Washington University Law Review

Volume 85 | Issue 3

2007

Technoconsen(t)sus

Andrea M. Matwyshyn
University of Pennsylvania

TECHNOCONSEN(T)SUS

ANDREA M. MATWYSHYN[*]

TABLE OF CONTENTS

---

* © Andrea M. Matwyshyn. Andrea M. Matwyshyn is an Assistant Professor of Legal Studies and Business Ethics at the Wharton School at University of Pennsylvania. She is also an Affiliate of the Centre for Economics & Policy at the University of Cambridge. The author wishes to thank Cem Paya, Chris Slobogin, Gerry Israel, Thomas Hurst, Jane Winn, Sharon Gordon, Jennifer Chandler, Ian Kerr, Jacqueline Lipton, Jum Carroll, Jonathan Cohen, Katherine Strandburg, Jim Chen, Bob Gomulkiewicz, Michael Siebecker, and Lee-ford Tritt for their helpful commentary and critiques.

INTRODUCTION

Popping your favorite band's new disc in a work computer can result in security compromise of your employer's computer network. Playing this disc in your home computer can result in your identity being stolen through financial data stored on your machine's hard drive and your machine becoming a remotely controlled spam zombie.[1] Consumers worry

1. Zombie drones are security compromised machines that can be controlled remotely without the user's knowledge for sending spam or other malicious purposes. *See, e.g.*, *Locking Your Cyber Front Door—The Challenges Facing Home Users and Small Businesses: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census*, 108th Cong. 84 (2004) (statement of Thomas M. Dailey, Chair and President U.S. Internet Service Providers Association, General Counsel, Verizon Online), *available at* http://a257.g.akamaitech.net/7/257/2422/10jan20051230/www.access.gpo.gv/congress/house/pdf/108hrg/96994.pdf (last visited Mar. 1, 2005); Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23 (2006); *Primer: Zombie Drone*, WASH. POST, Feb. 1, 2004, at F3.

Purchasing spam time on a zombie drone is also relatively inexpensive, costing as little as three to ten cents per host machine per week. *See, e.g.*, Andrea M. Matwyshyn, *Penetrating the Zombie*

about identity theft and express growing concern over information security,[2] yet they do not connect these concerns with their daily technology behaviors. Consumers appear to be regularly "consenting" to serious security risks, such as possible remote compromise of their machines, when they use everyday products with digital rights management technologies, or DRM. This contradiction in consumer behavior poses a critical question for the law: Is there a set of legal problems that contribute to this information security consent paradox? The answer is a resounding yes.

In the name of defending intellectual property, DRM now frequently engages in behaviors that, on their face, appear identical to hacking behaviors.[3] Many producers of digital products use DRM. In particular, digital music is being protected by the recording industry through security-invasive DRM that hides from users, cannot be easily uninstalled, compromises the security of user machines, stealthily reports on user behaviors, and permanently disables certain functions on the computers of users.[4] The determination of whether these DRM risks are known to consumers and are legally acceptable, as well as whether the DRM behaviors constitute hacking or permissible intellectual protection, turns solely on the question of whether a user consents. Therefore, digital "consent" now pushes together at least three bodies of law: intellectual property law, computer intrusion law, and contract law. Part of this information security paradox of consumer "consent" results from labels for doctrinal concepts in law crossing legal disciplines. The resulting

---

Collective: Spam as an International Security Issue, 3 SCRIPT-ed 370, 373 n.12 (Dec. 2006), *available at* http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/matwyshyn.asp. *See also* Posting of Can Read Me to Sun-breaks (Feb. 4, 2005, 11:05 EST), http://sunbreaks.blogspot.com/2005_02_01_archive.html.

2. *See, e.g.*, Juan Carlos Perez, *Security Concerns to Stunt E-Commerce Growth* (June 24, 2005), http://www.infoworld.com/article/05/06/24/HNsecurityconcerns_1.html.

3. Several recent DRM products have included features that monitor and remotely report user behaviors in the name of intellectual property protection. These products can install remotely executable code, change settings on user machines, hide themselves within other programs, lack a means of uninstallation, expose the user to security threats from malicious third parties by creating vulnerabilities on the user's machine, and communicate personal user information from the user's computer to the content owner. *See, e.g.*, Hiawatha Bray, *Security Firm: Sony CDs Secretly Install Spyware*, BOSTON GLOBE, Nov. 8, 2005, at D1, *available at* http://www.boston.com/business/technology/articles/2005/11/08/security_firm_sony_cds_secretly_install_spyware/.

4. *See, e.g.*, Bruce Schneier, *Real Story of the Rogue Rootkit*, WIRED, Nov. 17, 2005, http://www.wired.com/news/privacy/0,1848,69601,00.html.

Part of the U.S. Department of Homeland Security has advised consumers not to install software from an audio CD. *See* Press Release, U.S. Computer Emergency Readiness Team, First 4 Internet XCP (Sony DRM) Vulnerabilities (Jan. 2, 2006), http://www.us-cert.gov/current/archieve/2006/01/02/archive.html [hereinafter US-CERT].

"noise" from this accidental merger must be quickly addressed; this noise is a harbinger of an imminent large-scale security compromise of networks in the name of intellectual property protection.[5] In social systems, finding this type of legal noise triggers a need for review; sometimes, we need to prod our system toward developing into a more socially optimal regime.[6] Security-invasive DRM has revealed the need to doctrinally nudge "consent."

This Article proposes to ease doctrinal noise in consent through creating an objective "reasonable digital consumer" standard based on empirical testing of real consumers. In a manner similar to the way in which courts assess actual consumer confusion in trademark law, digital user agreements can be tested for legal usability. Specifically, a particular digital agreement would be deemed to withstand an unconscionability challenge only to the extent that a drafter can demonstrate a "reasonable digital consumer" is capable of meaningfully understanding its terms and presentation.

This proposal of an empirically generated reasonable digital consumer standard harnesses the dynamics of three separate types of code—computer code,[7] legal code,[8] and organizational code.[9] As Larry Lessig has articulated, computer code can act as a powerful form of regulation by transmitting the values of its creators, allowing legal code to then comment on computer code to exert a second regulatory force.[10] Lessig's framework can be expanded to include a third type of regulation—organizational code that arises from dynamic interactions. This regulation emerges[11] from the behavioral strategic norms of various actors, including end users in the aggregate, entities doing business, and the technology

5. Despite the urgency of the current information security situation, noise is not inherently bad. In fact, a small amount of noise in a system can result in more optimal functionality in the long term. *See, e.g.*, P.L. Mazzeo, M. Nitti, E. Stella, & A. Distante, *Visual Recognition of Noisy Fastening Bolts Using Neural Networks and Wavelet Transform*, *in* IASTED INTERNATIONAL CONFERENCE: VISUALIZATION, IMAGING, AND IMAGE PROCESSING 452-050, 566 (Sept. 6–8, 2004), *available at* http://www.actapress.com/PaperInfo.aspx?PaperID=18813.

6. Noise in law is a signal to examine doctrinal emergence and, perhaps, to modify our legal constructs in a more adaptive manner.

7. LAWRENCE LESSIG, CODE 53 (1999).

8. *Id.*

9. *See* Andrea M. Matwyshyn, *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy*, 98 NW. U. L. REV. 493, 499 (2004).

10. LESSIG, *supra* note 7.

11. Emergence is order that arises from the interactions of individual actors within a complex system, demonstrating a global pattern that could not have been forecast simply from understanding the behavior of one particular actor. *See, e.g.*, STEVEN JOHNSON, EMERGENCE: THE CONNECTED LIVES OF ANTS, BRAINS, CITIES AND SOFTWARE 18 (2001).

transactions bar. These forces shape and reshape the comparative power and legal strategies in response to changes in the system. Examining these three types of code and their regulation of digital "consent," this Article uses the case study of security-invasive DRM[12] to introduce the benefits of the reasonable digital consumer standard.

Part I of this Article introduces the challenges computer code presents to consent in the intellectual property space using the example of security-invasive DRM. It briefly describes DRM as a common business strategy for preemptively enforcing intellectual property rights. It then explains the negative consequences of this strategy for the information security of businesses, governments, and consumers. One of these negative consequences is industry confusion regarding the ethical norms of acceptable technology business conduct.

Part II examines legal code and consent, placing the norm confusion described in Part I in legal context. This section describes the strain that the emergence of security-invasive DRM has placed on copyright law, computer intrusion law, and contract law in the United States. This tension forces us to come to terms with the preexisting problems of contractual consent and form contracts in a digital context. Current doctrinal construction of digital consent has analyzed user agreements only on grounds related to procedural unconscionability. This approach is flawed as a matter of contract doctrine: procedural and substantive unconscionability must be analyzed simultaneously under either Williston's[13] or Corbin's[14] standard of unconscionability. Either of these two approaches would correctly assess as unconscionable many current user agreements.

Finally, Part III discusses the organizational code emerging at the intersection of computer code and legal code in digital contracting. It posits one possible legal approach to reconstructing meaningful consent in digital contracts in order to solve the problems of unconscionability discussed in Part II—generating an empirical objective "reasonable digital consumer" standard by looking to trademark law. Trademark case law offers well-established methods for determining whether a "reasonable" consumer is confused by a particular trademark or practice; these cases

12. For purposes of this Article, I define security-invasive DRM to refer to any DRM that changes user settings, disables functionality of the user's PC, and/or does not arrive with an uninstall capability, thereby exposing the user to additional security risks in the name of protecting digital content.

13. *See* SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS (3d ed. 1972).

14. ARTHUR L. CORBIN, CORBIN ON CONTRACTS (rev. ed. 1993).

employ empirical testing by experts using real consumers. Importing this "legal usability testing" into digital contracting would benefit both users and content owners through creating predictability of legal outcome. Similarly, a reasonable digital consumer standard leverages the naturally occurring "hubs" of understanding that both courts and content owners seek to generate through form contracts. The proposed method strikes a successful balance between customization and standardization by using the real understandings of users. It also allows for evolution of these understandings over time as users' familiarity with technology, and technology itself, advances.

I. COMPUTER CODE: DMCA, EMERGENCE OF SECURITY-INVASIVE DRM, AND DRM'S NEGATIVE CONSEQUENCES

The intersection of intellectual property, computer intrusion, and contract law has been a heated topic of legal discussion since at least the middle of the 1990s[15] and the passage of the Digital Millennium Copyright Act (DMCA).[16] The DMCA was watershed legislation: it limited the rights of users to take apart digital products they purchased and codified the right of content owners to engage in technological self-help against would-be copyright infringers.[17] Consequently, some content owners have adopted progressively more aggressive intellectual property strategies through digital means, using contract law as a backstop. A vivid case study of this dynamic is the latest iteration of DRM,[18] security-invasive DRM that frequently monitors and technologically restricts the behaviors of content users.[19] Emboldened by anti-circumvention restrictions of the DMCA,

15. One early hot-button issue at the intersection of intellectual property and data security was the so called "Clipper Chip." The clipper chip was a cryptographic device which allegedly provided the ability to protect private communications while at the same time permitting government agents to use the "keys" to unscramble communications upon presenting cause. *See, e.g.*, Electronic Frontier Foundation Archive, http://www.eff.org/Privacy/Key_escrow/Clipper_III/ (last visited May 3, 2006).

16. The DMCA amended the Copyright Act and was signed into law on October 28, 1998 as the United States' implementation of the World Intellectual Property Organization (WIPO) Copyright Treaty. However, the United States implemented the treaty in a manner that expanded copyright owners' protection more than the approaches of other countries. *See, e.g.*, U.S. COPYRIGHT OFFICE, THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 (1998), http://www.copyright.gov/legislation/dmca.pdf.

17. In the perception of the content owners DRM is a permissible self-help mechanism. In the perception of opponents to DRM, it is an illegitimate enclosure of digital commons. *See, e.g.*, LAWRENCE LESSIG, FREE CULTURE 175–60 (2004).

18. For a discussion of legal implications of DRM, see, e.g., Dan L. Burke, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537 (2005).

19. As used herein, "users" include consumers, businesses, and governments using the content protected by DRM.

DRM technologies have become progressively more invasive to the point where their conduct is, on its face, indistinguishable from criminal computer intrusion. The critical legal difference, it is frequently argued, is the user's contractual consent to the form contracts that, at least in theory, authorize the conduct.[20] This consent is usually manifested by the user,[21] with the click of a mouse, ostensibly saying "yes" to a contract that likely cannot be understood by many users and usually goes unread.[22] Meanwhile, this "consent," in theory, indicates the user's agreement to technological conduct[23] that might otherwise be considered hacking. The practice of relying on security-invasive DRM in lieu of subsequent legal action may make sense in the eyes of the companies engaging in it; it appears to be more cost effective to add a few hundred lines of code to a digital product on the front end than it is to pay several lawyers for hundreds of hours to litigate later. However, from a technology policy perspective this proactive content enforcement strategy is problematic. Apart from further straining the legitimacy of the regime created by the DMCA, these technologies also compromise information security. This compromise involves not only the security of the particular user machines the DRM inhabits, but the security of the entire information economy.[24] Consequently, a conflict in business norms has arisen regarding the ethical and legal permissibility of this conduct. This conflict reflects a belief held by parts of the technological community that users are not meaningfully "consenting" to security-invasive DRM. Put another way, they believe that users are putting themselves unknowingly at risk, installing products whose functionality and possible harms they do not understand and blindly clicking "yes" to every agreement before them.[25]

---

20. *See* Andrea M. Matwyshyn, *Technology, Commerce, Development, Identity*, 8 MINN. J.L. SCI. & TECH. 515, 523 (2007).

21. A manifestation of consent presumes the consumer is capable of finding the contract and is able to review it. Convention has arisen in the online world that user agreements are not necessarily presented in plain sight, frequently lurking at the bottom of websites in small font that is not necessarily readily visible to users. Some user agreements are not provided on website homepages. See, e.g., Google, http://www.google.com (last visited May 13, 2006), for an example of a website with a user agreement that is not visible from a homepage.

22. Users are frequently unable to read the license before proceeding with starting up a computer because no printed copy of the license is included. Users almost invariably click on "Accept" without reading the license. *See, e.g.*, Andrew Jankowitch, *EULAw: The Complex Web of Corporate Rule-Making in Virtual Worlds*, 8 TUL. J. TECH. & INTELL. PROP. 1, 5 (2006).

23. Security-invasive DRM has been labeled "spyware" in some contexts. *See infra* note 49.

24. *See infra* notes 28–30 and accompanying text.

25. *See, e.g.*, Posting of Fred Von Lohmann to Deeplinks Blog, http://www.eff.org/deeplinks/2005/11/now-legalese-rootkit-sony-bmgs-eula (Nov. 9, 2005).

A. Emergence of DRM as a Common Intellectual Property Management Strategy

Technical control measures limiting copying and use of software have been commonplace since the 1980s. However, during the 1990s, as music and movie content began to be distributed primarily through digital copies, content owners began to feel a sense of urgency for generating effective technological controls on the copying and use of content. Technological advances, particularly readily available high-speed internet access, changed the business landscape. Businesses began to view DRM as a necessary method of limiting content piracy, ensuring that only paying customers could benefit from their digital products.[26]

Proponents of any form of DRM point to widespread content piracy throughout the world[27] and the inadequacy of law in policing it. They assert digital self-help through DRM is their best hope to protect content from piracy.[28] Meanwhile, opponents of DRM have long argued against it on the principle that technology should be unfettered and that the affirmative defense of fair use prevents recovery of damages in many claims of copyright infringement asserted by content owners.[29] Similarly, opponents have pointed to technological disadvantages that DRM can bring, such as limiting functionality of applications, shortening battery life,[30] crippling the development of future computing architecture,[31] and now, perhaps most seriously, possible security compromise of user machines, allowing attackers, for example, to remotely take control of users' machines. Similarly, black markets for exploit code breaking DRM are emerging; in other words, code to circumvent DRM has acquired monetary value as a black market commodity.[32]

---

26. *See, e.g.*, Recording Industry of America Association, Piracy: Online and On the Street, http://www.riaa.com/physicalpiracy.php (last visited Mar. 9, 2006).

27. For example, it is estimated that over ninety percent of software in Vietnam consists of pirated copies and twenty-two percent of software in the United States is pirated. *See, e.g.*, NationMaster, Crime Statistics, http://www.nationmaster.com/graph-T/cri_sof_pir_rat (last visited Mar. 9, 2006).

28. *See, e.g.*, Andrew Orlovsky, *Mickey Mouse Blesses Microsoft DRM*, THE REGISTER, Feb. 10, 2004, http://www.theregister.co.uk/2004/02/10/mickey_mouse_blesses_microsoft_drm/.

29. *See* Electronic Frontier Foundation, Digital Rights Management and Copy Protection Schemes, http://www.eff.org/issues/drm (last visited Mar. 9, 2006).

30. Peter Laborge, *DRM Cuts Battery Life Short*, SECURITYFOCUS, Mar. 17, 2006, http://www.securityfocus.com/brief/166.

31. For a discussion of the systemic limitations DRM may impose on innovation and open architectures, see, e.g., CENTER FOR DEMOCRACY AND TECHNOLOGY, PROTECTING COPYRIGHT AND INTERNET VALUES (2005), http://www.cdt.org/copyright/20050607framing.pdf.

32. For a discussion of the relationship between technology black markets and intellectual

The mainstreaming of the internet and ease of digital file transfer has further catalyzed content owners' efforts to create "unbreakable" digital content protection mechanisms. Consequently, several prominent technological failures of DRM have occurred, including one DRM scheme that was easily broken simply by writing along the circumference of a CD with a permanent marker.[33] Against this technological backdrop, the DMCA[34] came into effect as the legal redundancy[35] to the technological copying restrictions of DRM. The DMCA prohibited, among other acts, circumvention of DRM.[36] As the DMCA debate continued in the legal community, prosecutions under it began. For example, in one (in)famous case, a Russian national was arrested at a technology security conference in Las Vegas in 1999 for posting code on the internet that broke a DRM scheme.[37]

These DMCA prosecutions attest that the technological knowledge to break DRM encryption schemes is likely to be possessed by many people

---

property, see, e.g., Annalee Newitz, *The High Tech Black Market*, S.F. BAY GUARDIAN, Dec. 10, 2003, *available at* http://www.alternet.org/columnists/story/17424/.

33. Team Register, *Christian Rockers Risk Wrath of DMCA with DRM Tips*, THE REGISTER, Sept. 21, 2005, http://www.theregister.co.uk/2005/09/21/christian_rockers_drm_tips/.

34. 17 U.S.C. §§ 1201–1205 (2000).

35. In computer terminology, redundancy means having additional duplicate components to improve the functionality of systems or as backup in case the initial component fails. *See* Institute for Telecommunications Science, http://www.its.bldrdoc.gov/fs-1037/dir-030/_4477.htm (last visited May 1, 2006).

36. For a discussion of the DMCA and DRM, see, e.g., Stefan Bechtold, *Digital Rights Management in the United States and in Europe*, 52 AM. J. COMP. L. 323 (2004) (arguing statutory limitations to the different means of DRM protection seem necessary); Burke, *supra* note 18 (examining social costs of deploying digital rights management systems to protect copyrighted content); Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003) (arguing that with some adjustments, DRM technologies could be harnessed to protect privacy); Chris Jay Hoofnagle, *Digital Rights Management: Many Technical Controls on Digital Content Distribution Can Create a Surveillance Society*, 5 COLUM. SCI. & TECH. L. REV. 1 (2004) (arguing DRM could lead to a "surveillance" society and proposing eight policy principles to extend privacy protection to the distribution of digital media); Jacqueline D. Lipton, *Solving the Digital Piracy Puzzle: Disaggregating Fair Use from DMCA's Anti-Device Provisions*, 19 HARV. J.L. & TECH. 111 (2005) (setting forth a new administrative complaint procedure and suggesting that the nature and scope of the fair use doctrine needs to be more fully developed for the doctrine to be a meaningful part of copyright law in the digital age); Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L.J. 501 (2003) (arguing that encryption researchers should be able to conduct and publish certain types of research without significant fear of liability under the DMCA); Declan McCullagh & Milana Homsi, *Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems*, 2005 MICH. ST. L. REV. 317 (surveying both the pro-DRM and anti-DRM remedies and arguing that both camps are mistaken and Congress should remain neutral and refrain from setting industrial policy); R. Polk Wagner, *Reconsidering the DMCA*, 42 HOUS. L. REV. 1107 (2005) (arguing that the DMCA might, contrary to the conventional wisdom, actually limit the development and deployment of DRM in the field of copyrighted goods).

37. For a list of DMCA prosecutions, see, e.g., Electronic Frontier Foundation, Recent EFF Legal Cases and Efforts, http://www.eff.org/legal/recent_legal.html (last visited Mar. 6, 2006).

apart from the creators of the DRM in question. Workarounds remind content owners that users of their content would not necessarily idly accept DRM; until DRM runs on tamper-resistant hardware,[38] digital content will remain vulnerable to copying by technologically adept, determined users. Thus, undoubtedly in frustration at the arms race between authors and breakers of DRM, content owners and DRM authors have started to resort to copyright protections in DRM that attempt to leverage security through obscurity[39]: in the words of one content owner, "[i]f consumers even know there's a DRM, what it is, and how it works, we've already failed."[40]

It comes as no surprise that the newest wave of DRM tries to hide itself and uses coding techniques that have traditionally been the domain of hackers. New variants of DRM trigger the urgent need to reconfigure the balance among copyright protection, consumer protection, and contractual consent.

B. Negative Consequences of Security-Invasive DRM for Information Security

While hacking was usually associated with users attempting to circumvent DRM technologies, in the last year the tables have turned. DRM schemes have themselves begun to use the tactics of hackers and malware authors.[41] These new breeds of DRM intend not only to prevent users from disabling the DRM but, more ominously, to prevent users from even knowing that the DRM has been installed and is operating in the background on their machines.[42] In just the last year, over 500,000 systems across 135 countries have been made vulnerable to remote

38. *See* Spencer Chang, Paul Litva & Alec Main, *Trusting DRM Software* (W3C Workshop on ORM, 2001), http://www.w3.org/2000/12/drm-ws/pp/cloakware.html.

39. "Security through obscurity" is the idea that adequate security should be driven by the subjective beliefs of the owners of a system regarding the security of that system. Therefore, if the owners believe that particular security flaws of the system are not widely known or inconsequential, then it must be the case that attackers are unlikely to find and exploit them as long as the owners keep information about the vulnerabilities secret. "Security through obscurity" is discredited in the tech community. *See, e.g.*, University of California at Irvine, The Swirl Project: Effective Security Through Visualization, http://www.isr.vic.edu/projects/swirl/ (last visited Nov. 29, 2004).

40. *Science Fiction?*, THE ECONOMIST, Sept. 3, 2005, at 62 (quoting Peter Lee, executive at Disney), *available at* http://www.economist.com/displaystory.cfm?story_id=4342418 (by subscription).

41. Two sets of Sony DRM were implicated: XCP and SunnComm's Media Max version 5. *See, e.g.*, Brian Krebs, *Study of Sony Anti-Piracy Software Triggers Uproar*, WASH. POST, Nov. 2, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/11/02/AR2005110202362.html.

42. *See, e.g.*, *Science Fiction?*, *supra* note 40.

compromise due to DRM that behaves like malicious code.[43] This means that remote attackers can readily access, examine, damage, and take control of the computers on these systems via the internet. Such systems have included systems within the military and government, including the U.S. Department of Defense.[44]

Specifically, several recent DRM products have included features that monitor and remotely report user behaviors in the name of intellectual property protection. These products can install remotely executable code, change settings on user machines, hide themselves within other programs, lack a means of uninstallation, expose the user to security threats from malicious third parties by creating vulnerabilities on the user's machine, and communicate personal user information from the user's computer to the content owner.[45] Even as the companies using these stealth DRM tactics released uninstallers, they have frequently been unapologetic for the security-invasive DRM itself;[46] they signal an unwillingness to give up security-invasive DRM as an intellectual property strategy. In at least one case, after the DRM's methodology was made known to the public, the company responsible for it provided an uninstaller that itself further compromised user machines[47] and allowed remote third parties to take control of the machines where the uninstaller had been used, turning them into "bots."[48] Once machines become bots, they can be stealthily

43. Over 200,000 copies of the program are installed on computers in Japan, 130,000 in the United States, 44,000 in the United Kingdom, 27,000 copies in the Netherlands and Spain, and between 8,000 and 12,000 in each of Korea, Peru, France, Australia, and Switzerland. *See, e.g.*, Paul F. Roberts, *Sony's 'Rootkit' Is on 500,000 Systems, Expert Says*, EWEEK, Nov. 15, 2005, http://www.eweek.com/article2/0,1759,1887181,00.asp?kc=EWRSS03119TX1K0000594.

44. Schneier, *supra* note 4; US-CERT, *supra* note 4. *See also supra* note 1.

45. Bray, *supra* note 3.

46. "'Most people, I think, don't even know what a rootkit is, so why should they care about it?' the head of Sony BMG's global digital business, Thomas Hesse, told National Public Radio." Brian Bergstein, *Copy Protection Still a Work in Progress*, ASSOCIATED PRESS, Nov. 18, 2005, http://news.yahoo.com/s/ap/20051118/ap_on_hi_te/music_copy_protection.

47. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=931 (Nov. 17, 2005, 13:46 EST).

48. Uninstallers to the Sony DRM allowed remote third parties to take control of PCs where the uninstaller was used. *Id*. Meanwhile, virus writers produced a Trojan which took advantage of the Sony-BMG rootkit and users who clicked on an alleged photograph in an e-mail installed malicious software which then connected to the Internet Relay Chat chat network and opened a channel to control the infected computer. John Borland, *'Bots' for Sony CD Software Spotted Online*, CNET NEWS.COM, Nov. 10, 2005, http://news.com.com/Bots+for+Sony+CD+software+spotted+online/2100-1029_3-5944643.html; Tom Espiner, *Trojan Horses Targeting Sony DRM Rootkit Found*, ZDNET UK, Nov. 10, 2005, http://news.zdnet.co.uk/internet/security/0,39020375,39236720,00.htm; John Leyden, *First Trojan Using Sony DRM Spotted*, THE REGISTER, Nov. 10, 2005, http://www.theregister.co.uk/2005/11/10/sony_drm_trojan/.

harnessed into networks for attacking other machines. Thus, the costs of security-invasive DRM go beyond an individual user's machine.

Meanwhile other technology companies have classified this type of DRM as "spyware," an information-collection application that is not consensually installed by a user.[49] Some companies have even released their own uninstallation tools for removing the offending code, not trusting the authors of the security-invasive DRM to fix the problems they have caused.[50] Consumer groups have filed multiple lawsuits and state attorney generals have initiated several actions resulting from at least one such DRM incident.[51]

These technology-driven dynamics demonstrate two business trends that impact construction of digital consent. First, the rise of security-invasive DRM points to progressive technological similarity of tactics used by legitimate business and criminal computer code authors. Just as information criminals surreptitiously push code to monitor user conduct onto user machines, security-invasive DRM can submit an unwitting consumer to hidden monitoring, in some instances prior to presenting the user with a User Agreement.[52]

Second, the technology business community lacks a consensus about acceptable conduct and about the role of User Agreements. The companies that have classified security-invasive DRM as spyware and released removal tools are either explicitly or implicitly condemning invasive DRM as a violation of ethical business conduct. Similarly, their actions question the practical impact of User Agreements, suggesting that had their users understood the implications of the DRM, they would not have consented to its installation. Software that exploits this informational disadvantage commonly goes by another name: "spyware."[53]

---

49. Microsoft classified Sony BMG's DRM as spyware and provided an uninstallation tool. *See, e.g.*, *Microsoft to Remove BMG Code*, BBC NEWS, Nov. 14, 2005, http://news.bbc.co.uk/1/hi/technology/4434852.stm.

50. *Id.*

51. Class action suits were filed against Sony BMG in New York and California. The Texas Attorney General also brought legal action against Sony BMG. New York and Sony reached a tentative settlement. *See, e.g.*, Associated Press, *Sony BMG Tentatively Settles Suits On Spyware*, N.Y. TIMES, Dec. 30, 2005, at C4, *available at* http://select.nytimes.com/gst/abstract.html?res=F20C10F938540C738FDDAB0994DD404482; *Sony Sued Over Copy-Protected CDs*, BBC NEWS, Nov. 10, 2005, http://news.bbc.co.uk/1/hi/technology/4424254.stm.

52. The XCP software was installed before the User Agreement appeared, and the User Agreement does not mention the XCP software explicitly. *See, e.g.*, Posting of Mark Russinovich to Sysinternals, http://blogs. technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspz (Oct. 31, 2005, 11:04 PST).

53. For example, if a content provider asks "do you want to play this CD?" without clearly explaining that certain PC functionality will be permanently disabled as a consequence, is this

These two technology trends demonstrate that noise[54] exists in the business community about the role and operational incorporation of digital consent. Just as Congress struggles with generating clear legal standards for delineating what behaviors make a piece of code illegal, the technology community is struggling with the extent of necessary disclosure about code's behavior to users. This set of evolving standards becomes complicated further when layered onto preexisting tensions in copyright law, computer intrusion law, and contract law.

II. LEGAL CODE: CURRENT DOCTRINAL TENSIONS IN INTELLECTUAL PROPERTY LAW, COMPUTER INTRUSION LAW, AND CONTRACT LAW

As explained above, noise exists in the technology community regarding ethical lines of disclosure, conduct, and obtaining meaningful user consent. Similarly, noise exists in the way the law is attempting to define digital consent at the intersection of multiple bodies of law, rekindling traditional debates about consent to form contracts with new complications. Due to technologies such as security-invasive DRM and the contracts that accompany them, doctrinal legal tensions are straining three bodies of U.S. law in particular—copyright law, computer intrusion law, and contract law.

Part of law's contribution to this information security paradox of consumer "consent" results from labels for doctrinal concepts in law crossing legal disciplines. Unlike the labels, conceptual meanings are frequently generated independently by legal disciplines and developed by different legal actors in an uncoordinated manner. Eventually these compartmentalized legal regimes bump into each other, and "noise" occurs in our system. Noise currently exists in intellectual property and technology regulation doctrine in the way law defines consent. This doctrinal tension has become painfully visible because of recent developments in DRM. The legal line between permissible copyright self-defense on the one hand and computer intrusion on the other turns solely on users' digital consent. This doctrinal noise forces us to address the

---

qualitatively different from a phishing e-mail? When a phishing e-mail arrives in a user's inbox asking "do you want us to reset your password?" and the user clicks yes, they are "consenting" to their information being shared with the fraudster. It can be argued that these two types of consent situations are not materially different; in both the user is not clear on the long-run consequences of consent.

54. The term "noise" refers to any disturbance tending to interfere with the normal operation of a device or system. *See, e.g.*, MERRIAM-WEBSTER ONLINE DICTIONARY, http://www.m-w.com/dictionary/noise (last visited May 2, 2006).

preexisting problems relating to contractual consent and form agreements or contracts of adhesion in a digital context.

A. Copyright Law, Theory, and Preemptive Self-Defense

The Constitution gives Congress the power to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[55] Under this power, Congress has enacted copyright legislation, in particular the Copyright Act[56] as amended by the DMCA.[57] Although the Copyright Act entitles the owner of a copyright to the exclusive right to reproduce, distribute, display, perform, and license the copyrighted work,[58] section 107 of the Copyright Act places a limit on this "exclusive right" through an exception for certain uses.[59] This gives rise to the idea that certain types of "fair use" exist that allow a person to copy material she has purchased within the parameters provided by the Copyright Act.[60] Copyright holders frequently view their protections more expansively than users,[61] and correspondingly argue for aggressive interpretations of what it means to commit piracy.[62] The DMCA fueled

55. U.S. CONST. art. I, § 8.

56. 17 U.S.C. §§ 101–122 (2000).

57. 17 U.S.C. §§ 1201–1205 (2000).

58. 17 U.S.C. § 106 (2000).

59. These uses include such acts that relate to criticism, comment, news reporting, teaching, scholarship and research. *Id. See generally* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994).

60. 17 U.S.C. § 106.

61. *See, e.g.*, RIAA, http://www.riaa.org (last visited May 23, 2006).

62. For a discussion of the evolving role of intellectual property rights in the digital age, see, e.g., Julie Cohen, *The Place of the User in Copyright Law*, 74 FORDHAM L. REV. 347 (2005). *See also, e.g.*, Margo Bagley, *Patent First, Ask Questions Later: Morality and Biotechnology in Patent Law*, 45 WM. & MARY L. REV. 469 (2003); Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm*, 112 YALE L.J. 369 (2002); Rochelle Cooper Dreyfus, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8, *available at* http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_81; William W. Fisher III, *Reconstructing the Fair Use Doctrine*, 101 HARV. L. REV. 1659 (1998); Jane C. Ginsburg, *Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience*, 29 COLUM. J.L. & ARTS 11 (2005); Wendy J. Gordon, *Render Copyright Unto Caesar: On Taking Incentives Seriously*, 71 U. CHI. L. REV. 75 (2004); Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 223 (2004); Mark A. Lemley, *What's Different About Intellectual Property?*, 83 TEX. L. REV. 1097 (2005); Jessica Litman, *Sharing and Stealing*, 27 HASTINGS COMM. & ENT L.J. 1 (2004); Robert P. Merges, *One Hundred Years of Solicitude: Intellectual Property Law, 1900–2000*, 88 CAL. L. REV. 2187 (2000); Eben Moglen, *Freeing the Mind: Free Software and the Death of Proprietary Culture*, 56 ME. L. REV. 1 (2004); Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems*, 83 MINN. L. REV. 129 (1998); Pamela Samuelson, *Toward a "New Deal" for Copyright in the Information Age*, 100 MICH. L. REV. 1488 (2002); Christopher Sprigman, *Reform(aliz)ing Copyright*, 57 STAN. L. REV. 485 (2004); Sara K. Stadler, *Forging a Truly Utilitarian Copyright*, 91 IOWA L. REV. 609 (2006); Eugene Volokh, *In*

this perception further. Specifically, the DMCA contains, among other things, an anti-circumvention provision that criminalizes circumvention of "a technological measure that effectively controls access to a work protected under [the DMCA]" as well as "manufactur[ing], import[ing], offer[ing] to the public, provid[ing], or otherwise traffic[king] in any technology, product, service, device, component, or part thereof . . . for the purpose of circumventing a technological measure that effectively controls access to a work protected under [the DMCA]."[63] However, from the plain language of the statute, Congress did not intend the DMCA protections for technological self-help measures to be absolute and included exceptions in the statute covering security research and spyware.[64]

Though perceived by some as providing the necessary legal support for content protection and an arguable extension of copyright law, others view the DMCA and its anti-circumvention provisions in particular as crossing the line into curtailing conduct previously defensible under fair use.[65] Let

---

Closing, The Trojan Doctrine: Trademarks and the Law of the Horse, 8 TEX. REV. L. & POL. 259 (2003); R. Polk Wagner, *The Perfect Storm: Intellectual Property and Public Values*, 74 FORDHAM L. REV. 423 (2005); Christopher S. Yoo, *Copyright and Product Differentiation*, 79 N.Y.U. L. REV. 212 (2004); Peter K. Yu, *Intellectual Property and the Information Ecosystem*, 2005 MICH. ST. L. REV. 1; Diane Leenheer Zimmerman, *Daddy, Are We There Yet? Lost in Grokster-Land*, N.Y.U. J. LEGIS. & PUB. POL'Y 75 (2005); Jonathan Zittrain, *Normative Principles for Evaluating Free and Proprietary Software*, 71 U. CHI. L. REV. 265 (2004).

63. 17 U.S.C. § 1201(a)(1)(2) (2000).

64. The language of the DMCA withdraws liability for circumventing DRM in certain instances:

> Protection of Personally Identifying Information.
>
> (1) Circumvention permitted.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if—(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected; (B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination; (C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and (D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.
>
> (2) Inapplicability to certain technological measures.—This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

17 U.S.C. § 1201(i).

65. For a discussion of how opponents of DRM believe it to be encroaching on fair use, see, e.g., Electronic Frontier Foundation, *supra* note 29.

us assume that a reasonable argument could be made in favor of non-invasive DRM using the historical justifications for copyright. In other words, let us presume for the moment that technological self-defense of intellectual property promotes economic and social welfare in the aggregate, defends the moral right of an author in the fruits of her labor, and furthers creators' self-realization by limiting others' uses of the intellectual property to those explicitly allowed by the author. However, even if one is to assume that these justifications have merit in the context of non-security-invasive DRM, they falter in the case of security-invasive DRM.

Security-invasive DRM fails to strike a balance between the rights of an author and the good of innovation generally; through security-invasive DRM one content owner potentially limits the ability of users to consume other authors' work or to generate independent digital work. On a large scale, an information economy composed of users with security compromised, crippled machines due to invasive DRM benefits no one. Innovation is stifled, and security threats include identity theft, fraud, and compromised machines being harnessed for denial of service[66] and other attacks. As such, neither economic efficiency nor self-realization of content creators is maximized when DRM crosses into the realm of security-invasiveness.

The DMCA exception relating to impermissible spyware has received little attention to date but is perhaps most on point when considering issues of security-invasive DRM. The DMCA exempts from the definition of a prohibited circumvention the act of disabling DRM that collects personally identifiable information about a user.[67] This exception implicates other bodies of law through notions of contractual consent: the framing of the exception relies on lack of "conspicuous notice" to the user.[68] However, the exception is written narrowly, allowing disabling of the DRM only if the sole effect of the disabling pertains to the data collection features, does not provide any additional access to the work, and only to the extent that the DRM was without "conspicuous notice of . . . collection or dissemination [of personally identifiable information], and

66. A denial of service attack is a type of attack where a malicious user, process, or system attempts to prevent legitimate users from accessing a network resource by exploiting a weakness in a system through, e.g., flooding network connections, filling disk storage, disabling ports, or removing power. For a discussion of service provider liability and denial of service attacks, see, e.g., Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221 (2006).

67. 17 U.S.C. § 1201(i).

68. *Id.*

without providing [the user] with the capability to prevent or restrict such collection or dissemination."[69] In essence, though, if DRM behaves in a manner described by this preceding provision without consent, it may fit both the statutory definition of spyware in many states' anti-spyware statutes[70] and, in some cases, will likely qualify as a criminal and civil computer intrusion. Thus, the determinative fact is whether a user meaningfully consented.[71]

B. Computer Intrusion Law and Theory

Just as in tort and criminal law generally, what constitutes an intrusion or an unwanted technological "touching" of a user's machine is contingent entirely on user consent. The language used by computer intrusion statutes revolves around "interception," i.e., monitoring without consent, and "exceeding authorized access," meaning surpassing the extent of consent.[72] Two federal statutes, as well as a patchwork of state statutes, use this framework of consent in the context of criminal and civil computer intrusion—the Electronic Communications Privacy Act (ECPA)[73] and the Computer Fraud and Abuse Act (CFAA).[74] DRM and

69. 17 U.S.C. § 1201(i)(1)(B).

70. Definitions of spyware vary across legislation. For a discussion of spyware legislative efforts, see, e.g., *California Goes After Spyware*, WIRED, Oct. 2, 2004, http://www.wired.com/news/politics/0,1283,65203,00.html. Spyware can be embedded as part of other products installed by the user. As such, it can bury itself into users' hard drives in a manner which makes it difficult to ferret out and uninstall. These programs then convey information back to their author. *See, e.g.*, Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH L.J. 1345 (2005).

71. For examples of state anti-spyware statutes see,, e.g., ALASKA STAT. §§ 45.45.792, 45.45.794, 45.45.798 (Supp. 2005); ARIZ. REV. STAT. ANN. §§ 44-7301–7304 (Supp. 2007); ARK. CODE ANN. §§ 4-111-101–105 (Supp. 2007); CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West Supp. 2006); GA. CODE ANN. §§ 16-9-150–157 (2007); IND. CODE ANN. §§ 24-4.8-1-1–24.4.8-3-2 (West 2006); IOWA CODE ANN. § 715.1–715.8 (West Supp. 2007); N.H. REV. STAT. ANN. §§ 359-H1–H6 (Supp. 2007); TEX. BUS. & COM. CODE ANN. §§ 48.001–48.102 (Vernon Supp. 2005); UTAH CODE ANN. §§ 13-40-101–401 (Supp. 2005); VA. CODE ANN. § 18.2-152.4 (2004 & Supp. 2006); WASH. REV. CODE ANN. §§ 19.270.010–900 (West 2007).

72. *See supra* notes 69, 70.

73. The ECPA is composed of Title I, amendments to the Wiretap and Title II, the Stored Communications Act. 18 U.S.C. §§ 2510–2522 (2000); 18 U.S.C. §§ 2701–2710 (2000). Generally, the Wiretap Act prohibits interception of communications, including those in transient storage. "Except as otherwise specifically provided in" the Act, "electronic communication[s]," which are defined expansively, may not be "intercepted." 18 U.S.C. § 2511(1)(a). An exception is provided for electronic communication service providers, but it only applies to "activity which is a necessary incident to the rendition of [the] service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i).

The Stored Communications Act restricts accessing communications that reside in a particular system. The Patriot Act clarified at least one existing possible ambiguity in the language of the Stored Communications Act by explicitly including voicemail messages under its coverage. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

other technology that collects data about users' behaviors without explicit user consent may be engaging in acts that are prohibited under both the the ECPA and the CFAA. Consequently, a finding of a legal circumvention under the DMCA can be construed to simultaneously mean a violation of the ECPA or the CFAA.

For example, the ECPA has been applied to business conduct, most recently to e-mail providers who have read and copied contents of user e-mails to their business advantage, exceeding the expectations of users created by the operative User Agreement.[75] Similarly, section 1030 of the CFAA is usually associated with criminal prosecution of hacking offenses. However, the civil and criminal offense arising out of "unauthorized access" to computer systems as well as the "transmission" of harmful

---

(USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). The Stored Communications Act's main criminal provision reads as follows:

> (a) Offense. Except as provided in subsection (c) of this section whoever—(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished.

18 U.S.C. § 2701(a).

74. 18 U.S.C. § 1001 et seq. (2000). The Stored Communications Act's contains an explicit "provider" exception: "Subsection (a) of this section does not apply with respect to conduct authorized—(1) by the person or entity providing a wire or electronic communications service." § 2701(c). It has been argued that § 2701(c)(1) establishes almost complete immunity for a service provider that "obtains, alters, or prevents authorized access to" e-mail that is "in electronic storage" in its system. *See* Fraser v. Nationwide Mut. Ins., 352 F.3d 107, 115 (3d Cir. 2003) ("[W]e read § 2701(c) literally to except from Title II's protection all searches by communications service providers."). A second provision of the Stored Communications Act prohibits "a person or entity providing an electronic communication service to the public [from] knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). This provision also has service provider exceptions, permitting a provider to give access to an electronic communication "to a person employed or authorized or whose facilities are used to forward such communication to its destination," or "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." §§ 2702(b)(4), (5). Some confusion exists regarding the interaction of the two statutes and certain potential definitional ambiguities. Most recently the interaction of the two parts of the ECPA was discussed in United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005).

75. *See Councilman*, 418 F.3d at 70. Bradford Councilman was a bookseller who provided a free e-mail service to his customers. Councilman directed his employees to intercept and copy all incoming communications to their customers from Amazon.com. The system administrator modified the server's procmail recipe to copy the message and place the copy in a separate mailbox that Councilman could access prior to customers' receiving the e-mails for the purpose of gaining competitive advantage over Amazon.com. The appeals court construed the provider exceptions to the Stored Communications Act liberally and deemed Councilman to fall within them. *Id*. at 79. With regard to the Wiretap Act, however, the appeals court overruled the lower court, concluding that the term "electronic communication" as used in the Wiretap Act includes transient electronic storage integral to the communication process, and therefore, an interception of an e-mail message in this transient storage is an offense under the Act. *Id*.

code[76] can apply to business practices as well. For instance, a wide range of relatively common business practices have been challenged in civil suits under section 1030, including automated searches,[77] dropping cookies,[78] sending spam,[79] changing hosts' communication configurations,[80] and port scanning.[81] These same behaviors, some of which are behaviors of security-invasive DRM, may run afoul of computer intrusion law unless prior consent of the system owner is obtained.

Similarly, behaviors prohibited in state spyware statutes include behaviors exhibited by security-invasive DRM.[82] More than ten states have passed anti-spyware statutes.[83] These statutes vary in their definition

76. For a discussion of the current state of criminal computer intrusion statutes see, e.g., Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1 (2004); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003). *See also* Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261 (2003).

77. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1062 (N.D. Cal. 2000).

78. *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001) (abrogated by Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 935 (9th Cir. 2004)).

79. Christian v. Sony Corp. of Am., 152 F. Supp. 2d 1184, 1187 (D. Minn. 2001); America Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000).

80. *See, e.g.*, *In re* AOL, Inc., Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1364 (S.D. Fla. 2001) (finding that AOL's transmission of its Version 5 software which allegedly "changes" the host system's communications configuration and settings to interfere with non-AOL communications and services deemed actionable under 1030(a)(5)(A)); *Christian*, 152 F. Supp. 2d at 1187 (deeming the inclusion of a defective FDC constituted a "transmission" within the meaning of section 1030).

81. *See* Steve Brewer, *County Cuts Off Computer Network*, HOUSTON CHRONICLE, Mar. 21, 2002, at A29, *available at* http://www.chron.com/cs/CDA/story.hts/topstory/1302663#top. *See also* Ann Harrison, *Plea Agreement In Distributed Computing Case*, SECURITYFOCUS, Jan. 18, 2002, http://www.securityfocus.com/news/311; John Leyden, *Ethical Hacker Faces War Driving Charges*, THE REGISTER, July 26, 2002, http://www.theregister.co.uk/2002/07/26/ethical_hacker_faces_war_driving/. As a result, computer security professionals fear that distributed computing itself may be illegal. *See* Ann Harrison, *Is Distributed Computing A Crime?*, SECURITYFOCUS, Dec. 20, 2001, http://www.securityfocus.com/news/300.

82. *See, e.g.*, ALASKA STAT. §§ 45.45.792, 45.45.794, 45.45.798 (Supp. 2005); ARIZ. REV. STAT. ANN. §§ 44-7301–7304 (Supp. 2007); ARK. CODE ANN. §§ 4-111-101–105 (Supp. 2007); CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West Supp. 2006); GA. CODE ANN. §§ 16-9-150–157 (2007); IND. CODE ANN. §§ 24-4.8-1-1–24.4.8-3-2 (West 2006); IOWA CODE ANN. § 715.1–8 (West Supp. 2007); N.H. REV. STAT. ANN. §§ 359-H1–H6 (Supp. 2007); TEX. BUS. & COM. CODE ANN. §§ 48.001–102(Vernon Supp. 2005); UTAH CODE ANN. §§ 13-40-101–401 (2005); VA. CODE ANN. § 18.2-152.4 (2004 & Supp. 2006) (requiring malicious intent); WASH. REV. CODE ANN. §§ 19.270.010–900 (West 2007).

83. To date, despite several attempts, no federal statute explicitly addresses spyware. *See, e.g.*, Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283 (2005); Susan B. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433 (2005); Paul M. Schwartz, *Privacy Inalienability and the Regulation of Spyware*, 20 BERKELEY TECH. L.J. 1269 (2005); Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH. L.J. 1345 (2005).

of spyware, as well as in the regulatory approaches they adopt, but generally also focus on prohibited behavior as behavior that lacks user consent. They set forth prohibitions on various conduct including software that changes user settings, software that cannot be uninstalled, software that usurps user control of a machine, and software that sends data to remote third parties, among others.[84] In other words, they criminally prohibit the behaviors exhibited by security-invasive DRM without user consent.

C. Contract Law and Theory

The legal nexus of digital consent is contract law. For many bodies of law, the technology revolution has added a complicating factor to the legal equation; in contract law, the uneasy peace of doctrine around form contracts/contracts of adhesion has been permanently disrupted.[85] As seen in the context of DRM, it is user consent to a form digital contract that

84. *See, e.g.*, Winn, *supra* note 83.

85. For a discussion of the tension between freedom of contract and consumer protection, see, e.g., Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87 (1989) (discussing significance of the distinction between default and mandatory rules for consumers); Randy E. Barnett, *The Sound of Silence: Default Rules and Contractual Consent*, 78 VA. L. REV. 821, 871 (1992) (describing a "conflict between the two aspects of the liberal conception of contractual freedom: freedom to contract and freedom from contract" (citing Richard E. Speidel, *The New Spirit of Contract*, 2 J.L. & COM. 193, 194 (1982))); Lisa Bernstein, *Private Commercial Law in the Cotton Industry: Creating Cooperation Through Rules, Norms, and Institutions*, 99 MICH. L. REV. 1724 (2001) (asserting that rules created by trade association to govern contractual disputes diverge from rules contained in Article 2 of U.C.C.); Richard Craswell, *Contract Law, Default Rules, and the Philosophy of Promising*, 88 MICH. L. REV. 489 (1989) (discussing the role of default rules); Melvin Aron Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 STAN. L. REV. 211, 252 (1995) ("[T]he problem raised by contracts to govern thick relationships is not a problem of unconscionability. Usually, neither party to such a relationship will have exploited the other at the time the contract was made. Quite the contrary, both parties will have probably been subject to exactly the same cognitive limits."); Christine Jolls, *Contracts as Bilateral Commitments: A New Perspective on Contract Modification*, 26 J. LEGAL STUD. 203, 205 (1997) ("Contrary to traditional wisdom, the parties to a contract may be better off if the law enables them to tie their hands, or ties their hands for them, in a way that prevents them from taking advantage of certain ex post profitable modification opportunities."); Michael Klausner, *Corporations, Corporate Law, and Networks of Contracts*, 81 VA. L. REV. 757 (1995) (describing network effects and the potential for suboptimal contracts); Zvika Neeman, *The Freedom to Contract and the Free-Rider Problem*, 15 J.L. ECON. & ORG. 685 (1999) (arguing that a person contracting with multiple actors can induce them to refrain from acting in their collective interest); Eric A. Posner, Essay, *Economic Analysis of Contract Law After Three Decades: Success or Failure?*, 112 YALE L.J. 829, 842 (2003) ("The premises of economics push in the direction of freedom of contract, and this current can be resisted only with difficulty."); Alan Schwartz & Robert E. Scott, *Contract Theory and the Limits of Contract Law*, 113 YALE L.J. 541, 619 (2003) (arguing that mandatory contract rules should center on regulating contracts tinged by unconscionability, fraud, or duress, and contracts that create externalities).

usually creates a critical legal distinction between legal and illegal digital conduct.

1. Why Digital Consent and Technology-Mediated Form Contracts are Different from Real Space Form Contracts

It is true that technology contracting triggers the age-old form contract doctrinal debate—customization versus standardization. However, the contours of this debate are altered in a digital medium. As Professor Radin has pointed out in the context of the internet,[86] the internet's increasing content customization in transactions is perhaps fundamentally incompatible with content owners' need for predictability in outcome and reliance on standardization through form contracts.

Technology-mediated contracting is a qualitatively different experience for users than real space contracting.[87] Individuals who might attempt to read a form contract in real space may behave differently in technology-mediated contracting contexts.[88] Unlike in many real space contract situations, inputs in technology contracting scenarios are impoverished: parties to contracts mediated by technology are rarely in the same room or in contact through any real time method. No humans are readily accessible; asking questions about the meaning of contractual terms becomes a cumbersome, if not impossible, undertaking. The importance of objective indicators of consent plays a greater role in virtual space than it might in real space. However, even objective consent determinations by

---

86. *See* Margaret Jane Radin, *Online Standardization and the Integration of Text and Machine*, 70 FORDHAM L. REV. 1125 (2002). *See also* Marcel Kahan & Michael Klausner, *Standardization and Innovation in Corporate Contracting (Or "The Economics of Boilerplate")*, 83 VA. L. REV. 713, 719–20 (1997).

87. *See, e.g.*, United States and International Perspectives on Electronic Marketplaces, 14 INT'L L. PRACTICUM 68, 74 (2001) (including the comments of Michael M. Maney). For discussion of business and consumer concerns in particular technology contracting contexts, see, e.g., Anita L. Allen, *Minor Distractions: Children, Privacy and e-Commerce*, 38 HOUS. L. REV. 751 (2001); Jay P. Kesan & Andres A. Gallo, *The Market for Private Dispute Resolution Services—An Empirical Re-Assessment of ICANN-UDRP Performance*, 11 MICH. TELECOMM. & TECH. L. REV. 285 (2005); Ronald J. Mann, *"Contracting" for Credit*, 104 MICH. L. REV. 899 (2006); Anita Ramasastry, *State Escheat Statutes and Possible Treatment of Stored Value, Electronic Currency, and Other New Payment Mechanisms*, 57 BUS. LAW. 475 (2001); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333 (2006).

88. Users behave differently in real and virtual space. For example, although most people would be hesitant to share the keys to their home with others or use the same key for both the door to their home and office, users engage in password sharing for websites frequently and usually use the same password for multiple websites. *See, e.g.*, Shannon Riley, *Password Security: What Users Know and What They Actually Do*, USABILITY NEWS, Aug. 1, 2006, http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.htm.

courts have limitations in digital context. For example, unlike in real space where each form contract copy is physically identical, "objective" factors, such as the size of text on a screen, may vary from computer to computer.[89]

Therefore, new technologies have generated challenges to determining meaningful consent, challenges that exist in digital form contracts but do not exist in real space form contracts. As a consequence, the risks of unconscionability in digital form contracts are higher than risks in real space contracts. The state of current digital contracting doctrine does not adequately reflect these subtleties. In the context of technology-mediated contracts and avoiding unconscionability, a stronger medium-specific contract doctrine of consent is needed.

2. The Current State of Digital Contracting Doctrine

To date, courts have approached the analysis of digital consent by focusing on objective procedural aspects of digital consent. Currently, courts are building doctrine around procedural fairness of digital consent through four lead cases—*ProCD, Inc. v. Zeidenberg*,[90] *Register.com, Inc. v. Verio, Inc.*,[91] *Specht v. Netscape Communications Corp.*,[92] and the most recent iteration of *Ticketmaster Corp. v. Tickets.com, Inc.*[93] These cases discuss the process of formation from an objective perspective and, specifically, whether a reasonable user is likely to have known digital consent was being given.[94]

In *ProCD, Inc. v. Zeidenberg*, an individual purchased software that displayed license terms in a "clickwrap" format[95] on the computer screen every time the user executed the software program. In other words, the user affirmatively demonstrated assent to the User Agreements by

89. Bob Baumel, Understanding Cross-Platform Text Size Differences (Jan. 2, 2004), http://home.earthlink.net/~bobbau/platforms/text-size/.

90. 86 F.3d 1447 (7th Cir. 1996).

91. 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd as modified* 356 F.3d 393 (2d Cir. 2004).

92. 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff'd* 306 F.3d 17 (2d Cir. 2002).

93. No. CV997654HLHVBKX, 2003 WL 21406289, (C.D. Cal. Mar. 07, 2003).

94. None of these cases have focused on the inability to negotiate the terms of the User Agreements. Nonnegotiability is a hallmark of contracts of adhesion and is a factor that may demonstrate procedural unconscionability of a contract.

95. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1450 (7th Cir. 1996). Clickwrap is the term used to describe an agreement presentation that appears in a window that opens to reveal the text of the agreement. The agreement is accompanied by a dialogue box with the button label "I agree" that the user must click prior to gaining access to the website content. For a discussion of clickwrap and browsewrap agreements, see, e.g., Ryan J. Casamiquela, *Contractual Assent and Enforceability in Cyberspace*, 17 BERKELEY TECH. L.J. 475 (2002).

selecting "yes" or "ok" on the screen.[96] The Seventh Circuit deemed the user to have had sufficient opportunity and notice in order to review the terms and to return the software if he did not wish to consent.[97] Consequently, the purchaser was contractually bound because of click-through consent to the terms which were conspicuously displayed on his screen.[98] *Register.com, Inc. v. Verio, Inc.* presented a slightly more nuanced internet contracting inquiry. A domain name registrar sued a service provider who repeatedly requested data electronically for marketing purposes from the website of the domain name registrar in violation of the registrar's User Agreements.[99] After each such query, the service provider was presented with a notice that the act of querying constituted consent to the registrar's User Agreements.[100] Because of the large number of times the service provider encountered the explicit, conspicuous notice of being bound by the registrar's User Agreements, and because of the service provider's acknowledgment that it was aware of the existence of the User Agreements, the court ruled in favor of the plaintiff registrar.[101] Thus, repeated exposure to a conspicuous notice of User Agreements presented in a sentence was deemed to constitute affirmative consent to the terms.[102]

However, *Specht v. Netscape Communications Corp.* explained that if a website does not explicitly and clearly communicate that by clicking a download button or taking another action a consumer is assenting to User Agreements, such User Agreements would not be upheld.[103] In *Specht*, the defendants moved to compel arbitration under the terms of a license agreement which was presented through a small link to the User Agreements at the bottom of the homepage.[104] The website at issue used a link that said "terms," and was presented below-the-fold in unremarkable type.[105] The defendants in *Specht* argued that the plaintiffs should be held to a standard of "reasonable prudence," and that they should have known to scroll to the bottom of the webpage to look for license terms. The court

96. *ProCD*, 86 F.3d at 1452.
97. *Id.*
98. *Id.* at 1453.
99. 126 F. Supp. 2d 238, 241.
100. *Id.* at 242
101. *Id.* at 254.
102. *Id.*
103. Specht v. Netscape Comm. Corp., 150 F. Supp. 2d 585, 595–96 (S.D.N.Y. 2001).
104. In *Specht*, internet users and a website operator brought a putative class action, alleging that a free software program invaded their privacy by transmitting information to the software provider without users' consent. *Id* at 586.
105. *Id*.

rejected this argument, noting that license terms on a screen not readily visible are not enforceable when the defendant does not provide conspicuous notice of their existence to users.[106] According to the *Specht* court, characteristics of unclear "browsewrap" links include use of small font, such as the font used for these footnotes, gray type on gray background, and unclear labeling of the link that intended to alert the user to the existence of an agreement behind the link.[107] Finally, the second iteration of *Ticketmaster Corp. v. Tickets.com, Inc.*[108] introduced a new generation of homepage User Agreement presentation. The Ticketmaster website presented a link to its User Agreements at the top of its homepage by embedding the link to the User Agreements in a sentence which stated that by browsing the website, the user was affirmatively consenting to be bound by the Ticketmaster User Agreements.[109] Ticketmaster argued that Tickets.com, among other things, violated the Ticketmaster User Agreements by copying ticket and show information off the Ticketmaster website through the use of spiders and bots[110] on a continuous basis in violation of the Ticketmaster User Agreements. Ticketmaster asserted Tickets.com was bound by the User Agreements because it had received notice of being bound by them through the browsewrap[111] embedded in a notice sentence on the Ticketmaster homepage. Tickets.com sought summary judgment on all counts, and the court deciding the matter dismissed all counts by Ticketmaster against Tickets.com except for this allegation in contract. The court deemed the contract issue worthy of surviving summary judgment; the obvious placement of the link to the User Agreements at the top of the Ticketmaster homepage and the link's being embedded in an explicit notice sentence of contract formation "could not be missed."[112]

106. *Id.* at 596.

107. *Id.* A browsewrap is an agreement whose content is linked and no additional notice aside from the presence of the link is provided to the consumer regarding the existence of the agreement.

108. No. CV997654MLHVBKX, 2003 WL 21406289 (C.D. Cal. Mar. 07, 2003). The first iteration of a lawsuit between the same parties ended with Ticketmaster's User Agreements not being upheld by the court deciding the matter. Ticketmaster Corp. v. Tickets.com, Inc., No. 00-56574, 2001 WL 51509 (9th Cir. 1998).

109. This notice sentence browsewrap presentation from around the time of the second *Ticketmaster* litigation can be viewed at Internet Archive, http://web.archive.org/web/20030403073630/www.ticketmaster.com/ (last visited Aug. 30, 2004).

110. Spiders and bots are small computer applications that run in the background and send data back to their originator on an ongoing basis. *See, e.g.*, Jeffrey M. Rosenfeld, *Spiders and Crawlers and Bots, Oh My: The Economic Efficiency and Public Policy of Online Contracts that Restrict Data Collection*, 2002 STAN. TECH. L. REV. 3.

111. *See supra* note 109.

112. *Ticketmaster*, 2003 WL 21406289 at *2.

When taken together, these four cases can be said to create a sliding scale of User Agreement enforceability. On the one hand, clickwrap agreements that prevent the user from accessing content without an explicit affirmative demonstration of consent will tend to be enforced by courts.[113] On the other hand, courts tend to decline to enforce a browsewrap agreement[114] with an ambiguous link located below-the-fold[115] with no affirmative demonstration of consent by the user.[116] In between these two extremes are browsewrap agreements which might be called "notice sentence browsewraps."[117] These "notice sentence browsewraps" intend to provide notice to a user of User Agreements through their placement and presentation of a link to the terms, usually in a full sentence above-the-fold on the homepage. In other words, the user is advised that taking a certain action constitutes consent to the terms of the linked agreement—the User Agreement presentation upheld by the *Ticketmaster* court.[118] The more objectively conspicuous the notice of terms, the more likely a court is to determine a contract is procedurally fair and that digital consent exists.

Under the current approach courts apply, commonality in understanding of the User Agreement between users and the content owner is not the critical inquiry, nor is the actual understanding of users. Currently, the only critical inquiry courts undertake is whether the terms of the User Agreement are presented in a conspicuous manner. If presentation is conspicuous in the subjective opinion of the court, the court deems consent to exist and enforces the terms as drafted and understood

---

113. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996).

114. *See, e.g.*, Casamiquela, *supra* note 95.

115. Below-the-fold means the portion of the graphical user interface which is not readily visible to a user within the confines of the user's monitor when the website loads. Accordingly, above-the-fold is the readily visible portion. *See, e.g.*, Marketingterms.com, http://www.marketingterms.com/dictionary/above_the_fold/ (last visited May 3, 2004).

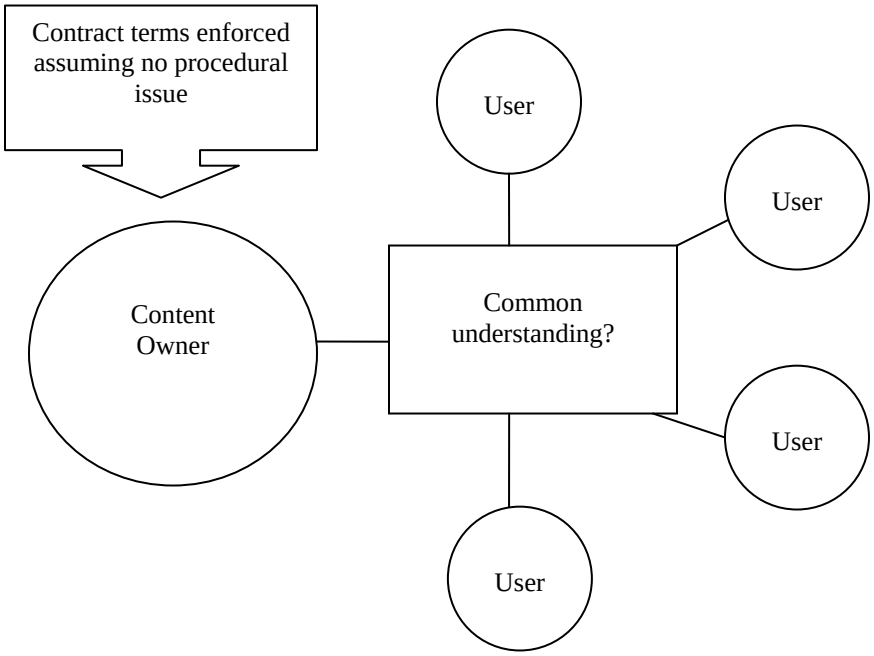
116. In *Specht*, the court deemed browsewrap User Agreements without a notice sentence and below-the-fold to be unenforceable. Specht v. Netscape Comm. Corp., 150 F. Supp. 2d 585, 595 (S.D.N.Y. 2001).

117. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 254 (S.D.N.Y. 2000). In *Verio*, the court deemed the defendant to have notice of the browsewrap User Agreements in a notice sentence within a data entry dialog box. *Id*. at 254. *See also Ticketmaster*, 2003 WL 21406289, at *6. In *Ticketmaster* (2003), above-the-fold browsewrap User Agreements embedded in a notice sentence were deemed adequate to survive summary judgment challenge to contract claim. *Id*.

118. At the time of this writing, Ticketmaster has changed the placement of their User Agreement link on their homepage following the *Ticketmaster* case. However, the notice sentence browsewrap remains. See, e.g., Ticketmaster, http://www.ticketmaster.com (last visited May 2, 2006) for an example of a notice browsewrap User Agreement presentation. *See, e.g.*, Yahoo!, http://www.yahoo.com (last visited May 2, 2006) for an example of a traditional browsewrap User Agreement presentation.

by the content owner. Thus, our current system can be depicted by Figure A below. Each circle represents a party to a User Agreement and the links represent commonalities of understanding of User Agreements. It is likely that many users will have common (mis)understandings of a User Agreement. However, the extent to which these user understandings overlap with each other, and especially with the understanding of the drafter, a content owner, is unknown. This deficit in mutual understanding, or "meeting of the minds," is represented by a question mark in Figure A.

FIGURE A: CONSENT IN OUR CURRENT SYSTEM



3. Both Williston's and Corbin's Definitions of Unconscionability are Met by Many User Agreements

Current case law's sliding scale of procedural fairness in execution of digital contracts is only half the picture. The other half relates to substantive fairness and preventing unfair surprise.[119] In the United States,

119. I am rejecting Epstein's argument that the only appropriate basis for findings of unconscionability include fraud, duress and undue influence. I recognize "unfair trade practices" that

challenges[120] could be brought to User Agreements on the basis of either or both procedural unconscionability and substantive unconscionability. To date, courts have focused solely on the procedural unconscionability, framing opinions using the language of consent.[121] This approach comports with neither Williston's nor Corbin's approach to unconscionability and merits reassessment.

Under traditional constructions of ensuring fairness and preventing unconscionability, procedural and substantive fairness are sometimes incorporated into a type of Willistonian sliding scale approach to unconscionability that combines both procedural and substantive factors in its analysis.[122] The method of execution and the complicated content in most User Agreements, when taken together, render most User Agreements wholly inaccessible to an average user, eviscerating the existence of meaningful consent under Williston's approach. Similarly, Corbin's test of unconscionability, which examines the terms in light of the general commercial background and the commercial needs of the particular trade, is also met in the context of many User Agreements.[123] Under Corbin's approach, User Agreements are allegedly authorizing conduct of ostensibly reputable companies, conduct that, in the opinion of other reputable companies in the same business, crosses the line into unwanted, even potentially illegal conduct as Part I of this Article describes. In the case study of invasive technologies such as security-invasive DRM, the combined weight of these two sets of factors bespeaks the urgency of reconstructing how and to what reasonable consumers

---

fall short of fraud in other legal contexts, and this concept seems logical to include in contract law as well. *See* Richard A. Epstein, *Unconscionability: A Critical Reappraisal*, 18 J.L. & ECON. 293 (1975). For additional views of unconscionability see, e.g., Richard L. Barnes, *Rediscovering Subjectivity in Contracts: Adhesion and Unconscionability*, 66 LA. L. REV. 123 (2005); Philip Bridwell, *The Philosophical Dimensions of the Doctrine of Unconscionability*, 70 U. CHI. L. REV. 1513 (2003); Richard Craswell, *Property Rules and Liability Rules in Unconscionability and Related Doctrines*, 60 U. CHI. L. REV. 1 (1993); Jeffrey L. Harrison, *Class, Personality, Contract, and Unconscionability*, 35 WM. & MARY L. REV. 445 (1994); Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203 (2003); Paul Bennett Marrow, *Squeezing Subjectivity From the Doctrine of Unconscionability*, 53 CLEV. ST. L. REV. 187 (2005); Horacio Spector, *A Contractarian Approach to Unconscionability*, 81 CHI.-KENT L. REV. 95 (2006).

120. European Union grounds for invalidation of User Agreements content include violation of, among other directives, the European Union Directive on Distance Contracts and the Directive on Unfair Terms. *See* James R. Maxeiner, *Standard-Terms Contracting in the Global Electronic Age: European Alternatives*, 28 YALE J. INT'L L. 109 (2003).

121. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (focusing on consent in contract formation).

122. *See* 15 SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS, § 1763A, at 213 (3d ed. 1972).

123. *See* ARTHUR L. CORBIN, CORBIN ON CONTRACTS § 128, at 188 (1952).

meaningfully consent. As previously discussed, companies using these invasive DRM methods frequently intentionally cloak their presence on user systems, inhibiting full understanding of their workings by almost all users. Meanwhile, other technology companies have labeled this type of DRM to be spyware rather than a legitimate intellectual property protection. Thus, under either Williston's or Corbin's standard for unconscionability, meaningful user consent to User Agreements is unlikely to exist in many instances. Consequently, relying on digital consent to User Agreements to authorize conduct otherwise tantamount to computer intrusion is a dubious legal approach. Users can not always find or understand the User Agreements to which they have allegedly consented. This difficulty arises both because of users' lack of technology knowledge and because of the agreements themselves.[124]

To resolve a portion of this doctrinal noise, courts should adopt a new approach for objectively assessing digital consent, an approach that would ensure User Agreements are likely to pass both Williston's and Corbin's tests for unconscionability. The next section introduces one such possible approach—an objective reasonable digital consumer standard.

III. ORGANIZATIONAL CODE: REDUCING NOISE THROUGH THE "REASONABLE DIGITAL CONSUMER"

Crafting an ideal legal regime of digital consent means taking into account three fundamental ecological tensions in the technology contracting space: (i) a macrosystem-level tension between content entrepreneurship and consumer protection, (ii) a mesosystem-level tension between legal content customization and legal standardization, and (iii) a microsystem-level tension in simultaneously aiding development of both content owners and users, despite an information power imbalance in favor of the content owner.

---

124. Similarly the U.C.C.'s approach to unconscionability would not save these User Agreements. U.C.C. section 2-302 requires a tribunal to focus on the commercial setting surrounding the transaction in question before making its determination as to unconscionability. U.C.C. § 2-302 (year). Here, even assuming that U.C.C. applies, a question that is not clear, the commercial standards are unclear and developing uniform law in this context would be hindered. It might also be argued that perhaps courts are adopting Professor Epstein's approach to unconscionability. Professor Epstein borrows the dichotomy between procedural and substantive unconscionability constructed by Professor Leff to argue that the only acceptable bases for unconscionability are solely procedural defects in formation. The substance of contractual provisions are not a primary concern under Epstein's approach. However some variants of DRM can be deemed to have even crossed Epstein's line: they install themselves prior to providing a copy of the user agreement for review. *See* Epstein, *supra* note 119, at 294. *See also* Arthur Allen Leff, *Unconscionability and the Code—The Emperor's New Clause*, 115 U. PA. L. REV. 485, 486–87 (1967).

On the macrosystem or social level,[125] a successful technology contracting architecture doctrinally constructs consent in a manner that both facilitates consumer protection concerns and allows for efficient business operations. It is only when both these interests are served that a stable, trusted commercial technology environment will develop. In other words, the need for innovation must be successfully balanced with the need for mass utilization[126] and continuous evolution in the technology and intellectual property space.[127] Practically speaking, this means creating a construction of consent that assists companies in mitigating business risk on the one hand, in exchange for ethical[128] treatment of users on the other.

The mesosystem or interpersonal level[129] of a successful architecture for technology contracting should foster development of relational commercial trust between the parties. Thus, machine-text convergence[130] appears to be an inevitability; the ever-increasing customization of digital content must be reconciled with legal predictability on a transaction-by-transaction basis.[131] In each transaction through a technology-mediated contract, users should have a meaningful opportunity to read and

125. This section adopts an ecological framework of analysis loosely based on the work of Urie Bronfenbrenner. *See* URIE BRONFENBRENNER, THE ECOLOGY OF HUMAN DEVELOPMENT 258 (1979). Macrosystem-level analysis requires examination at the level of culture as a whole, along with belief systems and ideologies underlying cultural rules and norms. In other words, the analysis focuses on the mechanisms of social governance and the worldview prevalent in civil society. *Id.*

126. Adopting the language of architectural theorist Le Corbusier, the question of internet data security contracting asks us to balance the need for constant architectural innovation with the need for mass utilization of the architecture. Creativity must coincide with functionality for the people who exist within the space. *See* LE CORBUSIER, TOWARDS A NEW ARCHITECTURE 265 (1931).

127. Turning to the lessons of cybernetics theory, Norbert Weiner's work, as expanded by cybernetics theorist Gordon Pask, points us to the importance of constructing architectures with feedback loops. Stagnancy in construction does not enable evolution of a space and results in obsolescence. NORBERT WEINER, CYBERNETICS 113 (1948); Gordon Pask, *The Architectural Relevance of Cybernetics*, 9 ARCHITECTURAL DESIGN 494, 496 (1969).

128. I use "ethical" here to refer to truthful disclosure and fulfillment of promised contractual obligations.

129. The mesosytem or interpersonal level of analysis focuses attention on interpersonal dynamics and the dynamics between the individual and secondary settings, such as work or business partners. BRONFENBRENNER, *supra* note 125, at 209. In other words, mesosystem refers to the level of each commercial exchange between a content owner and a user.

130. When Radin discusses machine-text convergence she means that legal and technical standardization are closely related and that a paradigm shift is occurring in the manner in which we conceptualize contracting. Radin, *supra* note 86, at 1138–39.

131. One option for reconciling this tension is creating standardization of process in lieu of standardization of content. Standardized process, meaning fair and uniform contract formation and enforcement rules, can provide a stable basis for contractual interpretation, while customized content both enables the user to obtain value for her data and contract upon terms of her choice.

understand the terms of User Agreements that govern their relationships, should they wish to do so.

Finally, on the microsystem or individual level of analysis, a successful digital contracting architecture would simultaneously foster development and economic self-realization of both the content owner[132] and user. In other words, development is a social process, and it is critical to acknowledge the influence of the social environment and its tools on development.[133] From the perspective of the companies that author User Agreements, a successful legal architecture of consent enables predictable outcomes for business development, expansion, and greater economic self-realization without unduly burdensome legal commitments to users. Meanwhile, from a user's developmental perspective, a successful consent architecture scaffolds[134] the user in technology contracting, protecting them from possible harms due to companies' unethical conduct. Perhaps most importantly, a successful technology contracting architecture may also assist users in evolving to view technology as a natural extension of their being.[135]

Elaborating on these concerns differently, the ideal architecture for digital consent would generate an exact overlap of understood meaning among users and a content owner. This meaning would be memorialized in a User Agreement that articulated all material risks faced by both users and the content owner. All parties in this ideal universe would share an identical understanding of the terms and no disagreements of meaning would arise. In Figure B below, each circle represents a party to the User Agreement and each link represents a commonality in understanding of the User Agreement's terms. Using the language of network theory, one could argue that consent in an ideal system resembles a highly interconnected random network, a network where no node is likely to be

132. Content owners are not necessarily large entities. One of the primary cultural shifts precipitated by the internet is a rise in entrepreneurship because the transaction costs of internet business are significantly lower than those in real space. Therefore, a content owner could be one individual entrepreneur who relies on an internet business as a primary source of income.

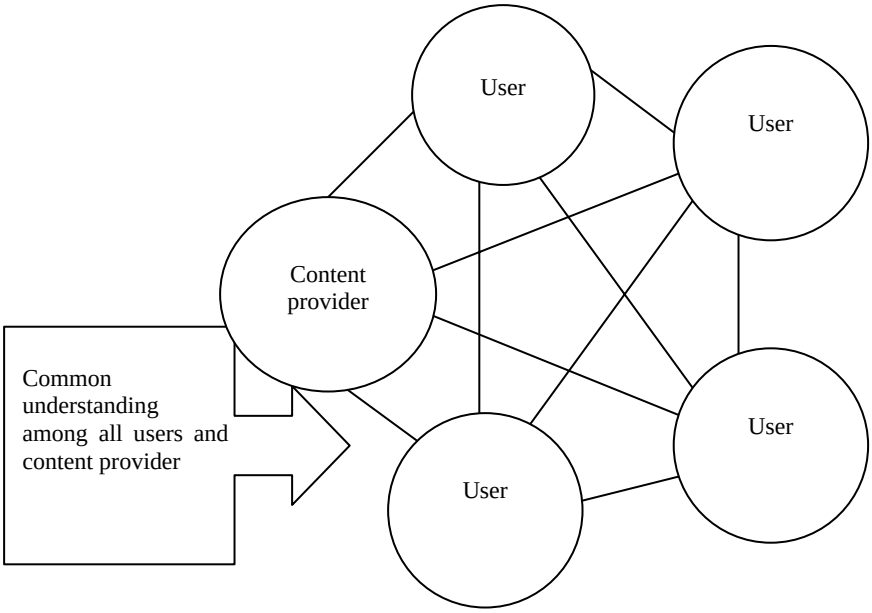
133. The perspective adopted here is that of nonlinear contextualist human development theory. As such, it views development as a dialectical process with the environment that uses the "cultural tools" of the environment to facilitate development. For a discussion of cultural tools, see James V. Wertsch & Peeter Tulviste, *L.S. Vygotsky and Contemporary Developmental Psychology*, *in* AN INTRODUCTION TO VYGOTSKY 59, 67 (Harry Daniels ed., 2d ed. 2005). *See also, e.g.*, LEV VYGOTSKY, THOUGHT AND LANGUAGE (1962).

134. The education theory concept of scaffolding refers to allowing a student to learn for herself while providing assistance to ensure her success. *See* KATHLEEN HOGAN & MICHAEL PRESSLEY, SCAFFOLDING STUDENT LEARNING: INSTRUCTIONAL APPROACHES AND ISSUES 9 (1997).

135. Users may develop a type of commercial identity that will evolve away the perceived "specialness" of technology contracting.

more connected than any other node.[136] Enforcement of the understanding of the User Agreement held by any node in an ideal system is equally likely to reflect the understanding of every other node. Unfortunately, this ideal universe cannot exist because of differences in sophistication and power among various consumers and content providers.

FIGURE B: CONSENT IN AN IDEAL SYSTEM



As described in the preceding sections, user consent, ostensibly demonstrated through User Agreements, is the lynchpin between the law of intellectual property and computer intrusion. Similarly, as demonstrated by Figure A, the structure of our current consent architecture does not resemble the ideal structure of consent in Figure B. It is not the case that enforcement of any node's understanding of a User Agreement is equally likely to reflect the understanding of any other node. Therefore, the commonality of understanding may need to be legally generated. This section proposes one possible legal approach to mitigate the doctrinal noise in a manner sensitive to the three sets of ecological concerns set

136. In random networks, at the peak of the distribution, one assumes that a majority of nodes reflect the same number of links; nodes that have a significant difference in the number of links are an aberration. *See, e.g.*, BARABASI, *infra* note 156, *at* 55–72.

forth above. This section advocates objectively defining digital consent through generating a standard contingent on empirical testing of the legal usability of agreements on real consumers.

A. Constructing the "Reasonable Digital Consumer" in the Context of Digital Contracting

As previously described in Part II, the law of digital contracting currently relies solely on objective indicators of consent in determining whether digital contracts are binding on users. Case law to date has examined issues relating to procedural fairness in generating an objective basis for believing consumer consent is present, but as yet has not adequately explored issues of consent triggered by the substantive fairness of contractual provisions. Meanwhile, the most common defense that arises in cases involving controversial technology contracting situations, such as those surrounding the User Agreements relating to invasive DRM, is that the consumer consented to the DRM though the User Agreement.[137] A court is then left to determine whether the User Agreement is enforceable and whether the consumer consented to the installation of the DRM.

Deciding whether consumer consent existed in a particular case can be accomplished through legally and empirically constructing a "reasonable digital consumer" standard. Specifically, through borrowing legal methods of constructing "reasonable" consumers from trademark law[138] and

137. User Agreements frequently contain the following types of terms, some of which may ultimately be deemed unconscionable: an explicit assent by user to be bound by use at own risk; incorporation of other product specific agreements by reference; an intellectual property rights retainer for the website owner or services provider; a limited intellectual property license to use for the user; an assignment of rights by the user in communications with the website; a disclaimer of any representations and warranties in connection with the website or services; a disclaimer of responsibility for third party content; a limitation of liability; a user indemnification for damages arising out of the user's use of the site or poor security behaviors such as password management; a prohibition on linking; a conduct code for the website; a securities disclaimer relating to forward looking statements and updating of content; a securities disclaimer stating no offer of securities is made through the site; user representations and warranties related to security of passwords, user warranties related to providing of notice about problem with password or leakage of data; a termination provision with no notice by the content owner; a choice of law provision; a choice of venue and consent to jurisdiction provision; a severability provision; a provision stipulating unilateral amendment of terms by the content owner; a provision stipulating unilateral amendment of site content on no notice; an integration clause; a provision providing for selective enforcement of remedies under the agreement by the content owner; and a prohibition on user assignment of rights and obligations under the User Agreements.

138. For discussion of trademark harms and the manner in which they are adjudicated by courts, see, e.g., Margreth Barrett, *Internet Trademark Suits and the Demise of "Trademark Use,"* 39 U.C. DAVIS L. REV. 371 (2006); Irene Calboli, *Trademark Assignment "With Goodwill": A Concept Whose*

importing them into the law of digital contracts, a standard for objective consent can be crafted. In this manner, objective consent becomes more readily determinable by courts and business entities alike, possibly triggering implied protections of neglected sections under the DMCA. This method of constructing objective consent also leverages the dynamic emergent processes already visible in the law and in digital contracting practices today.[139]

A consent regime predicated on an empirically constructed reasonable consumer would be built as follows. When a company drafts a new User Agreement, it would conduct a "legal usability test"[140] to ensure predictable outcomes in enforcement of the User Agreement. Many companies will not necessarily perceive this as unduly burdensome because they already run usability tests for their products on a regular basis.[141] For example, a company selling dancing pig screensaver downloads would likely conduct empirical tests with users to determine whether the user can successfully navigate the user interface and download the new dancing purple pig screensaver. During this product usability test, the company would add in a series of questions and exercises to test whether the users can also successfully navigate the user interface to read

---

Time Has Gone, 57 FLA. L. REV. 771 (2005); Stacey L. Dogan & Mark A. Lemley, *What the Right of Publicity Can Learn from Trademark Law*, 58 STAN. L. REV. 1161 (2006); David J. Franklyn, *Debunking Dilution Doctrine: Toward a Coherent Theory of the Anti-Free-Rider Principle in American Trademark Law*, 56 HASTINGS L.J. 117 (2004); Jane C. Ginsburg, *The Author's Name as a Trademark: A Perverse Perspective on the Moral Right of "Paternity"?*, 23 CARDOZO ARTS & ENT. L.J. 379 (2005); Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY L.J. 507 (2005); Laura A. Heymann, *The Birth of the Authornym: Authorship, Pseudonymity, and Trademark Law*, 80 NOTRE DAME L. REV. 1377 (2005); Daniel Klerman, *Trademark Dilution, Search Costs, and Naked Licensing*, 74 FORDHAM L. REV. 1759 (2006); Gideon Parchomovsky, *On Trademarks, Domain Names, and Internal Auctions*, 2001 U. ILL. L. REV. 211; Jennifer E. Rothman, *Initial Interest Confusion: Standing at the Crossroads of Trademark Law*, 27 CARDOZO L. REV. 105 (2005).

139. Through creating a reasonable digital consumer standard that evolves as consumer knowledge evolves, a sustainable standard can be crafted in a manner similar to the way evolutionary standards have been crafted in other areas of law, such as trademark law.

140. When I speak of legal usability I do not merely mean an expert counting numbers of syllables or words. I refer to a statistically significant sample of consumers interacting with an actual contract and attempting to derive meaning from it. For a discussion of early "usability" tests of counting syllables, such as the Flesch test, see, e.g., E.B. WHITE, THE SECOND TREE FROM THE CORNER 166 (1954).

141. Usability testing of user interfaces is an almost universal practice in the software industry. The major critiques of usability testing include the assertions that results are inaccurate because users are paid for participation, know they are being studied, and are generally using a machines that are not their own in the study. For a discussion of usability testing, see, e.g., CAROL M. BARNUM, USABILITY TESTING AND RESEARCH (2001); JOSEPH S. DUMAS & JANICE C. REDISH, A PRACTICAL GUIDE TO USABILITY TESTING (1999); JAKOB NIELSEN, USABILITY ENGINEERING (1994); JEFFREY RUBIN, HANDBOOK OF USABILITY TESTING: HOW TO PLAN, DESIGN, AND CONDUCT EFFECTIVE TESTS (1994).

and understand the User Agreement. In this way, companies would begin to view the User Agreement as an integral part of the product and worry about its functionality to the same extent they worry about the functionality of the product itself. These usability tests, if conducted thoroughly, would demonstrate which provisions and User Agreements consumers regularly fail to understand. Under this framework, a particular incentive exists to ensure that users understand provisions allowing a content provider to engage in behaviors otherwise prohibited by law. If this usability tested User Agreement is subsequently challenged in court, a finder of fact only needs to examine the validity of the usability test and its results, rather than constructing a theoretical "reasonable consumer" from the mind of the judge. If no usability test was done preemptively at the time of the litigation, the court would order a test be performed by a court-appointed expert.

This construction of a reasonable consumer to determine liability is not entirely novel. Trademark law has long used empirical consumer testing in litigation to ascertain whether the likelihood of consumer confusion exists. In a trademark case, if a plaintiff alleges that consumers were confused by the similarity between the plaintiff's mark and the defendant's mark, the plaintiff has the burden of providing evidence showing a likelihood of confusion.[142] The manner in which plaintiffs frequently demonstrate this likelihood is through presenting empirical survey evidence, which shows that consumers were actually confused by the relationship between the two marks.[143] A showing of actual confusion through empirical survey evidence is deemed strong evidence toward finding infringement.[144] Conversely, a defendant's demonstration that empirical survey evidence shows consumers were not confused by the relationship of two marks strongly refutes a plaintiff's allegation of confusion and infringement. This model can be adapted to the digital contracting context.

Specifically, in the context of security-invasive DRM, one can obtain empirical evidence to demonstrate whether a reasonable consumer was confused or is likely to have consented to the installation of the DRM in

142. *See, e.g.*, Zimmerman v. Nat'l Ass'n of Realtors 70 U.S.P.Q.2d 1425 (T.T.A.B. 2004), *available at* http://www.uspto.gov/web/offices/com/sol/foia/ttab/other/2004/92032360.pdf.

143. For example, in a famous cancellation petition before the United States Patent and Trademark Office Trial and Appeal Board regarding the servicemark "Realtor," a battle of empirical studies occurred with the board assessing the validity and strength of each. *See id.*

144. *See* Thane Int'l, Inc. v. Trek Bicycle Corp., No. 00-55293, 00-55599, 2002 U.S. App. LEXIS 18344, at *13 (9th Cir. Sept. 6, 2002). The U.S. Court of Appeals for the Ninth Circuit has held that a survey demonstrating actual consumer confusion may be sufficient to prove a likelihood of confusion as a matter of law. *Id*. Likelihood of confusion is a key element of proving infringement. *Id*.

question. Provided that this empirical evidence is collected and analyzed in accordance with generally accepted social science research methods, results can reveal the likelihood that a reasonable consumer was able to find and understand the User Agreement allegedly authorizing the DRM installation. The study would be performed by asking a sample group[145] of consumers a series of questions probing their understanding of the User Agreement at issue. The questions would examine the following subjects. Was the user presented with the User Agreement before the security-invasive DRM installed itself? At the time the user first used the product accompanied by security-invasive DRM, was the user aware that he had entered into a contract involving the DRM? Was the user expressly advised that security-invasive DRM may potentially jeopardize the security of the user's system, and did the user understand what this meant? Was the extent of the risk explained? Was the DRM-particular behavior being litigated explicitly authorized or understood by a reasonable consumer through the User Agreement? For example, do users understand that terms such as "a small proprietary software program"[146] when used in a User Agreement, unless clearly defined,[147] can be referring to rootkits and other malware, types of code generally used by hackers that harm security? If the answer to these types of questions is yes, then consent is deemed to exist and the User Agreement is deemed enforceable. If, however, one or more of these key elements does not exist, the contract is deemed unenforceable on the basis of an absence of meaningful consent.[148]

---

145. In empirical research, the larger the sample and the more carefully the sample is constructed, the more generalizable the results. Samples with fewer than thirty subjects are usually deemed flawed. For a discussion of proper sampling methodology see, e.g., WILLIAM G. COCHRAN, SAMPLING TECHNIQUES (1977); PAUL S. LEVY & STANLEY LEMESHOW, SAMPLING OF POPULATIONS : METHODS AND APPLICATIONS (2d ed. 1991).

146. This language was used in Sony's User Agreement to describe the rootkit installed by Sony CDs on user machines that created a security hole on user machines and allowed hackers to take control of these machines. *See infra* note 148.

147. For a defense of textualist contract analysis, see Schwartz & Scott, *supra* note 85, at 568 n.50 (proposing textualism for interpretation of contract between commercial parties). *But see* Steven J. Burton, *Default Principles, Legitimacy, and the Authority of a Contract*, 3 S. CAL. INTERDISC. L.J. 115, 139 (1993) ("[E]ven if efficiency justified enforcing deals the parties made, the justification for enforcing a deal made by the parties is not a justification for enforcing a deal they did not make."); Michael P. Van Alstine, *Of Textualism, Party Autonomy, and Good Faith*, 40 WM. & MARY L. REV. 1223, 1224–28 (1999) ("[M]odern celebration of the authority of text threatens to consign the doctrine of good faith to an inconsequential marginal note in the law of contracts. . . . [E]very expressly conferred contractual power is presumptively absolute and unrestricted.").

148. Using the language of one of the Sony-BMG User Agreements involved in litigation, a usability test would question whether a reasonable user understands that the following language

Intellectual property holders draft User Agreements solely for the purpose of obtaining additional benefits over and above what they already possess in intellectual property law. A finding of inadequate consent to a User Agreement would mean that the intellectual property owner is not entitled to the additional benefits carved out in the User Agreement, but the owner still retains all those rights explicitly provided under intellectual property law. As such, in the event that a User Agreement is deemed unenforceable, content owners would not be stripped of all intellectual property protections. The only benefits content owners would be denied are those additional benefits sought through contracts that were not theirs already by virtue of law. On the consumer side, a finding that a User Agreement is unenforceable due to lack of consent opens the door to possible civil or criminal litigation against the intellectual property holder. Without consent, as was previously discussed, security-invasive DRM can be legally reclassified as an actionable computer intrusion for installation of code on a third party machine.[149]

---

authorized installation of a rootkit that could be exploited by third parties to remotely control the user's machine and collect data from the user's hard drive:

> As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program (the "SOFTWARE") onto your computer. The software is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the digital content. Once installed, the software will reside on your computer until removed or deleted. However, the software will not be used at any time to collect any personal information from you, whether stored on your computer or otherwise.

See Sony User Agreement, http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=136855 (last visited Mar. 2, 2006). Further, the language in the limitation of liability in this EULA limits consumer recovery for any bad acts of Sony's "small proprietary software" to $5 in some states: "IN ANY CASE, THE ENTIRE LIABILITY OF THE SONY BMG PARTIES, COLLECTIVELY, UNDER THE PROVISIONS OF THIS EULA SHALL BE LIMITED TO FIVE US DOLLARS (US $5.00)." *Id.*

149. A practical difficulty in civil and criminal suits resulting from unenforceable User Agreements under current computer intrusion law is the assessment of damages. The ECPA and the CFAA have been plagued by difficulty of quantifying damages for computer intrusions. For example, in the context of intentional violations, under the CFAA no statutory damages are available and courts vary in the ways they assess damages. Under § 1030(g), a private right of action is available for any victim who suffers "damage or loss" due to a violation of the Act. 18 U.S.C. § 1030(a) (2000). Damage is defined under § 1030(e)(8) of the statute and requires either (A) losses aggregating $5,000 during any one-year period to one or more individuals; (B) impairment to medical diagnosis or treatment; (C) physical injury to any person; or (D) a threat to public health or safety. § 1030(5)(a). Many plaintiffs have encountered problems meeting the $5,000 threshold for damages. Two schools of thought exist regarding the proper interpretation of the CFAA damage requirements in § 1030(g) creating a private right of action for anyone suffering "damage or loss." While "damage" is defined and requires plaintiffs to meet a threshold of $5,000, the term "loss" is not clearly defined, causing courts to struggle with calculating damages. Courts have also differed as to whether damages to multiple plaintiffs in a class action lawsuit can be aggregated in order to meet the $5,000 threshold and the extent to which loss of goodwill can be included in calculations. But under the ECPA, minimum statutory damages of $10,000 are available for violations of Title I and $1,000 for violations of Title II,

B. Reducing "Noise" in the System: The Legal and Practical Benefits of Legal Usability Testing and the Reasonable Digital Consumer Standard

Introducing legal usability testing and the "reasonable digital consumer" standard into contract law provides six principal legal and practical benefits to ease the current legal noise in our system. First, such an approach offers minimum disruption to the trend in prior digital contract case law toward objective, rather than subjective, determinations of consent. Simultaneously, it pushes case law toward the contractual ideal of the meeting of the minds. Second, it acknowledges that consumers' understanding of contract terms is an emergent construct; it changes in response to external social influences over time. Third, constructing an objective consent standard through the empirical legal usability testing of contracts improves businesses' ability to engage in effective legal risk management planning. To increase the likelihood of enforceability of agreements, businesses can choose to usability test them in advance of litigation to mitigate legal risk and re-test them when terms are changed. Fourth, this approach neither patronizes consumers as incapable of consent nor does it leave them without recourse for draconian and unconscionable contracts, or for code that harms the security of their systems. Fifth, an objective construction of consumer consent controls for the drastically varying levels of technological savvy among judges. Finally, this regime leverages the naturally occurring structures of organization in both the construction of legal consent and the way that legal forms are transmitted among the lawyers who draft User Agreements.

---

in part because of the difficulty of quantifying damages for security breaches. *See, e.g.*, 18 U.S.C. § 2520. However, a debate exists in the courts whether courts have the discretion not to award any damages in some cases. *See, e.g.*, Culbertson v. Culbertson, 143 F.3d 825 (4th Cir. 1998) (holding that courts have discretion not to award damages); Reynolds v. Spears, 93 F.3d 428 (8th Cir. 1996); Nally v. Nally, 53 F.3d 649 (4th Cir. 1995) (holding that courts have discretion not to award damages). *But see* Desilets v. Wal-Mart Stores, Inc., 171 F.3d 711, 713 (1st Cir. 1999) (suggesting in dicta that courts must award damages); Rogers v. Wood, 910 F.2d 444 (7th Cir. 1990) (holding that courts must award a minimum of $10,000 in statutory damages per violation); Menda Biton v. Menda, 812 F. Supp. 283 (D.P.R. 1993) (holding that courts must award damages). However, in this case of security-invasive DRM, perhaps we can seek guidance from the Copyright Act itself. For example, if Congress were to pass a statutory corollary allowing the minimum copyright statutory damages to apply to each instance of invasive DRM activity, the issue would be resolved. By using the statutory damages amounts specified by the Copyright Act as a basis for DRM intrusion damages, the issue of damages can be resolved.

1. Consonance with the Trends of Prior Digital Contracting Case Law and Moving Toward the Contractual Ideal

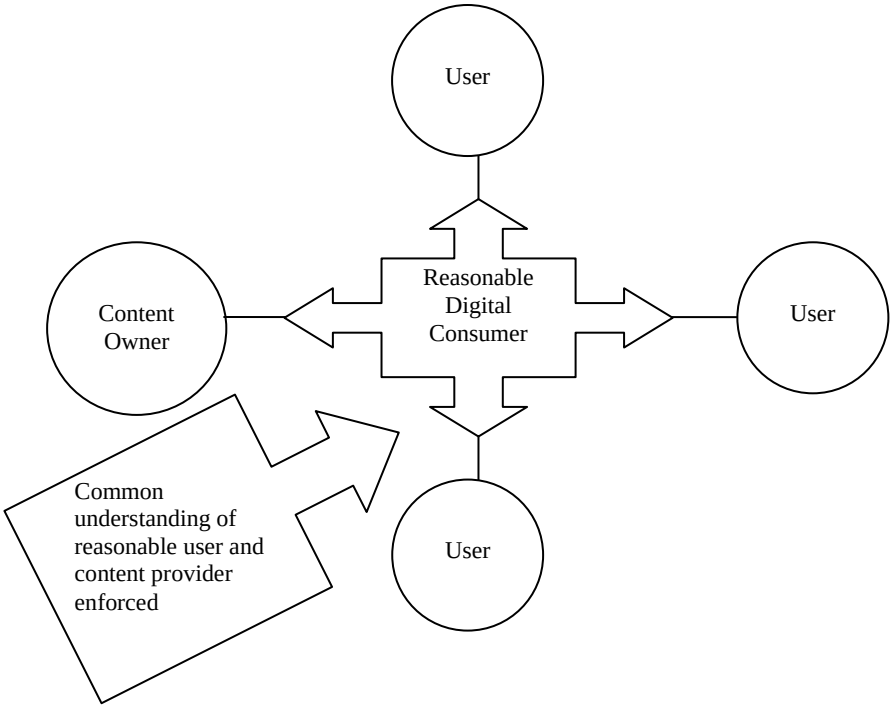
To date, digital contracting case law has indicated a clear preference for objective constructions of consent over subjective constructions of consent. This preference arises in part because of the difficulty in determining subjective consent in digital context. An objective standard strikes a better balance between customization and standardization than a standard subjective to each transaction could offer. Similarly, language of "reasonable" consumer behaviors is doctrinally pervasive in both contract law and intellectual property law. Generating a reasonable digital consumer standard-of-consent continues these trends, resolving doctrinal tensions with minimal disruption to the preexisting system.

Theoretically, adopting a reasonable digital consumer standard eliminates the deficit of a meeting of the minds set forth in Figure A. It also more closely approximates Figure B, the ideal structure of consent, than does our current regime. As illustrated in Figure C below, a reasonable digital consumer standard merges the subjective contractual interpretations of all parties to the User Agreement, i.e. both content owner and users, into one common objective understanding. It is as if a new person has been added to the contractual relationship, a person that always shares some understandings of both parties. The circles in Figure C represent these parties to the User Agreement and the links between them indicate a common understanding of a User Agreement term. In Figure A, our current legal regime, we cannot ascertain whether a link of common understanding exists between the content provider's and users' understanding of the User Agreement. In Figure C, we are more confident this link exists through the reasonable digital consumer standard. Unlike in Figure A where the content provider's subjective understanding of terms is enforced absent procedural unfairness, Figure C shifts the doctrinal balance from purely procedural concerns to both procedural and substantive concerns. Concern over both procedure and substance has been the hallmark of the traditional unconscionability doctrine.[150] A reasonable digital consumer standard checks the power imbalance between the content owners who draft User Agreements, and the users who are bound by them: User Agreements can assert additional legal rights for content owners only to the extent that reasonable users understand these additional

150. *See* Leff, *supra* note 124.

legal rights have been asserted. A reasonable digital consumer legally generates a fictional "hub" of common understanding of the parties.

FIGURE C: CONSENT WITH THE REASONABLE DIGITAL CONSUMER STANDARD



2. Allowing for Evolution in Consumer Understanding of Digital Consent

The average levels of technology skills change over time within individuals and across cohorts. As different cohorts of users reach contractual capacity, the level of technology skills held by a reasonable digital consumer will also evolve. Adopting a contractual standard of consent predicated on empirical testing of real consumers at a particular point in time ensures that contractual notions of reasonable consumer behavior are closely aligned with the social realities of consumer technological proficiency.[151]

151. This evolution will result in a need to update usability test legal agreements on a regular

3. Facilitating Greater Predictability in Legal Outcomes to Assist in Enterprise Risk Management Planning

The most effective method of mitigating corporate legal risks is a proactive approach creating a process of regular, legal strategic planning. Its goal is to accurately assess legal risks associated with corporate information assets and generate legal feedback loops to mitigate these risks in both the present and future. Therefore, it is likely that many large companies would be willing to usability test their legal documents in advance of litigation; the business certainty these tests would provide facilitates more effective enterprise risk management.

In essence, a usability testing option for technology-mediated contracts translates legal uncertainty into a business risk calculus that companies will be able to understand more clearly than the current legal landscape. To increase the likelihood of enforceability for their agreements, businesses can choose to usability test them in advance of litigation to mitigate legal risk and re-test them when terms are changed. Conversely, if a business wishes to accept the legal risk of entering litigation with a non-usability tested User Agreement, they are accepting a certain quantifiable risk—the loss of all protections in the agreement apart from these intellectual property rights they hold by law. They also will have time-shifted the costs associated with usability testing the contract to the time of the litigation.

4. Protecting Consumers from Security Risks Without Infantilizing Them

Due to the severity of widespread data vulnerability in the United States, teaching users and technologists to protect themselves through legal means is increasingly critical. Currently, many users, even sophisticated users, click "yes" to every box that appears on their screen and download potentially harmful code without reading the accompanying legal agreements or understanding the technological and legal ramifications of their actions. Simultaneous legal and technological user education is necessary to mitigating the epidemics of phishing, malspam,[152] zombie drones, and identity theft. Law and technology must

basis. As terms and consumer understanding changes, the reasonable digital consumer may understand a particular agreement differently.

152. Malspam is spam that exploits security vulnerabilities on a user's PC. *See* Matwyshyn, *supra* note 1.

evolve together and push users to help solve their own security problems. In this way, users' trust in technology, particularly in the internet as a commercial medium, will not be further diminished despite the prevalent and serious security concerns that accompany its use.

Many technologists would turn every PC into a user-proof black box and remove users from the security equation as much as possible. Our current legal regime of technology-mediated contracts, in essence, does the legal equivalent—reasonable users are unlikely to be capable of understanding most User Agreements at present, assuming the users even notice that the agreements exist and govern their conduct. Even if users struggled through a User Agreement allowing security-invasive DRM as currently drafted, users' ability to understand possible consequences of their consent is limited by their own technological knowledge and experience. At this point in the technological development of our society, users need help in defending themselves from overly aggressive code.[153] If average users can understand neither code nor the User Agreements associated with code, their ability to make informed decisions is severely impaired.

5. Correcting for Varying Levels of Judges' Technology Knowledge

This empirically constructed reasonable consumer standard, in essence, leverages tools already used by courts and intellectual property owners. Adopting an empirically generated reasonable digital consumer standard would simplify the lives of judges and smooth out the practical effects of variations of technological knowledge from judge to judge.[154] The reasonable digital consumer standard eliminates the need for a judge to walk through the particular website or application at issue and only requires a judge to determine the credibility of the usability studies entered into evidence. A complicated question of digital consent is thereby

153. For example, the Sony User Agreement includes a provision which is likely to be the provision Sony would allege authorizes the installation of the rootkit, which describes the rootkit as "a small proprietary software program." *See supra* note 148. It is unlikely that a user, even if the user knew what a rootkit was, would interpret this provision to allow for installation of a rootkit and its attendant security risks.

154. These variations in knowledge are discussed in the contract literature as influencing outcomes, particularly in the absence of clear instructions from the parties in the contract regarding how they wish the dispute to be resolved. *See* Eric A. Posner, *A Theory of Contract Law Under Conditions of Radical Judicial Error*, 94 NW. U. L. REV. 749, 754 (2000) (assuming that "parties lack the clairvoyance needed to give courts the proper guidance if a dispute arises, and courts lack the genius that would be needed to enforce contracts properly in the absence of such guidance").

transformed into a typical "battle of experts" scenario, which courts face in numerous other non-technological legal contexts.

Similarly, trademark case law has well-established methods for determining whether a "reasonable" consumer is confused by a particular trademark or practice; these cases employ empirical testing by experts using real consumers. Little new methodology would need to be generated by courts to incorporate a consent construction based on a reasonable digital consumer.

6. Leveraging the Natural Structure of the System—The Scale-Free Nature of Objective Consent and Form Transmission Patterns of Lawyers

Our social system is a complex system. Complex systems are characterized by a large number of similar but independent actors who persistently move, respond, and evolve in relation to each other in an increasingly sophisticated manner.[155] The result of this evolution is a form

155. For various applications of complex systems theory to other legal contexts see, e.g., David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent": Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055 (1998) (arguing that legal theory would be enriched by paying attention to algorithms derived from the study of complex systems in contexts such as competitive federalism and the "patching" algorithm). *See also*, *e.g.*, Erica Beecher-Monas & Edgar Garcia-Rill, *Danger at the Edge of Chaos: Predicting Violent Behavior in a Post-*Daubert *World*, 24 CARDOZO L. REV. 1845 (2003); Brenner, *supra* note 76; Jim Chen, *Webs of Life: Biodiversity Conservation as a Species of Information Policy*, 89 IOWA L. REV. 495 (2004); Susan P. Crawford, *The Biology of the Broadcast Flag*, 25 HASTINGS COMM. & ENT. L.J. 603 (2003); Robert A. Creo, *Mediation 2004: The Art and the Artist*, 108 PENN ST. L. REV. 1017 (2004); Gerald Andrews Emison, *The Potential for Unconventional Progress: Complex Adaptive Systems and Environmental Quality Policy*, 7 DUKE ENVTL. L. & POL'Y F. 167 (1996); Daniel A. Farber, *Probabilities Behaving Badly: Complexity Theory and Environmental Uncertainty*, 37 U.C. DAVIS L. REV. 145 (2003); Thomas Earl Geu, *Chaos, Complexity, and Coevolution: The Web of Law, Management Theory, and Law Related Services at the Millennium*, 66 TENN. L. REV. 137 (1998); Scott H. Hughes, *Understanding Conflict in a Postmodern World*, 87 MARQ. L. REV. 681 (2004); Jeff L. Lewin, *The Genesis and Evolution of Legal Uncertainty About "Reasonable Medical Certainty,"* 57 MD. L. REV. 380 (1998); Patricia A. Martin, *Bioethics and the Whole: Pluralism, Consensus, and the Transmutation of Bioethical Methods into Gold*, 27 J.L. MED. & ETHICS 316 (1999); Thomas R. McClean, *Application of Administrative Law to Health Care Reform: The Real Politik of Crossing the Quality Chasm*, 16 J.L. & HEALTH 65 (2001–2002); Jeffrey G. Miller, *Evolutionary Statutory Interpretation: Mr. Justice Scalia Meets Darwin*, 20 PACE L. REV. 409 (2000); J.B. Ruhl & James Salzman, *Mozart and the Red Queen: The Problem of Regulatory Accretion in the Administrative State*, 91 GEO. L.J. 757 (2003); J.B. Ruhl, *The Co-Evolution of Sustainable Development and Environmental Justice: Cooperation, Then Competition, Then Conflict*, 9 DUKE ENVTL. L. & POL'Y F. 161 (1999); J.B. Ruhl, *The Fitness of Law: Using Complexity Theory to Describe the Evolution of Law and Society and Its Practical Meaning for Democracy*, 49 VAND. L. REV. 1407 (1996); James Salzman, J.B. Ruhl & Kai-Sheng Song, *Regulatory Traffic Jams*, 2 WYO. L. REV. 253 (2002); Daniel S. Goldberg, Comment, *And the Walls Came Tumbling Down: How Classical Scientific Fallacies Undermine the Validity of Textualism and Originalism*, 39 HOUS. L. REV. 463 (2002).

of self-organization in which order in the system forms spontaneously and local rules govern the conduct of each actor. Numerous independent actors, acting in clustered groups,[156] frequently follow local rules[157] and demonstrate increasingly complicated visible patterns of natural organizational behaviors and norms. Legal behaviors can follow this pattern.[158]

One type of network structure that exists in complex systems is a scale-free network structure.[159] Scale-free networks consist of different points or "nodes" in the network, which evidence drastically different levels of connectivity—some nodes are connected to a very large number of other nodes and some nodes are connected to only a few others.[160] In a scale-free network, no typical node exists and the network is composed of a continuous hierarchy of nodes with a few "hubs"[161] and numerous small nodes.[162]

I postulate that both the naturally occurring structure of a legal regime of objective consent—either the one that we currently have or one driven by the proposed reasonable digital consumer standard—in essence generates a scale-free network distribution of first, the meaning of consent, and second, the spread of legal "forms" through our economy due to document sharing behaviors of transactional lawyers.

a. A Reasonable Digital Consumer Standard Generates an Objective "Hub" of Shared Understanding for Both Contract Procedure and Substance

An objective construction of consent aims to find external evidence that courts and businesses can rely on across contractual instances.

156. *See* ALBERTO LASZLO BARABASI, LINKED 49 (2002).

157. For example, outside of User Agreements, online communities often have additional community rules of conduct. *See, e.g.*, AOL Instant Messenger Web Chat Rules & Etiquette, http://www.aol.com/community/rules.html (last visited May 3, 2004).

158. The behavior of complex adaptive systems frequently cannot be accurately predicted and can naturally evolve to a state of self-organization on the border between order and disorder. *See* GARNETT P. WILLIAMS, CHAOS THEORY TAMED 234 (1997).

159. BARABASI, *supra* note 156, at 55–72. By contrast, in random networks, at the peak of the distribution, one assumes that a majority of nodes reflect the same number of links and nodes, and thus a significant difference in the number of links represents an aberration.

160. *Id.*

161. Hubs are nodes with an unusual, disproportionately large number of other nodes connected to them. *Id.* For example, Google is, as of this writing, a hub. *See* Google, http://www.google.com (last visited May 2, 2006).

162. Erdos and Renyi's random network theory, as extended by Watts and Strogatz, asserted that the number of nodes with a particular number of links decreases on an exponential basis, which is a rate of decay that is swifter than the rate predicted by a power law. BARABASI, *supra* note 156, at 56.

Therefore, the broader goal of an objectively based regime of consent is to generate "hubs" of shared understanding of what behaviors equate to contractual consent. The reasonable digital consumer is a legal generation of hubs of shared understanding eliminating the power imbalance between content providers and consumers. Currently, the hubs of (allegedly) shared understanding have been constructed by courts, on the one hand using self-referential bases, i.e., whatever the judge thinks, and on the other hand by enforcing the understandings of companies drafting the User Agreements.

These dynamics have resulted in what is known as a "rich get richer" phenomenon.[163] As I have empirically demonstrated in other work,[164] User Agreements have become progressively more draconian in their terms over time because their authors generated their content, crafting the hubs of understanding through use of form agreements. This behavior evidences a self-reinforcing mechanism of preferential attachment[165] driven by using the most draconian forms available, meaning that drafters tend to gravitate toward the most restrictive language. Meanwhile, the content of User Agreements has frequently been enforced by courts. Courts have been focusing their attention solely on generating procedural hubs of shared digital behavior to determine if contractual consent has occurred, and have ignored concerns over content. These two concerns should be taken together to generate a legal hub of common understanding.

Courts have rarely seen a workable alternative option to rampant use of unilaterally generated form agreements in digital contracting contexts. Generating a reasonable digital consumer standard for consent may offer just such an alternative. This new standard creates hubs of understanding, with the critical difference being that the hubs are centered around genuine understandings, both procedural and substantive, of actual consumers. A reasonable digital consumer standard does not use a hypothetical consumer postulated by a particular court, nor does it give undue deference to the one-sided User Agreement forms many companies will continue to use if left unchecked.

---

163. *See, e.g.*, Koen Frenken, *Technological Innovation and Complexity Theory*, 15 ECON. OF INNOVATION AND NEW TECH. 137 (2006).

164. *See* Andrea M. Matwyshyn, *Mutually Assured Protection: Development of Relational Internet and Privacy Contracting Norms*, *in* SECURING PRIVACY IN THE INTERNET AGE (Margret Radin et al. eds., 2008) (forthcoming) (on file with author).

165. For a discussion of preferential attachment, see BARABASI, *supra* note 156, at 86–89.

b. A Reasonable Digital Consumer Standard Leverages Lawyers' "Form Sharing" Behaviors and Would Quickly Spread

Pragmatically, a reasonable digital consumer standard, as embodied by the usability tested forms that reflect it, would slowly permeate the system because of another scale-free network—the scale-free network of form sharing among transactional lawyers. Transactional attorneys often "borrow" forms from each other and use each others' cumulative experience. Particularly in the context of User Agreements that are available online, a transactional attorney will frequently review other attorneys' work as a point of reference before drafting his own User Agreements. Consequently, what develops over time is a network structure with "hubs" of agreements and provisions that look essentially alike. Norms of language and document structure develop that are then reinforced by further sharing and court enforcement. Transactional attorneys seek to use norms to their advantage rather than to go against them when drafting. Consequently, even if only a few influential companies that use digital contracts shift to agreements that reflect usability tested standards, they will be able to instigate the emergence of a new norm in the system over time through lawyers' drafting behaviors. The other "node" companies will follow the lead of the influential "hub" companies.

In this way, the reasonable digital consumer standard leverages the naturally occurring structures of our social system but gently nudges them toward more optimal emergence; it helps guide development of these structures of regulation in a manner that reconciles the noise currently surrounding the construct of digital consent in our system.

CONCLUSION

In its preceding pages, this Article has set forth doctrinal tensions that exist in the meaning of "consent" in technology contracting. It has argued that the policy and legal challenges causing systemic noise in meanings of consent among three bodies of law require reconciliation through a new contracting construct for objective consent. The arrival of security-invasive DRM illustrates the necessity of clarifying the meaning of consent in digital contracting case law.

One possible avenue for building this new consent construct may be the generation of a "reasonable digital consumer." A "reasonable digital consumer" standard can be generated through external empirical means modeled on the manner in which consumer confusion is determined in

trademark case law. This proposal leverages the naturally occurring structures in our complex social system to minimize the noise that currently surrounds doctrinal construction of consent.