4-7-2003.pdf.

[81] According to art. 6(4) EUCD these measures include agreements between rightholders and other parties concerned.

[82] Art. 6(4) EUCD refers to "exception[s] or limitation[s] provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e)."

[83] *Cf.* Urs Gasser & Michael Girsberger, Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States 9 et seq. (2004), http://cyber.law.harvard.edu/media/files/eucd.pdf.

[84] *Cf.* Markus Fallenböck, *On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions* 42 (2002), http://www.ijclp.net/files/ijclp_web-doc_4-7-2003.pdf. *Cf. also* Thomas P. Heide, *Copyright, Contract and the Legal Protection of Technological Measures – Not "the Old Fashioned Way": Providing a Rationale to the "Copyright Exceptions Interface"* 11, http://ssrn.com/abstract=418000.

permit certain noninfringing uses.[85] A circumvention of technological protection measures is therefore categorically prohibited under art. 6 EUCD. This is in stark contrast to 17 U.S.C. § 1201 which provides numerous statutory exemptions from the circumvention prohibition.

2.1.3. Comparative Assessment of 17 U.S.C. § 1201, the EU Computer Programs Directive and the EU Copyright Directive

17 U.S.C. § 1201 as well as the EUCD and the EUCPD effectively de-authorize the owner of a personal computer to use certain software components of the computer. Although 17 U.S.C. § 1201—in contrast to the EUCD and the EUCPD—does contain significant statutory exemptions (in particular regarding security testing), it does not contain a "fair use" exemption. Neither do the EUCD or the EUCPD take the exceptions and limitations of traditional copyright into account. Ultimately, the breadth of the de-authorization has to be determined on a case-by-case basis. It depends on two aspects of the technological protection measure in question.

First, what works does the technological protection measure protect? The more works a technological protection measure protects, the more the user's authority to use his computer is diminished. For example, if the technological protection measure protects all system files and all files ever installed on the system, the owner's authority is practically reduced to zero.

Second, and probably more importantly, what else does the technological protection measure effectively prevent access to? Even if the technological protection measure only protects an insignificant graphic work in the form of a small JPEG file, stored somewhere on the operating system's file system, the technological protection measure might nevertheless result in a very significant de-authorization if it does not only prevent access

---

[85] *See* NICOLA LUCCHI, DIGITAL MEDIA & INTELLECTUAL PROPERTY 58 et seq. (2006). For how the EUCD was transposed in the EU Member States *see, e.g.*, Urs Gasser & Michael Girsberger, Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States 12 et seq. (2004), http://cyber.law.harvard.edu/media/files/eucd.pdf.

to said JPEG file (i.e. by means of file encryption) but to the entire file system altogether. This is essentially why technological protection measures that protect works other than computer programs can have an equally de-authorizing effect.

In the example above, the breadth of de-authorization would not be proportional to the protected work. However, proportionality to the protected work is not a requirement under 17 U.S.C § 1201, or the EUCPD. By contrast Recital 48 EUCD does state that the legal protection of technological protection measures "should respect proportionality."[86] However, this is not sufficient to exempt all "overly protective" technological protection measures from the legal protection afforded by the plain language of art. 6(1) EUCD. Recital 48 EUCD also specifically refers in the same sentence to "devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection." Its comprehensive meaning is understood as demanding proportionality with regard to a circumvention technology's alternative use(s), which are enumerated in art. 6(2)(b) EUCD.

Ultimately, 17 U.S.C § 1201, the EUCD, and the EUCPD give copyright holders the legal power to create closed systems[87] and protect them from any interference by the owner of the personal computer. As further discussed below, this drastically reduces the owner's capability to mitigate risks to which the personal computer is exposed. Furthermore, it increases the homogeneity of personal computers resulting in a higher probability of "class breaks" (as defined below in chapter 4.3), possibly compromising entire product lines.

---

[86] *Cf. also* art. 5(4) Treaty on European Union as amended by the Treaty of Lisbon, 2006 O.J. (C 321E) (stating that "[u]nder the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.").

[87] *See* Timothy B. Lee, *Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act, Cato Institute Policy Analysis no. 564* 3 (2006), http://www.cato.org/pubs/pas/pa564.pdf.

3. Authorizing Third Parties

3.1. Authorizing Vendors to Hinder the Functioning of the Computer

Some end-user license agreements contain a provision that supposedly grants the vendor the authority to hinder the functioning of the licensed software if the licensee (usually the owner of the computer) is deemed in violation of the terms of the contract. This is particularly severe if the software in question is an operating system.

For example, the Microsoft Software License Terms for Windows 7 provide in § 5.c:

> If, after a validation check, the software is found to be counterfeit, improperly licensed, a non-genuine Windows product, or include unauthorized changes, the functionality and experience of using the software will be affected, for example: […] you may *not be able to use or continue to use the software* or some of the features of the software […].[88] (emphasis added)

Contract provisions like the one cited above raise the question of whether they would be enforceable. This issue is discussed below under U.S. law and EU law.

3.1.1. Enforceability Under U.S. Law

Due to the economic importance of the State of California, the following discussion will focus exclusively on California state law.[89]

End-user license agreements usually come in the form of shrink-wrap or click-wrap contracts:

Shrink-wrap contracts are contracts of adhesion shipped inside retail software packages and therefore not accessible to the user before opening the package. The user is only left

---

[88] Microsoft Software License Terms for Windows 7, http://www.microsoft.com/about/legal/useterms/default.aspx.

[89] The interpretation of the specific license cited above is governed by Washington state law. *See* Microsoft Software License Terms for Windows 7, § 24(a), http://www.microsoft.com/about/legal/useterms/default.aspx. For a discussion of the Washington unconscionability standard and its application on the Windows Vista EULA *see* Rebecca K. Lively, *Microsoft Windows Vista: The Beginning or the End of End-User License Agreements as We Know Them?*, 39 ST. MARY'S L. J. 339, 358 et seq. (2007).

with the choice of either accepting the terms by using the software or rejecting them by returning the package to the store. In *ProCD v. Zeidenberg*, the 7th Circuit famously held that shrink-wrap contracts are indeed enforceable.[90] However, as shrink-wrap contracts simply employ a different method of contract formation, they are still vulnerable to general contract defenses, in particular, unconscionability.[91]

Click-wrap contracts are very similar to shrink-wrap contracts in the sense that the licensee can either "take it or leave it." The only difference is that they are not printed on paper but displayed on a computer screen. The user can either accept the terms by clicking on an acceptance button or aborting the installation. Today, almost all standard software products employ click-wrap contracts. Like shrink-wrap contracts, click-wrap contracts are enforceable but subject to defenses such as unconscionability.[92]

Under California contract law, the doctrine of unconscionability has a procedural and a substantive element. The procedural element focuses on oppression or surprise due to unequal bargaining power while the substantive element focuses on overly harsh or one-sided results. A contract provision is unenforceable due to unconscionability only if both elements are satisfied. However, the two prerequisites "need not both be present to the same degree."[93] A "sliding scale" is to be applied so that "the more substantively

---

[90] *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996).

[91] *Cf.* Timothy J. Maun, *iHack, Therefore iBrick: Cellular Contract Law, the Apple iPhone, and Apple's Extraordinary Remedy for Breach*, 2008 WIS. L. REV. 747, 764 et seq.

[92] *See* Kevin Grierson, *Enforceability of "Clickwrap" or "Shrinkwrap" Agreements Common in Computer Software, Hardware, and Internet Transactions*, 106 A.L.R. 5th 309 (2003). *See also* Timothy J. Maun, *iHack, Therefore iBrick: Cellular Contract Law, the Apple iPhone, and Apple's Extraordinary Remedy for Breach*, 2008 WIS. L. REV. 747, 765.

[93] *Shroyer v. New Cingular Wireless Services, Inc.*, 498 F.3d 976, 982 (9th Cir. 2009) (quoting *Nagrampa v. MailCoups, Inc.*, 469 F.3d 1257, 1280 (9th Cir. 2006).

oppressive the contract term, the less evidence of procedural unconscionability is required to come to the conclusion that the term is unenforceable, and vice versa."[94]

The procedural element of an unconscionable contract generally takes the form of a contract of adhesion. Under California law, a contract of adhesion is defined as "a standardized contract imposed upon the subscribing party without an opportunity to negotiate the terms."[95] If imposed and drafted by the party of superior bargaining strength, a contract of adhesion relegates to the subscribing party only the opportunity to adhere to the contract or reject it ("take it or leave it" approach).[96] Absent unusual circumstances, use of a contract of adhesion establishes a minimal degree of procedural unconscionability notwithstanding the availability of market alternatives.[97] End-user license agreements used by any of the major software vendors therefore satisfy the procedural element of unconscionability.

The substantive element of the unconscionability analysis focuses on overly harsh or one-sided results.[98] When applying these loose principles to any contract provision that authorizes the licensor of operating system software to disable the operating system, two aspects require further analysis.

The first aspect is the extent to which the law protects the owner's interest in ensuring that the functionality of the operating system running on his computer is not hindered. It is

---

[94] *Shroyer v. New Cingular Wireless Services, Inc.*, 498 F.3d 976, 982 (9th Cir. 2009) (quoting *Armendariz v. Foundation Health Psychcare Service, Inc.*, 99 Cal. Rpt. 2d 745, 767 et seq. (Cal. Sup. Ct. 2000)).

[95] *Id* at 983 (quoting *Nagrampa v. MailCoups, Inc.*, 469 F.3d 1257, 1281 (9th Cir. 2006)).

[96] *Id* at 982 (quoting *Discover Bank v. Superior Court of Los Angeles*, 30 Cal. Rptr. 3d 76, 85 (Cal. Sup. Ct. 2005)).

[97] *Id* at 985. *Cf Gatton v. T-Mobile USA, Inc.*, 61 Cal. Rptr. 3d 344, 352 (Cal. Ct. App. 2007) (holding that "a finding of a contract of adhesion is essentially a finding of procedural unconscionability" quoting *Flores v. Transamerica HomeFirst, Inc.*, 113 Cal. Rptr. 2d 376, 382 (Cal. Ct. App. 2001)).

[98] *Shroyer v. New Cingular Wireless Services, Inc.*, 498 F.3d 976, 982 (9th Cir. 2009) (quoting *Discover Bank v. Superior Court of Los Angeles*, 30 Cal. Rptr. 3d 76, 85 (Cal. Sup. Ct. 2005)).

important to emphasize that a disabled operating system renders the entire personal computer effectively useless—that is until a new operating system is installed. Furthermore it needs to be noted that, in the case of Windows 7, "the software will from time to time perform a validation check of the software" which "may be initiated by the software or Microsoft."[99] This means that the deactivation of one's system may occur at any time during the lifetime of the operating system.

The Computer Fraud and Abuse Act (CFAA)[100] prohibits "intentionally caus[ing] damage without authorization, to a protected computer" by "knowingly caus[ing] the transmission of a program, information, code, or command."[101] The CFAA also prohibits "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage."[102] The CFAA protects, *inter alia*, a computer "used in or affecting interstate or foreign commerce or communication"[103] which has been interpreted very broadly as covering any computer connected to the Internet.[104] The statutory damage threshold is $5,000 but the damages caused to different computers over a period of one year might be aggregated.[105] Disabling operating systems without permission might therefore constitute a federal crime.

---

[99] Microsoft Software License Terms for Windows 7 Professional, § 5(b), http://www.microsoft.com/about/legal/useterms/default.aspx.

[100] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2009).

[101] 18 U.S.C. § 1030(a)(5)(A).

[102] 18 U.S.C. § 1030(a)(5)(B).

[103] 18 U.S.C. § 1030(e)(2)(B).

[104] *See United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (holding that, with a connection to the Internet, the victim's computers were part of a system that is inexorably intertwined with interstate commerce and thus protected under 18 U.S.C. § 1030, irrespective of the victim organization's not-for-profit status). *Cf.* MARK G. MILONE, INFORMATION SECURITY LAW: CONTROL OF DIGITAL ASSETS § 9.01[1] (2009).

[105] 18 U.S.C. § 1030(c)(4)(A)(i)(I). *See* MARK G. MILONE, INFORMATION SECURITY LAW: CONTROL OF DIGITAL ASSETS § 9.01[2][c][ii] (2009).

Furthermore, California Penal Code § 502(c)(4) provides that any person who "[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network" is guilty of a public offense. California Penal Code § 502(c)(5) defines a similar public offense against any person who "[k]nowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network." Disabling an operating system without permission therefore constitutes a public offence under California Penal Code § 502(c)(5) and—should data be altered, damaged, deleted or destroyed in the process—also under § 502(c)(4).

The CFAA and California Penal Code § 502(c) express the value attributed not only to the confidentiality and integrity of data but also to the integrity and availability of (personal) computers in general.

The second aspect involves the conditions that must be met before the software vendor is authorized to deactivate the operating system. These conditions essentially determine the interest the software vendor might have in disabling the system. The example quoted above uses the following triggers: "the software is found to be counterfeit, improperly licensed, a non-genuine Windows product, or includ[ing] unauthorized changes." The last trigger seems particularly harsh given the fact that it also covers users who have paid their license fees and have only made modifications to the software that are covered by the fair use doctrine. The other triggers can be equated to the licensor's interest in receiving a license fee. However, irrespective of the particular trigger, the determination of whether all conditions are met ultimately rests with the software vendor. When compared to the traditional recourse provided by the legal system, this constitutes a form of "self-help"[106]

---

[106] *See* Mark Rasch, *Vista's EULA Product Activation Worries* (Nov. 20, 2006), http://www.securityfocus.com/columnists/423.

that reverses the burdens of the vendor and the user. It is now the user who has to initiate recourse to the courts if he is of the opinion that he did not violate the terms of the license.

This reversal of positions combined with the drastic effects of the disabling of an operating system should encourage a court to favour a finding of substantive unconscionability that tips the "sliding scale," and consequently rendering the contract provision unconscionable and unenforceable. However, it is to be expected that at least some courts will not follow this reasoning, leaving users with considerable legal uncertainty.

3.1.2. Enforceability Under EU Law

EU law on international jurisdiction and conflict of laws shall be discussed first before considering substantive EU contract law regarding the issue of enforceability.

As many end-user license agreements stipulate an exclusive U.S. jurisdiction, the issue of international jurisdiction is of particular importance. Art. 15 Brussels I Regulation[107] provides that the consumer-specific rules on jurisdiction apply if, *inter alia*, the contract has been concluded between a consumer[108] and a person who pursues commercial or professional activities in the Member State of the consumer's domicile or directs such activities to that Member State, and the contract falls within the scope of such activities. As most vendors of standard software direct their activities to all EU Member States by means of Internet advertising and as art. 15 Brussels I Regulation covers all types of contracts,[109] consumer-specific rules on jurisdiction apply. According to art. 16(1) Brussels I Regulation, a consumer may bring proceedings against the other party in the courts for the place where the consumer is domiciled. This is also the only jurisdiction in which

[107] Council Regulation 44/2001, 2001 O.J. (L 12) 1-23 (EC).

[108] Art. 2(b) of Council Directive 93/13 defines "consumer" as "any natural person who […] is acting for purposes which are outside his trade, business or profession."

[109] *See* Case C‑180/06, Ilsinger v. Dreschers, 2009 O.J. (C 153) 3, Recital 50 (holding that art. 15(1)(c) Brussels I Regulation covers, apart from certain transport, all contracts, whatever their purpose, if they have been concluded by a consumer with a professional and fall within the latter's commercial or professional activities).

proceedings may be brought against the consumer. Under art. 17 Brussels I Regulation, contractual derogation of these provisions that would transfer exclusive jurisdiction to the U.S. is not possible (unless the corresponding agreement is entered into after the dispute has arisen). Contract provisions that provide for exclusive jurisdiction in the U.S. are therefore of no legal consequence to EU consumers.

The national law applicable to a consumer contract is to be determined under art. 6 Rome I Regulation.[110] In general, a consumer contract is governed by the law of the country where the consumer has his habitual residence if, *inter alia*, the professional by any means, directs his commercial or professional activities to that country and the contract falls within the scope of these activities (art. 6(1)(b) Rome I Regulation). According to art. 6(2) Rome I Regulation, the parties may choose a different law. However, such a choice may not have the result of depriving the consumer of the protection afforded to him by *ius cogens*[111] which, in the absence of choice, would have been applicable. Depending on the consumer's habitual residence, a large body of substantive consumer protection law might be applicable, ultimately determining whether a provision that grants the software vendor the authority to hinder the functioning of the licensed software is enforceable or not.

Art. 3(1) of the Unfair Terms Directive,[112] which has been implemented by all Member States, is of particular importance in this regard. It provides that a contractual term in pre-formulated standard contract shall be regarded as unfair and not binding[113] on the consumer if, "contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer." Art. 3(1) Unfair Terms Directive therefore serves a similar purpose as the unconscionability doctrine in U.S. law.

---

[110] Parliament and Council Regulation 593/2008, 2008 O.J. (L 177) 6-16 (EC).

[111] Referred to by art. 6(2) Rome I Regulation as "provisions that cannot be derogated from by agreement by virtue of the law."

[112] Council Directive 93/13, 1993 O.J. (L 95) 29-34 (EEC).

[113] Art. 6(1) Unfair Terms Directive.

3.2. Authorizing Vendors to Automatically Download and Install "Updates"

Today, many end-user software license agreements contain a provision that grants the software vendor the authority to secretly initialize the download and installation of "updates."

For example, the Google Chrome Terms of Service, which apply to the executable code version of the Google Chrome browser state in § 11.1:

> The Software which you use may automatically download and install updates from time to time from Google. These updates are designed to improve, enhance and further develop the Services and may take the form of bug fixes, enhanced functions, new software modules *and completely new versions*. You agree to receive such updates (and permit Google to deliver these to you) as part of your use of the Services.[114] (emphasis added)

Another example is the license agreement and terms of use for Amazon Kindle, which state under § 4:

> Automatic Updates. In order to keep your Software up-to-date, Amazon may automatically provide your Device with updates/*upgrades* to the Software.[115] (emphasis added)

Similarly, the license agreement for Norton AntiVirus or Norton Internet Security states in § 2.A:

> In order to optimize the Software Symantec may, at its discretion and without notice, add, modify or remove features from the Software at any time.[116]

The warranty disclaimer and software license agreement for Adobe Reader 9.0 and Adobe Flash Player 10.0 provides in § 6.2:

---

[114] Google Chrome Terms of Service, as of Oct. 20, 2009, http://www.google.com/chrome/intl/en/eula_text.html (last visited Nov. 17, 2009).

[115] Amazon Kindle: License Agreement and Terms of Use, as of Feb. 9, 2009, http://www.amazon.com/gp/help/customer/display.html?nodeId=200144530 (last visited Nov. 17, 2009).

[116] Norton License Agreement for Norton AntiVirus 2010 or Norton Internet Security 2010, http://www.symantec.com/content/en/us/about/media/NAV-NIS_2010_EULA.pdf (last visited Nov. 17, 2009).

> Updating. You acknowledge and agree that the Software may cause your Computer to automatically connect to the Internet to check for updates [i.e. *upgrades*, *modified versions*, *updates*, *additions*, and copies of the foregoing, provided to you by Adobe at any time (see § 1)] that are available for automatic download to your Computer and to let Adobe know the Software is successfully installed.[117] (emphasis added)

Furthermore, Adobe's general Terms of Use that supposedly cover "[a]ny Software that is made available via the Site" given that "no license agreement accompanies the Software" provides in § 4.c:

> The Software may automatically download and install updates from Adobe from time to time. These updates are designed to improve, enhance and further develop the Services and may take the form of bug fixes, enhanced functions, new Software modules and *completely new versions*. You agree to receive such updates (and permit Adobe to deliver these to you with or without your knowledge) as part of your use of the Services.[118] (emphasis added)

3.2.1. Enforceability Under EU and U.S. Law

Contract provisions that supposedly authorize vendors to secretly initialize the download and installation of additional software, including security updates, should be seen in comparison to the contract provisions discussed in chapter 3.1 which supposedly authorize vendors to hinder the functioning of the entire computer.

Applying the unconscionability standard of California contract law,[119] it seems rather unlikely that a court would find the automatic download and installation of software to constitute a sufficiently one-sided result.

However, it should be noted that these contract provisions grant software vendors significant authority over a user's personal computer. This is particularly so because the

---

[117] Warranty Disclaimer and Software License Agreement for Adobe Reader 9.0 and Adobe Flash Player 10.0, http://www.adobe.com/products/eulas/pdfs/Reader_Player_AIR_WWEULA-Combined-20080204_1313 .pdf (last visited Nov. 17, 2009).

[118] Adobe Terms of Use, as of Oct. 15, 2008, http://www.adobe.com/misc/copyright.html (last visited Nov. 17, 2009).

[119] *See* chapter 3.1.1 *supra*.

authority to automatically download and install software does not only cover security updates but also feature updates (referred to in the above contract provisions as "completely new versions," "upgrades," or "additions").[120]

Even if the authority was limited to the installation of security updates (often referred to as "patches"), concerns for the security of a personal computer might still exist. A patch might turn out to be incompatible with certain third party software or might otherwise eliminate functionality on which the user relies. Ultimately a patch might therefore constitute a threat to the availability of certain services or applications. This is precisely why the patch management process of many corporations includes the testing of patches.[121] However, as owners of personal computers generally lack the motivation and resources to perform any testing of patches, a quick installation of available security patches is usually in the best interest of the security of a personal computer. Furthermore, an argument can be made that forcing users to install security updates increases the overall level of security.

However, no such arguments can be made for the automatic installation of feature updates.[122] Every new feature is necessarily accompanied by new security

---

[120] *Cf.* StopBadware.org's guidelines which state under II.A: "Application installations must be designed in a manner that ensures that an application is installed by end users in a knowing and willful manner. Applications which install deceptively are always considered badware. […] Automatic-updating is permissible, however, if the use of automatic-updates is clearly disclosed to the user during installation of the application and either is used only to make non-substantive updates to the application itself or seeks the user's consent before making any changes. Automatic-updates may not modify other software or be used to introduce substantive changes to the original application's functionality […]." *See* http://stopbadware.org/home/guidelines (last visited Nov. 17, 2009).

[121] *Cf.* Felicia M. Nicastro, *Security Patch Management: The Process in,* INFORMATION SECURITY MANAGEMENT HANDBOOK 185, 195 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007).

[122] For a strong argument of why patches should be kept separate from feature updates *see* ROSS ANDERSON ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET 5, 61 et seq., http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport.

vulnerabilities.[123] Whether or not the increased productivity provided by the new feature outweighs the newly introduced vulnerabilities, is a matter for risk-benefit analysis. If the user does not even want to use the new feature, installing it would therefore be contrary to the (security) interests of the user.

Furthermore, the automatic installation of additional software components, other than security updates, leads to a situation in which the owner of a personal computer has no idea what software is installed on his computer. This is problematic as vendors only seek the *authority* to install security and feature updates as they wish but do not accept any *responsibility* for installing the security updates. If security updates are not made available users might want to uninstall the software altogether. However, if users do not know that a certain software component is installed on their system, they cannot be expected to either manually install patches for it or uninstall the software. The automatic installation of new features without the specific knowledge of the owner of the personal computer therefore effectively reduces the level of security of the personal computer.

Although the effects on the security of a personal computer are significant, they are certainly not comparable to the disablement of the entire operating system. In the absence of substantive unconscionability, contract provisions granting the vendor the authority to secretly install updates would therefore have to be enforced under applicable contract law.

Whether a court of an EU Member State would find that such a contract provision "contrary to the requirement of good faith, […] causes a significant imbalance in the parties' rights and obligations arising under the contract" will largely depend on the Member State's implementation of art. 3(1) Unfair Terms Directive.

---

[123] Programmer and security expert Wietse Venema estimates that there is roughly one security bug per 1000 lines in his source code. *See* MARK G. GRAFF & KENNETH R. VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 5 (2003).

4. Effects on the Security of Personal Computers

Both EU and U.S. law lead to a disconnection of the concept of ownership and the concept of authorization to use a personal computer. The legal protection of technological protection measures leads to a significant de-authorization of the owner of a personal computer, while the enforcement of contract provisions granting software vendors the authority to secretly install additional software or hinder the functioning of the operating system result in the authorization of somebody other than the owner. The following chapters analyze how this disconnection affects the security of personal computers and IT security in general.

4.1. Ownership and the Burden of the Security Risk

Generally, the owner of a personal computer is the one person who suffers most should his personal computer become compromised. Malware threatens the confidentiality, integrity, and availability of the owner's stored data and communications. Additionally, malware is often not programmed well or incompatible to other malware running on the compromised system, ultimately threatening the functioning of the entire computer. It can therefore be said that the bearing of the security risks a personal computer is exposed to, is very much connected to the concept of ownership of the personal computer.

4.2. Reducing the Owner's Capability to Mitigate Security Risks

The de-authorization of the owner to use certain software components of his personal computer combined with the authorization of third parties effectively reduces the owner's capabilities to mitigate the security risks to which his computer is exposed.

All risks consist of the following components: an asset, vulnerabilities, safeguards, threats, and threat agents.[124] While threats (e.g. an exploit[125] for a newly discovered vulnerability)

---

[124] For further discussion of these risk components *see, e.g.*, DOUGLAS J. LANDOLL, THE SECURITY RISK ASSESSMENT HANDBOOK 30, 34, 36 (2006); SHON HARRIS, CISSP CERTIFICATION ALL-IN-ONE EXAM GUIDE 61 et seq. (4th ed. 2008).

and threat agents (e.g. a new criminal organization) are beyond the influence of an individual, the first three risk components (assets, vulnerabilities, safeguards) can generally be altered by the owner of a personal computer—that is if the law permits the owner to do so:

What and how much data (i.e. assets) is being stored on the computer is generally within the sole discretion of the owner of the computer. That of course is not the case where a technological protection measure prevents access to certain data. For example, temporary files are often kept longer than they are needed. Their existence creates the risk that their confidentiality might be compromised. The best risk mitigation strategy would be to remove the unneeded temporary files, thereby eliminating the risk. If however, technological protection measures prevent access to these files or even the entire file system (as does the iPhone),[126] removal of the files is not possible.[127]

Eliminating vulnerabilities in standard software usually involves the software vendor issuing a patch for the vulnerability. However, installing a patch is not the only way to eliminate a vulnerability. The software component that contains the vulnerability might also be uninstalled altogether by the owner. This of course requires that: (1) the owner is aware that the software is installed on his system, and (2) he has the authority to uninstall it. The first requirement is not fulfilled if vendors are granted and subsequently exercise the authority to secretly install new software. The second requirement cannot be met if the

---

[125] The term exploit refers to programs that automatically test a vulnerability and in most cases attempt to leverage that vulnerability by executing code. See JAMES C. FOSTER ET AL., BUFFER OVERFLOW ATTACKS 10 (2005).

[126] *See e.g.*, Jesus Diaz, iPhone File System Hacked, Custom Ringtones to Come Soon (July 10, 2007), http://gizmodo.com/276723/iphone-file-system-hacked-custom-ringtones-to-come-soon.

[127] *See* chapter 2.1.2.1 *supra* for a discussion on 17 U.S.C. § 1201(i) and its very limited scope.

software component itself (or the means to uninstall it) is protected by an access control measure whose circumvention is prohibited.[128]

The installation of additional safeguards allows the owner to prevent the exploitation of known vulnerabilities that cannot be eliminated (e.g. installing a personal firewall to prevent the exploitation of a vulnerability in a network-enabled service) or that are yet unknown (e.g. installing an intrusion detection system, in case the system is compromised). Furthermore, additional safeguards can compensate for other safeguards that prove ineffective to a certain threat.[129] However, installing additional safeguards requires a certain amount of access to one's own computer. If such access is prevented by a technological protection measure (e.g. by preventing the installation of applications that are not "authorized" by the vendor), no safeguards can be added to the system.

The disconnection of the concept of ownership and the concept of authorization to use a personal computer therefore drastically reduces the owner's capabilities to mitigate security risks.

4.3. Increasing the Possibility of Class Breaks by Promoting Homogeneity

Class breaks can be defined as "attacks that can break every instance of some feature in a security system."[130] This means that a certain kind of attack can be used to compromise not just one computer but an entire "class" of computers. Homogeneity of computer systems leads to larger "classes" that share the same security properties and are therefore vulnerable to the same kind of attack. By using a different word processor, browser, anti-virus software or personal firewall, owners of personal computers are able to achieve some level of diversity, irrespective of the operating system chosen. That diversity, however, is

---

[128] As uninstalling the entire software cannot be equated to "good faith testing, investigating, or correcting, a security flaw or vulnerability," the security exemption provided in 17 U.S.C. § 1201(j) does not apply.

[129] This principle is known as defense in depth. *See, e.g.,* STEPHEN NORTHCUTT ET AL., INSIDE NETWORK PERIMETER SECURITY 613 (2003).

[130] BRUCE SCHNEIER, BEYOND FEAR 93 (2006).

drastically reduced if the owner is not anymore able to choose freely between the different alternatives available on the market. Technological protection measures can be and are being used to allow the owner only the installation of third party applications specifically authorized by the software vendor. If the software vendor only authorizes one single application for each application category, effectively granting certain third parties a monopoly within his customer base,[131] diversity is eliminated altogether. This increases the probability of class breaks which, depending on the size of the homogenous customer base, can have a very high impact on the entire society.

4.4. Insufficient Incentives for Authorized Third Parties to Mitigate Risks

As discussed above, the disconnection of the concept of ownership and the concept of authorization to use a personal computer is problematic as it decreases the risk mitigation capabilities of the entity bearing most of the risk (the owner). This disconnection furthermore creates another problem: it transfers the risk mitigation capability to an entity (the software vendor) that has insufficient incentives to actually mitigate the risks.

Software vendors do not accept any liability for the security of their products or for a timely issuance of security patches, should vulnerabilities be discovered. Vendors therefore only bear the (security) risks related to their products to the extent that a public relations problem might arise. The security risks are therefore still primarily borne by the owners of the computers on which the product is installed. This leaves the vendors with insufficient incentives to use their risk mitigation capability effectively.[132]

---

[131] Companies selling (exclusive) access to their customer base is a long-standing practice. *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES 162 et seq. (1999).

[132] *Cf.* Bruce Schneier, *Make Vendors Liable for Bugs* (June 6, 2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/06/71032, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 147-9 (2008). *Cf. also* Ross J. Anderson, *Liability and Computer Security: Nine Principles in*, COMPUTER SECURITY – ESORICS 94 231-45 (Dieter Gollmann ed., 1994).

5. Conclusion

EU and U.S. law increasingly disconnect the concept of ownership and the concept of authorization to use personal computers. On the one hand, the prohibition of the circumvention of technological protection measures as provided for in 17 U.S.C. § 1201, in the EU Computer Programs Directive, and in the EU Copyright Directive, effectively de-authorizes the owner of a personal computer to use certain software components of his computer. On the other hand, the enforcement of contractual provisions that grant software vendors the authority to secretly download and install additional software or to even disable the licensed software, should the licensee be deemed in violation of the terms, effectively grant significant authority over a personal computer to somebody other than the owner, namely the software vendor. This disconnection has substantial negative effects on the security of personal computers. While the owner's capability to mitigate security risks is reduced, the vendor to whom the risk mitigation capability is transferred has insufficient incentives to use this capability. Furthermore, the de-authorization of owners leads to more homogenous systems, thereby increasing the possibility of class breaks.

Bibliography

ANDERSON, ROSS ET AL., SECURITY ECONOMICS AND THE INTERNAL MARKET, http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport

Anderson, Ross J., *Liability and Computer Security: Nine Principles in,* COMPUTER SECURITY – ESORICS 94 231-45 (Dieter Gollmann ed., 1994)

Broache, Anne & McCullagh, Declan, *Seeking changes to the DMCA*, CNET News.com, Apr. 3, 2006, http://www.zdnetasia.com/news/business/0,39044229,39347541,00.htm

Defeo, Mark, *Unlocking the iPhone: How Antitrust Law Can Save Consumers from the Inadequacies of Copyright Law* 49 B.C. L. REV. 1037 (2008)

Diaz, Jesus, iPhone File System Hacked, Custom Ringtones to Come Soon (July 10, 2007), http://gizmodo.com/276723/iphone-file-system-hacked-custom-ringtones-to-come-soon

DREIER, THOMAS & HUGENHOLTZ, BERNT, CONCISE EUROPEAN COPYRIGHT LAW (2006)

EILAM, ELDAD, REVERSING: SECRETS OF REVERSE ENGINEERING (2005)

Fallenböck, Markus, *On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions* (2002), http://www.ijclp.net/files/ijclp_web-doc_4-7-2003.pdf

FOSTER, JAMES C. ET AL., BUFFER OVERFLOW ATTACKS (2005)

GARFINKEL, SIMSON ET AL., PRACTICAL UNIX AND INTERNET SECURITY (3d ed. 2003)

Gasser, Urs & Girsberger, Michael, Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States (2004), http://cyber.law.harvard.edu/media/files/eucd.pdf

Ginsburg, Jane C., *Copyright Legislation for the "Digital Millennium,"* 23 COLUM.-VLA J.L. & ARTS 137 (1999)

Ginsburg, Jane C., *Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience*, Columbia Public Law Research Paper No. 5-93 (2005), http://ssrn.com/abstract=785945

Ginsburg, Jane C., The Pros and Cons of Strengthening Intellectual Property Protection: Technological Protection Measures and Section 1201 of the US Copyright Act (Feb. 1, 2007), http://ssrn.com/abstract=960724

GRAFF, MARK G. & VAN WYK, KENNETH R., SECURE CODING: PRINCIPLES AND PRACTICES (2003)

Grierson, Kevin, *Enforceability of "Clickwrap" or "Shrinkwrap" Agreements Common in Computer Software, Hardware, and Internet Transactions*, 106 A.L.R. 5th 309 (2003)

Hafner, Katie, *Altered iPhones Freeze Up*, N.Y. Times, Sept. 29, 2007, at C1, *available at* http://www.nytimes.com/2007/09/29/technology/29iphone.html.

Halderman, J. Alex & Felten, Edward W., Lessons from the Sony CD DRM Episode (Feb. 14, 2006), http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf.

HARRIS, SHON, CISSP CERTIFICATION ALL-IN-ONE EXAM GUIDE (4th ed. 2008)

Haubenreich, John, *The iPhone and the DMCA: Locking the Hands of Consumers*, 61 VAND. L. REV. 1507 (2008)

Heide, Thomas P., *Copyright, Contract and the Legal Protection of Technological Measures – Not "the Old Fashioned Way": Providing a Rationale to the "Copyright Exceptions Interface"*, http://ssrn.com/abstract=418000.

Heide, Thomas, *Copyright in the EU and U.S.: What "Access-Right"?*, 48 J. COPYRIGHT SOC'Y U.S.A. 363 (2001)

Herman, Bill D. & Gandy, Oscar, *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121 (2006), *available at* http://ssrn.com/abstract=844544

Hoover, J. Nicholas, Microsoft Updates Windows Without User Permission, Apologizes (Sept. 13, 2007), http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=201806263

INT'L ORG. FOR STANDARDIZATION, ISO/IEC 27000:2009 INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY (2009)

LANDOLL, DOUGLAS J., THE SECURITY RISK ASSESSMENT HANDBOOK (2006)

Lee, Timothy B., *Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act, Cato Institute Policy Analysis no. 564* (2006), http://www.cato.org/pubs/pas/pa564.pdf

LESSIG, LAWRENCE, FREE CULTURE (2004)

LITMAN, JESSICA, DIGITAL COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET (2001)

Lively, Rebecca K., *Microsoft Windows Vista: The Beginning or the End of End-User License Agreements as We Know Them?,* 39 ST. MARY'S L. J. 339 (2007)

LUCCHI, NICOLA, DIGITAL MEDIA & INTELLECTUAL PROPERTY (2006)

Maun, Timothy J., *iHack, Therefore iBrick: Cellular Contract Law, the Apple iPhone, and Apple's Extraordinary Remedy for Breach*, 2008 WIS. L. REV. 747

McReynolds, Kevin, *SDMCA Laws: Preemption and Constitutional Issues*. 12 UCLA ENT. L. REV. 63 (2004)

MILONE, MARK G., INFORMATION SECURITY LAW: CONTROL OF DIGITAL ASSETS (2009)

NAT'L INST. OF STANDARDS AND TECH., FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 200 - MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS (2006), http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUBLICATION 800-12 – AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK (1995), http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Netanel, Neil Weinstock, *Digital Rights Management: Temptations of the Walled Garden: Digital Rights Management and Mobile Phone Carriers*, 6 J. ON TELECOMM. & HIGH TECH. L. 77 (2007)

Nicastro, Felicia M., *Security Patch Management: The Process in*, INFORMATION SECURITY MANAGEMENT HANDBOOK 185 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007)

Nimmer, David, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673 (2000)

NIMMER, MELVILLE B. & NIMMER, DAVID, NIMMER ON COPYRIGHT (2002)

NORTHCUTT, STEPHEN ET AL., INSIDE NETWORK PERIMETER SECURITY (2003)

Rasch, Mark, *Vista's EULA Product Activation Worries* (Nov. 20, 2006), http://www.securityfocus.com/columnists/423.

Russinovich, Mark, More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home (Nov. 4, 2005), http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx

Russinovich, Mark, Sony, Rootkits and Digital Rights Management Gone Too Far (Oct. 31, 2005), http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx

Schneier, Bruce, Microsoft Updates Both XP and Vista Without User Permission or Notification (Sept. 17, 2007), http://www.schneier.com/blog/archives/2007/09/microsoft_updat.html

SCHNEIER, BRUCE, APPLIED CRYPTOGRAPHY (2d ed. 1996)

SCHNEIER, BRUCE, BEYOND FEAR (2006)

Schneier, Bruce, *Everyone Wants to "Own" Your PC* (May 4, 2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70802, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 161-3 (2008)

Schneier, Bruce, *Make Vendors Liable for Bugs* (June 6, 2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/06/71032, *reprinted in* BRUCE SCHNEIER, SCHNEIER ON SECURITY 147-9 (2008)

SHAPIRO, CARL & VARIAN, HAL R., INFORMATION RULES (1999)

Stone, Brad, *Amazon Erases Orwell Books From Kindle*, N.Y. Times, July 18, 2009, at B1, *available at* http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html

Tiller, James S., *Access Control*, in OFFICIAL (ISC)² GUIDE TO THE CISSP CBK 93 (Harold F. Tipton & Kevin Henry eds., 2007)

List of Abbreviations

A.L.R.	American Law Reports
aff’d	affirmed
B.C. L. Rev.	Boston College Law Review
Cardozo Arts & Ent. L.J.	Cardozo Arts & Entertainment Law Journal
cf.	confer
Colum.-VLA J.L. & Arts	Columbia-VLA Journal of Law & the Arts
e.g.	exempli gratia
ed.	editor/edition
eds.	editors
et seq.	et sequentes
i.e.	id est
id.	idem
J. Copyright Soc'y U.S.A.	Journal of the Copyright Society U.S.A.
J. on Telecomm. & High Tech. L.	Journal on Telecommunications & High Technology Law
St. Mary's L. J.	St. Mary's Law Journal
sub nom.	sub nomen
U. Pa. L. Rev.	University of Pennsylvania Law Review
UCLA Ent. L. Rev.	UCLA Entertainment Law Review
Vand. L. Rev.	Vanderbilt Law Review
Wis. L. Rev.	Wisconsin Law Review