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

Lukas Feiler

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation


Available at: http://digitalcommons.law.scu.edu/chtlj/vol27/iss1/4

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
SEPARATION OF OWNERSHIP AND THE AUTHORIZATION TO USE PERSONAL COMPUTERS: UNINTENDED EFFECTS OF EU AND US LAW ON IT SECURITY

Lukas Feiler†

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 US contract law and (para-)copyright law disconnect the concepts of ownership and authorization to use a personal computer and how that affects the security of personal computers.

† Lukas Feiler is Vice Director at the European Center for E-Commerce and Internet Law, Vienna. He is also a Fellow at the Stanford-Vienna Transatlantic Technology Law Forum (TTLF) and a Research Fellow at the Forum on Contemporary Europe (FCE). He studied law at the University of Vienna School of Law and the Santa Clara University School of Law and holds a Systems Security Certified Practitioner (SSCP®) certification from (ISC). Previously, he worked as a software developer and system administrator in Vienna, Leeds, and New York, held a teaching position for TCP/IP networking and web application development at the SAE Institute Vienna, and interned with the European Commission, DG Information Society & Media, Unit A.3 “Internet; Network and Information Security” in Brussels. He can be reached at lukas.feiler@lukasfeiler.com.
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 owners to install and uninstall any and all programs or even install an entirely different operating system.\(^1\)

However, this congruence of the concepts of ownership and authorization to use a personal computer 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 US contract law and (para-)copyright\(^2\) 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 US law disconnect the concepts of ownership and authorization to use personal computers:

Apple claimed that the circumvention of the SIM-lock or a “jailbreak”\(^3\) on its iPhone constituted a breach of contract and/or a violation of 17 U.S.C. § 1201(a) as it involved the circumvention of a technological measure that effectively controlled access to a work protected under 17 U.S.C.\(^4\). When Apple released their version 1.1.1

---


3. The term “jailbreak” 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, Comment, iHack, Therefore iBrick: Cellular Contract Law, the Apple iPhone, and Apple’s Extraordinary Remedy for Breach, 2008 Wis. L. Rev. 747, 751 (2008).

4. Responsive Comment of Apple Inc., In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, No. RM 2008-8, at 2 (US Copyright Office Feb. 2, 2009), http://www.copyright.gov/1201/2008/responses/apple-inc-31.pdf (claiming that a jailbreak would result in “in copyright infringement […] and breach of contract”). In 2007 Apple released the following statement: “Apple strongly discourages users from installing unauthorized unlocking programs on their iPhones. Users who make unauthorized modifications to the software on their iPhone violate their iPhone software license agreement.” See Mark Hachman, Update: Apple Issues Warning on iPhone Hacking,
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.\(^5\)

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.\(^6\)

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 be exploited by other malware.\(^7\)

The Microsoft License Terms for Windows 7 provides 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,”\(^8\) supposedly granting Microsoft the authority to remotely disable a user’s operating system.\(^9\)

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.\(^10\)

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 is addressed in Part 2 and the latter in Part 3. Part 4 will then assess

---


the effects of this disconnection on the security of personal computers.\textsuperscript{11}

2. DE-AUTHORIZING OWNERS

The acquisition of ownership of a personal computer, in principle, transfers full and exclusive authorization to the new owner to use that computer in any way or form. The discussion below describes various statutory and corresponding contractual means that 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.\textsuperscript{12} Technological protection measures were thought to be the "silver bullet" against copyright infringement committed by digital means.\textsuperscript{13} As no technological protection measure can be one hundred percent "secure," at least for a long-term period, copyright holders have successfully lobbied for a prohibition of the circumvention of technological protection measures.\textsuperscript{14}

2.1.1. Statutory Prohibitions

US as well as EU law provides statutory prohibitions regarding the circumvention of technological protection measures. These prohibitions will be discussed in Part 2.1.1.2 and 2.1.1.3 respectively.

\textsuperscript{11} The idea that a disconnection between ownership and authorization would undermine security was first articulated by information security expert Bruce Schneier. See Bruce Schneier, \textit{Everyone Wants to "Own" Your PC}, WIRED, May 4, 2006, http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70802, reprinted in BRUCE SCHNEIER, SCHNEIER ON SECURITY 161-63 (2008).

\textsuperscript{12} See CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 81-102 (1999).

\textsuperscript{13} See, e.g., LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 157 (2004).

\textsuperscript{14} 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, \textit{Temptations of the Walled Garden: Digital Rights Management and Mobile Phone Carriers}, 6 J. ON TELECOMM. & HIGH TECH. L. 77, 77 (2007).
Both legislative regimes have to be seen in the context of international law which is briefly discussed first.

2.1.1.1. International Background

Article 11 of the WIPO Copyright Treaty (WCT)\(^{15}\) 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 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.”\(^{16}\)

2.1.1.2. 17 U.S.C. § 1201

The Digital Millennium Copyright Act (DMCA)\(^{17}\) was enacted on October 28, 1998, *inter alia*, to implement the WCT in the United States. The DMCA specifically introduced 17 U.S.C. § 1201 to implement article 11 of the WCT.\(^{18}\)

Section 1201 contains three principal prohibitions regarding the circumvention of technological protection measures:\(^{19}\)

Section 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”).\(^{20}\) 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

---

15. See WIPO Copyright Treaty, December 20, 1996, S. Treaty Doc. No. 105-17, at 10 (1997); see also Council Decision 2000/278, 2000 O.J. (L 89) 6 (EC) (approving the WIPO Copyright Treaty on behalf of the European Community with regard to matters within its competence).


19. 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).

the copyright owner."21

Section 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 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.22

Section 1201(b) contains the same prohibition as the aforementioned § 1201(a)(2) but instead of referring to an access control measure 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").23

Section 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)).24 Second, it distinguishes access control measures from copy control measures: the prohibition on circumvention only applies to access control measures (§ 1201(a)(1)), whereas the prohibition on trafficking circumvention technology applies to access control measures and copy control measures (§ 1201(a)(2) and § 1201(b)).25

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).26

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 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.

In Lexmark Int'l, Inc. v Static Control Components, Inc., the District Court stated that the term "access" should be given its ordinary and customary meaning, which is the "ability to enter, to obtain, or to make use of." The Court held that an authentication protocol 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.

28. See, e.g., NAT'L INST. OF STANDARDS AND TECH., AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK 195 (1995), available at 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., MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS 2 (2006), available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (stating with regard to access control that "[e]nganizations 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)); INT'L ORG. FOR STANDARDIZATION, ISO/IEC 27000: INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – OVERVIEW AND VOCABULARY 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).
30. 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 (Phil Sutherland ed., 2d ed. 1996).
under this title" is otherwise accessible.\textsuperscript{33} As the object code of the printer software was accessible 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.\textsuperscript{34} The court therefore effectively imposed the requirement that access control measures must (at least) control the "ability to [] obtain a copy of the work."\textsuperscript{35} A measure that only limits the ability to modify or execute a program would therefore fall outside this definition.\textsuperscript{36}

This is in line with other widely noted cases, such as RealNetworks, Inc. v. Streambox, Inc. In 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).\textsuperscript{37} 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."\textsuperscript{38}

The second issue to be addressed is that of "effective" access control. Section 1201(a) only covers technological measures that "effectively" control access to a protected work.\textsuperscript{39} The statute provides that an access control measure is "effective" if the measure "in the ordinary course of its operation," requires the authority of the copyright owner, to gain access to the work.\textsuperscript{40} As a result, a rather low

\textsuperscript{33.} Id. at 547.
\textsuperscript{34.} Id. at 546-47.
\textsuperscript{35.} Id. at 547.
\textsuperscript{36.} 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." See SIMSON GARFINKEL ET AL., PRACTICAL UNIX AND INTERNET SECURITY 131 (Deborah Russell ed., 3d ed. 2003).
\textsuperscript{38.} 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).
standard is used by most courts.41

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".42 Somebody who has the authority to circumvent would therefore not violate § 1201(a)(1).43

Some commentators suggest that authority to access the work is sufficient to evade a violation of § 1201(a)(1).44 In Chamberlain Group, Inc. v. Skylink Technologies, Inc., the Federal Circuit seems to have gone in that direction.45 At issue in the case 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.46 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.47 The court sided with the defendant, holding that the plaintiff's customers did not violate access to a work for both § 1201(a)(1) and § 1201(a)(2)); see also 17 U.S.C. § 1201(b)(2)(B) (2006) (noting that § 1201(b) uses a similar definition of effectiveness: a copy control measure is "effective" if "the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title").

41. 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, 531-33 (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 party other than the defendant did not constitute a "circumvention" targeted by 17 U.S.C. § 1201(a). But cf. Agfa Monotype Corp. v. Adobe Sys., 404 F. Supp. 2d 1030, 1036 (N.D. Ill. 2005) (holding that embedded "bits" which encode permissions do not by themselves constitute an "effective" technological protection measure).


43. Id. (emphasis added).

44. See Markus Fallenböck, On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions, 7 INT'l J. COMM. L. & POL'Y 1, 19 (2002), available at http://www.ijclp.net/files/ijclp_web_doc_4-7-2003.pdf (framing authority to access a work 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).


46. See id. at 1183-85.

47. See id. at 1203.
§ 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).

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.

The different readings of the authorization requirement of § 1201(a) by the Federal Circuit in Chamberlain Group, Inc. v. Skylink Technologies, Inc. and by the 2nd Circuit in Universal City Studios, Inc. v. Corley are particularly significant with regard to software installed on a personal computer: users are typically authorized to use installed software but not to circumvent any technological measures protecting it. If the former type of authorization was deemed sufficient by the courts with regard to personal computer software, many circumventions would escape § 1201(a) liability. Such a judicial position is, however, for the reasons discussed supra, rather unlikely.

48. See id. at 1204 (holding that Chamberlain "has failed to show [...] the requisite lack of authorization").
49. See id. (holding that Chamberlain's customers are immune from § 1201(a)(1) circumvention liability because "[t]he Copyright Act authorized Chamberlain's customers to use the copy of Chamberlain's copyrighted software embedded in the [garage door openers] that they purchased").
50. Id.
51. See 17 U.S.C. § 1201(a)(3)(A) (2006) (providing 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").
52. See Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001).
53. See id.
2.1.1.3. The EU Computer Programs Directive and the EU Copyright Directive

European Union (EU) law provides three distinct statutory schemes for technological protection measures: the EU Computer Programs Directive (hereinafter referred to as EUCPD), the EU Copyright Directive (hereinafter referred to as EUCD), and the EU Conditional Access Directive. 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.

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. 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, Article 6 of the EUCD provides a distinction between the act of circumvention itself (Article 6(1)) and trafficking in circumvention technology (Article 6(2)). Article 6(1) of the EUCD obligates EU Member States to provide adequate legal protection against circumvention while Article 6(2) obligates Member States to “provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes” of certain circumvention tools.

---

54. 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 as the EC. See Consolidated Version of the Treaty on European Union, art. 1, Dec. 13, 2007, 2010 O.J. 83-16.


59. Pursuant to Article 6(1) of the EUCD, “adequate legal protection” has to be provided against circumvention while Article 6(2) obligates Member States to “provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes” of certain circumvention tools. Parliament and Council Directive 2001/29, art. 6(2), 2001 O.J. (L 167) 10-19 (EC).
protection against the circumvention of any "effective technological measures," which is carried out "with knowledge, or reasonable grounds to know," 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 do so knowingly or at least negligently ("with reasonable grounds to know"). The term "technological measures," as it is used in Article 6(1) of the EUCD, is defined in Article 6(3) of the 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 subject matter, which are not authorized by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of the EU Database Directive.

According to Article 6(3) of the 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".

This wording indicates that Article 6(1) of the EUCD prohibits the circumvention of both access control measures and copy control measures. The circumvention prohibition of Article 6(1) of the 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, not copy control measures. As Article 6(1) of the EUCD covers both types of measures, their distinction, which is important under 17 U.S.C. § 1201, is almost irrelevant here.

Article 6(2) of the EUCD prohibits the trafficking of
circumvention technology.\textsuperscript{65} 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.\textsuperscript{66} The substance and even the wording of Article 6(2) of the EUCD is almost identical to that of 17 U.S.C. § 1201(a)(2) (regarding access control measures)\textsuperscript{67} and 17 U.S.C. § 1201(b) (regarding copy control measures).\textsuperscript{68}

This section will discuss the EUCPD which, according to Recital 50 EUCD, applies exclusively to “technological measures used in connection with computer programs.”\textsuperscript{69} Article 7(1)(c) of the 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 unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.”\textsuperscript{70}

Article 7(1)(c) of the EUCPD is far more narrow than Article 6 of the EUCD or 17 U.S.C. § 1201. First, it only prohibits “acts of putting into circulation” and “the possession for commercial purposes.”\textsuperscript{71} The act of circumvention itself is therefore not prohibited.

Second, a plain reading of Article 7(1)(c) of the EUCPD only prohibits putting “means” into circulation or possessing “means.”\textsuperscript{72} Unlike Article 6(2) of the EUCD or 17 U.S.C. § 1201, providing services for the purpose of facilitating circumvention is not

\begin{footnotes}
\footnote{66. Id.}
\footnote{71. Id.}
\footnote{72. See id.}
\end{footnotes}
prohibited. 73

Third, it only covers "means" where the "sole intended purpose of which is to facilitate the unauthorized removal or circumvention" of a technical protection measure. 74 In contrast to Article 6(2) of the EUCD and 17 U.S.C. § 1201, Article 7(1)(c) of the EUCPD does not cover technology that has only limited commercially significant purpose, or use other than to circumvent, 75 or that is promoted, advertised or marketed for the purpose of circumvention. 76

Finally, Article 7(1)(c) of the EUCPD only protects "technical device[s] which may have been applied to protect a computer program." 77 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). 78 Under the principle of uniform interpretation, 79 the different language versions must be given a uniform interpretation. As there is a divergence between the versions, Article 7(1)(c) of the 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 17 U.S.C. § 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." 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.

On the other hand, in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.* the Federal Circuit rejected a reading of § 1201(a) 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 grants to the public. Such a reading would be contrary to § 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." 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

---

80. 17 U.S.C. § 1201(c)(1). *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).
82. *Id.*
The opposing conclusions drawn by courts from §1201(c)(1) is indeed remarkable and leaves users with a significant legal risk should they decide to rely on a fair use defense. Section 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.

Title 17 U.S.C. §1201 codifies various exemptions to the prohibitions of §1201: exemption for nonprofit libraries, archives, and educational institutions (§1201(d)); law enforcement, intelligence, and other government activities (§1201(e)); reverse engineering (§1201(f)); encryption research (§1201(g)); exceptions regarding minors (§1201(h)); protection of personally identifying information (§1201(i)); and security testing (§1201(j)). 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.

Section 1201(f) provides exemptions for reverse engineering that is performed for the purpose of obtaining interoperability information. According to §1201(f)(1), it does not constitute a

86. 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 Chamberlain, 381 F.3d at 1196; Chamberlain, 381 F.3d at 1203; Corley, 273 F.3d at 443, n.13; H.R. REP. No. 105-551, pt. 2, at 25, 26 (1998).
87. 17 U.S.C. §1201(d) (this section only provides an exemption for 17 U.S.C. §1201(a)(1)).
88. 17 U.S.C. §1201(e) (this section provides exemptions for 17 U.S.C. §§1201(a)(1), 1201(a)(2) and 1201(b)).
89. 17 U.S.C. §1201(f) (this section provides exemptions for 17 U.S.C. §§1201(a)(1), 1201(a)(2) and 1201(b)).
90. 17 U.S.C. §1201(g) (this section provides an exemption for 17 U.S.C. §1201(a)(1) and a narrow exemption for 17 U.S.C. §1201(a)(2)).
91. 17 U.S.C. §1201(h) (this section provides an exemption for 17 U.S.C. §§1201(a)(1) and 1201(a)(2)).
92. 17 U.S.C. §1201(i) (this section only provides an exemption for 17 U.S.C. §1201(a)(1)).
93. 17 U.S.C. §1201(j) (this section provides an exemption for 17 U.S.C. §§1201(a)(1) and (2)).
95. Reverse engineering can be defined as the process of discovering technological information about computer hardware or software by examining it. Cf. ELDAD EILAM,
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 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. It does not allow access control measures to be circumvented for the purpose of installing (as opposed to developing) interoperable software. Section 1201(f) therefore has minimal effect on the authority to use one's own personal computer.

Section 1201(g) provides an exemption from § 1201(a)(1) and (a)(2) 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.

Section 1201(i) creates an exemption from § 1201(a)(1)—but not

---

101. The exemption from 17 U.S.C. § 1201(a)(2) only applies regarding "another person with whom [the researcher] is working collaboratively." 17 U.S.C. § 1201(g)(4)(B). It is therefore a very limited one.
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 the access control measure (or the work it protects) contains the "capability of collecting or disseminating personally identifying information reflecting the online activities" 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). 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., writing a document using a locally installed word processor instead of Google Docs) falls outside the scope of § 1201(i).

107. The statute states that a circumvention is only permissible if the collection or dissemination of PII is performed "without providing conspicuous notice [...] , and without providing [...] the capability to prevent or restrict such collection or dissemination," 17 U.S.C. § 1201(i)(1)(B) (emphasis added). This strongly suggests that both conspicuous notice and a prevention/restriction capability must be absent in order for the exception to apply. Accordingly, the presence of either of the conditions eliminates the exemption. See JAY DRATLER, CYBERLAW: INTELLECTUAL PROPERTY IN THE DIGITAL MILLENNIUM § 3.03[4], n.129 (Rev. Ed. 2009) (2000). The legislative history is inconsistent on the issue of whether conspicuous notice alone eliminates the exemption: H.R. Rep. No. 105-551, pt. 2, at 45 (1998) (hereinafter Commerce Rep.) states that § 1201(i) was "designed to ensure that if a copyright owner conspicuously discloses [the] data gathering capability, and the consumer is given the capability to curtail or prohibit effectively any such gathering or dissemination of personal information, then the consumer could not legally circumvent the technological protection measure" (emphasis added). Contrary to what is suggested by the statute, this language indicates that a consumer could still claim the exemption if only one of the two conditions (e.g. conspicuous notice) is fulfilled. In its background section, the Commerce Rep. emphasizes the problem of "surreptitiously gather[ing] consumers' personal information." Id. at 27 (emphasis added). However, this problem is perfectly addressed by conspicuous notice alone. But see 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.05[B][1] (Matthew Bender Rev. Ed. 2010) (1963) (stating that for the exemption to be eliminated, conspicuous notice "and" a prevention/restriction capability must be present).
108. Id.
Section 1201(j) provides an exemption from § 1201(a)(1) and (2) for "security testing."\textsuperscript{109} "Security testing" 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."\textsuperscript{110} It is important to recognize that this definition of security testing very much centers on the term "vulnerability," which is used synonymously with "security flaw."\textsuperscript{111} 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. Section 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."\textsuperscript{112} 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.\textsuperscript{113} Section 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.\textsuperscript{114}

In addition to the exemptions codified in § 1201(d) to (j), subsections 1201(a)(1)(B) and (C) provide a more general exemption

\textsuperscript{110} 17 U.S.C. § 1201(j)(1).
\textsuperscript{111} Id.
\textsuperscript{112} Id.
\textsuperscript{113} 17 U.S.C. § 1201(j)(3).
\textsuperscript{114} 17 U.S.C. § 1201(j)(3)(B). 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 17 U.S.C. § 1201, including a violation of privacy or breach of security pursuant to 17 U.S.C. § 1201(j)(3)(B). Id.
and an associated rulemaking procedure. The prohibition of § 1201(a)(1) "shall not apply 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 three-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.\textsuperscript{115} Identification of those "classes of works" is left up to the Librarian of Congress pursuant to § 1201(a)(1)(B); every three years, the Librarian shall make the determination in a rulemaking proceeding.\textsuperscript{116} 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) such other factors as the Librarian considers appropriate.\textsuperscript{117}

The Librarian of Congress’ determination, currently in force, was published on July 27, 2010.\textsuperscript{118} It superseded the 2006 determination\textsuperscript{119} which was extended by the Librarian on an interim basis on Oct. 27 2009.\textsuperscript{120} The new determination defines six classes of copyrighted works, of which only three are relevant here:\textsuperscript{121}


\textsuperscript{117} 17 U.S.C. § 1201 (a)(1)(A).

\textsuperscript{118} Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. § 201.40(b) (2010). It became effective on the date of its publication. See 75 Fed. Reg. 43826.


\textsuperscript{120} 74 Fed. Reg. 55138-9 (Oct. 27, 2009).

\textsuperscript{121} 37 C.F.R. § 201.40(b). The three other classes deal with motion pictures on DVDs that are protected by the Content Scrambling System (CSS) when circumvention is
1. “Computer programs that enable wireless telephone handsets to execute software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset.”¹²²

2. “Computer programs in the form of firmware or software that enable used wireless telephone handsets to connect to a wireless telecommunications network, when circumvention is initiated by the owner of the copy of the computer program solely in order to connect to a wireless telecommunications network and access to the network is authorized by the operator of the network.”¹²³

3. “Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works, when circumvention is accomplished solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities.” In the case of security testing, “the derived information has to be used primarily to promote the security of the owner or operator of a computer” and must not be used or maintained in a manner that facilitates copyright infringement or a violation of applicable law.¹²⁴

The first class was newly introduced by the 2010 determination and grants users the authority to “jailbreak” their smartphones—that is to circumvent technological measures that would otherwise prevent third party software applications from being installed and run on smartphones, in particular the iPhone¹²⁵ (hereinafter referred to as the iPhone Jailbreaking Exemption).¹²⁶ The iPhone Jailbreaking Exemption was proposed by the Electronic Frontier Foundation (EFF)

accomplished in order to incorporate short portions of motion pictures into new works for the purpose of criticism or comment, and where the circumvention is necessary for the purpose of certain educational uses, documentary filmmaking, or noncommercial videos (37 C.F.R. § 201.40(b)(1) (2010)); computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete (37 C.F.R. § 201.40(b)(5) (2010)); 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 that render the text into a specialized format (37 C.F.R. § 201.40(b)(6) (2010)).

¹²⁵ See 75. Fed. Reg. 43825, 43828 (July 27, 2010) (noting that “[t]he factual record with respect to this proposed class focused primarily on Apple’s iPhone, although there are allegations in the record involving other mobile phone manufacturers as well”).
to address growing concerns over the iPhone’s closed architecture which made it impossible for an owner of an iPhone—without jailbreaking the device—to install and use third party applications on the device not previously approved for distribution by Apple through its App Store.127 It has to be emphasized that the iPhone Jailbreaking Exemption applies exclusively to smartphones, but not to other mobile devices such as an iPad, a laptop, or a traditional PC.

The second class affords owners of a used cell phone the authority to use the phone—irrespective of any access controls—for the limited purpose of connecting to a different carrier’s network (referred to hereafter as the SIM Lock Exemption).128 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 § 1201(a).129 The first court applying the exemption after it was introduced in 2006 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 telecommunications network and therefore was outside of the exemption’s scope.130

The third class concerns video games accessible on personal computers if the circumvention is accomplished solely for the purpose of “good faith testing for, investigating, or correcting security flaws or

127. See id.

128. This exemption is based on an almost identical exemption contained in the 2006 determination. Cf. 71 Fed. Reg. 68472, 68476 (Nov. 27, 2006). However, the new determination limited the exemption to “used” cell phones in order not to cover “bulk resellers” who purchase new mobile phones at subsidized prices and, without actually using them on the networks of the carriers who market those handsets, resell them for profit. See 75 Fed. Reg. 43825, 43831 (July 27, 2010).


130. TracFone Wireless, Inc. v. Dixon, 475 F. Supp. 2d 1236, 1238 (M.D. Fla. 2007). Note that this decision applied the SIM lock exemption as defined in the 2006 determination. Cf. 71 Fed. Reg. 68472, 68476 (Nov. 27, 2006). However, its holding remains applicable for the new SIM lock exemption defined in the 2010 determination. 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 (2008).
vulnerabilities” (hereinafter referred to as the Video Game Vulnerability Exemption).\textsuperscript{131} Testing for vulnerabilities typically involves using the software in ways not expected by the developers (e.g., providing the software with overlong input data).\textsuperscript{132} The investigation of a vulnerability will require some degree of reverse engineering in order to find the particular part of the software that creates the vulnerability.\textsuperscript{133} Correcting the vulnerability might require modifications of the software.\textsuperscript{134}

This class is based on a class contained in the 2006 determination which covered sound recordings distributed on a CD if protected by technological measures that “create or exploit security flaws or vulnerabilities that compromise the security of personal computers”\textsuperscript{135} (hereinafter referred to as the Sony BMG Exemption). The Sony BMG Exemption had been created in 2006 in response to a digital rights management system contained on music CDs distributed by Sony BMG Music Entertainment.\textsuperscript{136} Upon insertion of those music CDs into a computer’s CD drive, a spyware and a rootkit were installed.\textsuperscript{137}

\begin{enumerate}
\item[132.] Cf. e.g., BARTON P. MILLER, AN EMPIRICAL STUDY OF THE RELIABILITY OF UNIX UTILITIES, 32 (Communications of the ACM) (Dec. 1990) (report of an early study showing how UNIX utilities behave when given unexpected input).
\item[133.] For example, if a video game crashes when a username is entered that has more than a certain amount of characters, it is likely that the video game software, somewhere in the code, copies the username provided as input into a buffer that is too small to store the entire input. This leads to a so-called “buffer overflow.” To correct this vulnerability, it has to be investigated where in the code the buffer is being written to. Cf. JAMES C. FOSTER ET AL., BUFFER OVERFLOW ATTACKS 161 (2005).
\item[134.] If the source code is not available, the binary code of the video game might have to be modified.
\item[135.] 71 Fed. Reg. 68472, 68477 (Nov. 27, 2006).
\item[136.] See 71 Fed. Reg. 68477 n. 6 (Nov. 27, 2006). For a detailed rationale see 37 C.F.R. § 201.40(b)(6).
\item[137.] Id. This “automatic” installation was only performed if Microsoft Windows’ AutoRun feature was enabled, which it is by default. For a detailed technical description, see MARK RUSINOVICH, 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 RUSINOVICH, MORE ON SONY: DANGEROUS DECLOAKING PATCH, EULAS AND PHONING HOME (Nov. 4, 2005), http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-
It might have been argued that §1201(j) already provided an exemption for cases covered by the Video Game Vulnerability Exemption or for cases previously covered by the Sony BMG Exemption, but in his 2006 recommendation to the Librarian of Congress, the Register of Copyrights stated that “it is not clear whether that provision extends to such conduct.” The ambiguity of §1201(j) is demonstrated by 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.

However, in its 2010 determination, the Librarian of Congress only included an exemption for video game vulnerabilities but no exemption with regard to sound recordings because no evidence was presented in the proceeding that “the prohibition on circumvention is adversely affecting or is likely, in the next three years, to adversely affect the ability to engage in noninfringing uses of sound recordings.”

The final issue to discuss with regard to statutory exemptions is whether they can be derogated from by contractual arrangement. 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 US Constitution. Title 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


141. US 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.”
106..."142 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 § 106.143

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"144 (field preemptions).145 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 legal requirement that a circumvention must "not constitute [...] a violation of applicable law"—which might be construed to include contract law.146 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)(D)), the encryption research exemption (§ 1201(g)(2)(D)), the reverse engineering exemption (§ 1201(f)(3)), and the video game vulnerability exemption (37 C.F.R. § 201.40(b)(4)).147

In summary, the exemptions discussed supra only mitigate § 1201’s effects to a rather small extent. In particular, none allow the owner of a personal computer to circumvent technological protection measures for the purpose of increasing the computer’s security.

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 from its general prohibitions regarding the circumvention of protection measures, whereas not a single exemption is available through the EUCPD.148 Recital 48 of the

145. 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 preemption see Kevin McReynolds, SDMCA Laws: Preemption and Constitutional Issues, 12 UCLA ENT. L. REV. 63, 81 (2004).
EUCD states that the legal protection of technological measures "should not hinder research into cryptography."\textsuperscript{149} If a circumvention of technological measures is performed for the purpose of cryptography research, the prohibitions of Article 6 of the EUCD do not apply. However, it should be noted that cryptography is traditionally defined as "the art and science of keeping messages secure"\textsuperscript{150} as opposed to the art and science of breaking encrypted messages (referred to as "cryptanalysis").\textsuperscript{151}

Furthermore, regarding the prohibition of circumventions performed for the purpose of making noninfringing uses, the EUCD implements a remarkable approach.\textsuperscript{152} Article 6(4) of the EUCD provides that only in the absence of voluntary measures taken by rightholders,\textsuperscript{153} shall Member States take appropriate actions to ensure that noninfringing\textsuperscript{154} uses are possible.\textsuperscript{155} This provision therefore prohibits all circumventions by default (whether or not performed to make noninfringing uses) and leaves much latitude and discretion to Member States for regulating technical protection measures with


\textsuperscript{150.} BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 1 (2d ed. 1996).

\textsuperscript{151.} Cryptography and cryptanalysis are collectively referred to as cryptology; see id.


\textsuperscript{154.} "Noninfringing" 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)." Id.

respect to the uses they must permit. 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 permit certain noninfringing uses. A circumvention of technological protection measures is therefore categorically prohibited under Article 6 of the 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

Title 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 extent to which the prohibition of the circumvention of a specific technological protection measure results in a de-authorization has to be determined on a case-by-case basis.


157. See NICOLA LUCCHI, DIGITAL MEDIA & INTELLECTUAL PROPERTY 58 (2006). For how the EUCD was transposed in the EU Member States see, e.g., URS GASSE & MICHAEL GIRSBERGER, TRANSPOSING THE COPYRIGHT DIRECTIVE: LEGAL PROTECTION OF TECHNOLOGICAL MEASURES IN EU-MEMBER STATES 12-17 (Berkman Center for Internet & Society at Harvard Law School) (2004), http://cyber.law.harvard.edu/media/files/eucd.pdf.


160. See GASSER, supra note 157, at 17.

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, to what else does the technological protection measure effectively prevent access? 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 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 because the owner of the computer would be de-authorized to directly access any and all files in the file system (of which there may be thousands) only to protect a single file. However, proportionality to the protected work is not a requirement under 17 U.S.C. § 1201, or the EUCP. By contrast Recital 48 of the EUCD does state that the legal protection of technological protection measures "should respect proportionality." This is not sufficient to exempt all "overly protective" technological protection measures from the legal protection afforded by the plain language of Article 6(1) of the EUCD. Recital 48 of the EUCD makes clear that any national law adopted pursuant to Article 6(1) only has to be proportional in the sense that it also specifically refers in the same sentence to "should not prohibit those devices or activities which have a commercially significant purpose or use other than to


circumvent the technical protection.” In light of Recital 48, the comprehensive meaning of Article 6(1) is therefore to be understood as demanding proportionality with regard to a circumvention technology’s alternative use(s).

Ultimately, 17 U.S.C. § 1201, the EUCD, and the EUCPD give copyright holders the legal power to create closed systems and to protect these systems from any interference by the owner of the personal computer. As discussed infra, 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 infra in part 4.3), possibly compromising entire product lines.

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[...].\textsuperscript{167}

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

3.1.1. Enforceability Under US Law

Due to the economic importance of the State of California, the following discussion will focus exclusively on California state law.\textsuperscript{168} 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 are not accessible to the user before opening the package. The user is only left with the choice of either accepting the terms by using the software or rejecting them by returning the package to the store. In \textit{ProCD v. Zeidenberg}, the 7th Circuit famously held that shrink-wrap contracts are indeed enforceable.\textsuperscript{169} However, as shrink-wrap contracts simply employ a different method of contract formation, they are still vulnerable to general contract defenses, in particular, unconscionability.\textsuperscript{170}

Click-wrap contracts are very similar to shrink-wrap contracts in the sense that the licensee can either “take-it” (and enter the contract) “or-leave-it” (and not enter the contract).\textsuperscript{171} The only difference is that the click-wrap terms are not printed on paper but are displayed on a computer screen. The user can either accept the terms by clicking on an acceptance button or reject the terms by aborting the installation. Today, almost all standard software products employ click-wrap contracts.

\begin{itemize}
    \item 169. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).
    \item 170. \textit{Cf.} MAUN, supra note 3, at 764.
\end{itemize}
contracts. Like shrink-wrap contracts, click-wrap contracts are enforceable but subject to defenses such as unconscionability.  

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.” A “sliding scale” is to be applied so that “the more substantively 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.”

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.” 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). Absent unusual circumstances, use of a contract of adhesion establishes a minimal degree of procedural unconscionability notwithstanding the availability of market alternatives.

End-user license agreements used by any of the major software vendors therefore satisfy the procedural element of unconscionability.

172. See Kevin Grierson, Enforceability of “Clickwrap” or “Shrinkwrap” Agreements Common in Computer Software, Hardware, and Internet Transactions, 106 A.L.R. 5th 309 § 3[a], [b], [h] (2003). See Maun, supra note 3, at 765.


See also Davis v. O’Melveny & Myers, 485 F.3d 1066, 1072 (9th Cir. 2007).

174. 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)).

175. Id. at 981-82 (9th Cir. 2009) (quoting Armendariz v. Found. Health Psychcare Serv., Inc., 6 P.3d 669, 690 (Cal. 2000)).

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

177. Id. at 982 (quoting Discover Bank v. Superior Court of Los Angeles, 30 Cal.4th 148, 160 (Cal. Sup. Ct. 2005)).

The substantive element of the unconscionability analysis focuses on overly harsh or one-sided results. 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 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 Professional, “the software will from time to time perform a validation check of the software” which “may be initiated by the software or Microsoft.” 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) prohibits “intentionally caus[ing] damage without authorization, to a protected computer” by “knowingly caus[ing] the transmission of a program, information, code, or command.” The CFAA also prohibits “intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage.” The CFAA protects, inter alia, a computer “used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.” The statutory damage threshold is $5,000, but the damages

184. 18 U.S.C. § 1030(e)(2)(B). As regards computers located in the U.S., “used in or affecting interstate […] commerce” has been interpreted very broadly, effectively covering any computer connected to the Internet. 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 that were located in Missouri 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. also MARK G. MILONE, INFORMATION SECURITY LAW: CONTROL OF DIGITAL ASSETS § 9.01[1] (2009).
caused to different computers over a period of one year might be aggregated.\textsuperscript{185} Disabling operating systems without permission might therefore constitute a federal crime in the United States.

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.\textsuperscript{186} 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.”\textsuperscript{187} Disabling an operating system without permission therefore constitutes a public offense under California Penal Code § 502(c)(5) and under § 502(c)(4).\textsuperscript{188} 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 Windows 7 example (quoted above) uses the following triggers: “the software is found to be counterfeit, improperly licensed, a non-genuine Windows product, or including unauthorized changes.”\textsuperscript{189} 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.\textsuperscript{190} When compared to the traditional recourse provided by the

\textsuperscript{186} CAL. PENAL CODE § 502(c)(5) (LexisNexis 2010).
\textsuperscript{187} Id. at (c)(4)-(5).
\textsuperscript{188} Id. at (c)(4)-(5).
\textsuperscript{189} Microsoft Software License Terms for Windows 7 Professional, § 5(c), http://download.microsoft.com/Documents/UseTerms/Windows%207_Professional_English_7b b89e9f-20ea-4555-892f-394539ec1090.pdf (last visited Sept. 12, 2010).
\textsuperscript{190} See Mark Rasch, Vista’s EULA Product Activation Worries, SECURITY FOCUS, Nov.
legal system, this constitutes a form of "self-help" 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 favor 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 US jurisdiction, the issue of international jurisdiction is of particular importance. Article 15 of the Brussels I Regulation provides that the consumer-specific rules on jurisdiction apply if, *inter alia*, "the contract has been concluded between a consumer 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 Article 15 of the Brussels I Regulation covers all types of contracts, consumer-specific rules on jurisdiction apply. According to Article 16(1) of the

---


191. *Id.*


194. *Council Directive 93/13, art. 2(b), 1993 O.J. (L 95) 31 (EC) (defines "consumer" as "any natural person who [. . .] is acting for purposes which are outside his trade, business or profession").*


196. *See Case C-180/06, Ilsinger v. Dreschers, 2009 E.C.R.153, (Recital 50 holds 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.").*
Brussels I Regulation, “a consumer may bring proceedings against the other party” in the courts where the consumer or party is domiciled.197 This is also the only jurisdiction in which proceedings may be brought against the consumer. Under Article 17 of the Brussels I Regulation, contractual derogation of these provisions that would transfer exclusive jurisdiction to the US may be possible if a corresponding agreement is entered into after the dispute has arisen.198 Contract provisions that provide for exclusive jurisdiction in the US are therefore of no legal consequence to EU consumers.

The national law applicable to a consumer contract is to be determined under Article 6 of the Rome I Regulation.199 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.200 According to Article 6(2) of the Rome I Regulation, the parties may choose a different law.201 However, such a choice may not have the result of depriving the consumer of the protection afforded to him by ius cogens202 which, in the absence of choice, would have been applicable.203 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.

Article 3(1) of the Unfair Terms Directive,204 which has been implemented by all Member States, is of particular importance in this regard. It provides that a contractual term in a pre-formulated standard contract shall be regarded as unfair and not binding205 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.”206 Article 3(1)
of the Unfair Terms Directive therefore serves a similar purpose as the unconscionability doctrine in US law.\textsuperscript{207}

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.\textsuperscript{208}

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.\textsuperscript{209}

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.\textsuperscript{210}

The warranty disclaimer and software license agreement for Adobe Reader 9.0 and Adobe Flash Player 10.0 provides in § 6.2: “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 Definitions))\(^{211}\) "that are available for automatic download to your Computer and to let Adobe know the Software is successfully installed."\(^{212}\) 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.\(^{213}\)

3.2.1. Enforceability Under EU and US 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 part 3.1 which supposedly authorize vendors to hinder the functioning of the entire computer.

Applying the unconscionability standard of California contract law,\(^{214}\) 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 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


\(^{214}\) See part 3.1.1 supra.
"additions".\textsuperscript{215}

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.\textsuperscript{216} 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.\textsuperscript{217} Every new feature is necessarily accompanied by new security vulnerabilities.\textsuperscript{218} 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 where the owner of a personal computer has no idea what software is installed on his computer. This is problematic as vendors only seek

\textsuperscript{215} Cf. StopBadware.org, Software Guidelines, http://stopbadware.org/home/guidelines (last visited Sept. 9, 2010) (stating under §III.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. . . .


\textsuperscript{217} 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, 64 (2008), http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport.

\textsuperscript{218} Programmer and security expert “Wietse Venema estimates that there is roughly one security bug per 1000 lines in his source code.” MARK G. GRAFF & KENNETH R. VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 5 (O’Reilly 2003).
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 Article 3(1) of the Unfair Terms Directive.\(^{219}\)

4. **EFFECTS ON THE SECURITY OF PERSONAL COMPUTERS**

Both EU and US 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 results in the authorization of somebody other than the owner. The following sections 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.\(^{220}\) All risks consist of the following components: an asset, vulnerabilities, safeguards, threats, and threat agents.\(^{221}\) While threats (e.g. an exploit\(^{222}\) for a newly discovered vulnerability) 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 act.

What and how much data (i.e. assets) are 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 parts of the entire file system (as does the iPhone or the iPad),\(^{223}\) removal of the files is not possible.\(^{224}\)

\(^{220}\) Note that the de-authorization of the owner may also have the positive effect that fewer Trojan horses (software that appears legitimate but contains hidden malicious functionality) are installed by users on their systems. However, since Trojan horses are a rather insignificant threat when compared to the wide array of other threats, the positive effects of de-authorization are indeed limited. \textit{But cf. Jonathan Zittrain, The Future of the Internet—and How To Stop It} 57, 150 (Yale U. Press 2008) (disregarding other threats than Trojan horses on Skype and arguing that closed systems would be more secure than open systems).

\(^{221}\) For further discussion of these risk components see Douglas J. Landoll, \textit{The Security Risk Assessment Handbook} 29-34, 36-7 (Auerbach 2006); Harris Shon, \textit{CISSP Certification All-in-One Exam Guide} 61 (4th ed. 2008).

\(^{222}\) The term exploit refers to "programs that automatically test a vulnerability and in most cases attempt to leverage that vulnerability by executing code." James C. Foster et al., \textit{Buffer Overflow Attacks} 10 (Syngress Pub. Inc. 2005).

\(^{223}\) The iPhone's and the iPad's operating system "iOS" prevents applications—and
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 software component itself (or the means to uninstall it) is protected by an access control measure whose circumvention is prohibited.

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. 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


224. See Part 2.1.2.1 supra for a discussion on 17 U.S.C. § 1201(i) and its very limited scope.

225. 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.

instance of some feature in a security system." 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 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, 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 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

227. BRUCE SCHNEIER, BEYOND FEAR 93 (Copernicus Books 2003).
228. Companies selling (exclusive) access to their customer base is a long-standing practice. See CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 162 (Harv, Bus. Sch. Press 1999).
their risk mitigation capability effectively.²²⁹

5. CONCLUSION

EU and US 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 grants 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.

²²⁹ Cf. Bruce Schneier, Make Vendors Liable for Bugs (June 6, 2006), WIRED.COM, http://www.wired.com/politics/security/commentary/securitymatters/2006/06/71032, reprinted in BRUCE SCHNEIER, SCHNEIER ON SECURITY 147-49 (2008) (arguing for the introduction of software liability because “[s]oftware vendors are in the best position to improve software security” but “don’t have much interest [in doing so]”).