HIDDEN ENGINES OF DESTRUCTION: THE REASONABLE EXPECTATION OF CODE SAFETY AND THE DUTY TO WARN IN DIGITAL PRODUCTS

Andrea M. Matwyshyn[*]

I. INTRODUCTION 109

II. HOW DIGITAL PRODUCTS HARM 110
A. *Code Harms* 111
1. Functionality Harms 112
2. Information Security Harms 113
3. A Framework for Risks of Code Harm 115
B. *Lack of Transparency* 118
C. *Lack of Feedback Loops* 121

III. HOW TO WARN ABOUT CODE RISKS 125
A. *Lessons from Prior Technology Regulation* 125
1. Improving Information Parity 125
2. Improving Consumer Control Over Digital Products 127
B. *Lessons from the Duty to Warn About the Condition of Land* 131
1. Reasonable Expectations of Safety: A Duty to Inspect 132
2. Reasonable Expectations of Safety: A Duty to Warn and Protect from Hidden Dangers 133
3. Reasonable Expectations of Safety: A Duty to Repair Promptly 135
C. *The Reasonable Expectation of Code Safety: A Three-Tiered Duty to Inspect, Warn and Repair* 136
1. The Reasonable Expectation of Code Safety 137
2. A Three-Tiered Approach 139
a. Tier 1: Labeling 140
b. Tier 2: Hybrid Labeling and Code Prohibition 142
c. Tier 3: Code Prohibition 142
3. The Consequences to Code Creators and Operators 143

IV. CODE WARNINGS AND THE FIRST AMENDMENT 145
A. *Content Neutrality* 146
B. *Liability for Knowledge of Risk and Failure to Warn* 150
C. *Chilling and Speaker Neutrality* 153

---

* Andrea M. Matwyshyn is an assistant professor of Legal Studies and Business Ethics at the Wharton School at the University of Pennsylvania. The author thanks the Zicklin Center for Business Ethics Research for their support of this project and their ongoing support of her research. The author also thanks Martin Redish, Cem Paya, Marcia Tiersky, G. Richard Shell, Kevin Werbach, Jennifer Chandler, Lilian Edwards, Christopher Marsden, Christopher Yoo, Susan Crawford, and Gerry Faulhaber for their insightful comments and critiques. She can be reached at amatwysh@wharton.upenn.edu.

D. *Compelled Speech* 155

V. CONCLUSION 157

I. INTRODUCTION

This Article explores a seemingly straightforward question: to what extent is a consumer entitled to know how digital products work and the likelihood of digital harm? In previous work, I have explored this question in the context of contract law and consumer consent.[1] This Article approaches the question from a different legal context. Specifically, this Article considers whether a duty to warn should exist in connection with digital products. Even if we assume arguendo that a harmed consumer will have difficulty quantifying actual damages, an independent duty to warn on the part of the digital product creator or operator may still exist.

Part II, focusing on functionality and information security harms, explains the dominant ways that digital products can harm consumers through their code and not their content.[2] Part III reviews existing regulation of digital products. It argues in favor of borrowing the scope of the reasonable expectation of safety and duty to warn owed by possessors of land to their business visitors upon it. Finally, Part III proposes a "reasonable expectation of code safety," along with a three-tiered framework inspired by systems theory and the land-based duty to warn, protect and repair. Part IV further considers the primary challenge against the proposed framework on First Amendment grounds and finds it to fully comport with First Amendment protections. Part V concludes.

II. HOW DIGITAL PRODUCTS HARM

Although digital products come in various forms with assorted hardware and interfaces, they are all ultimately composed of two components: data and code.

Data is stagnant information. Like a newspaper, data is a non-interactive image. However, unlike a newspaper, in order to view, open, close or otherwise interact with data, assistance is required.[3] This

1. In previous work I have explored digital consent and generating a reasonableness standard for digital contracting, particularly in the context of security-invasive digital rights management technology. *See, e.g.*, Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L.R. 529, 530–33 (2007).

2. Code, such as the code in digital rights management software (DRM) or a website, frequently knowingly cripples consumers' existing software and exposes consumers to information security risks. DRM software refers to code used to prevent a user from copying or otherwise using code in ways not intended by the author. For a discussion of legal implications of DRM see, for example, Dan Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537 (2005).

3. For example, a .jpg file is a stagnant image. However, to open a .jpg, code is required. It is this code to open .jpg files that has been previously compromised. *See, e.g.*, Microsoft, *Security Bulletin MS04-028: Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)* (Sept. 14, 2004), *available at* http://www.microsoft.com/technet/security/

assistance comes in the form of code. Code is software that facilitates data use. In other words, data is a type of speech—a picture, a paragraph of text; code is the method of delivery of the speech—the truck with a bullhorn, the pamphleteer on the street corner. The critical difference across digital products is simply the number of layers of code that interact to generate the user's emergent experience.

Although policymakers and scholars frequently consider the impact of data content, rarely do they consider the changing impact of the code underlying the visible data. Stated succinctly, data involves harms that a user can see. For example, through the viewing of a disturbing image, data may cause emotional harms to a user; however, these harms are nothing new. Although technology may facilitate greater exposure to this disturbing content, it is still the individual, under the First Amendment, who engages in self-censorship regarding this content. Code, on the other hand, involves harms that a user cannot see and assess preemptively and therefore, cannot engage in the same self-censorship.

A. *Code Harms*

Digital products and communications became a regular fixture in our lives in the 1990s.[4] At first, code involved relatively transparent harms or was substantially harmless by many estimates.[5] Apart from a relatively brief "cookie scare" in the late 1990s,[6] unwanted emails garnered attention as the primary policy problem. Ten years later, the current code harms to consumers are more serious than a mere inconvenience; they increasingly involve consumers' loss of control and use of their own computers and exposure to information security risks.[7]

Two categories of digital harm appear to have caused the most frustration for consumers: functionality harms and information security harms. Functionality harms refer to consumers' unexpected loss of control and use of their own machines. Information security harms refer to consumers' unwitting exposure to information security crime. Regarding both these harms, an information imbalance exists in favor of

---

bulletin/MS04-028.mspx [hereinafter Microsoft, *Security Bulletin*]. For example, when technologists speak of a ".jpg compromise," what they really mean is that the code used in connection with a .jpg file has been compromised—not the .jpg images themselves.

4. *See, e.g.*, Oscar Cisneros, *ISPs Say Spam Study Full of Fat*, WIRED, June 15, 1999, http://www.wired.com/science/discoveries/news/1999/06/20234.

5. For a discussion of the costs of spam, see, for example, Andrea M. Matwyshyn, *Penetrating the Zombie Collective: Spam as an International Security Issue*, 3 SCRIPTED 370, 370–71 (2006).

6. For a discussion of the cookie scare of the late 1990s, see, for example, STEPHEN NORTHCUTT ET AL., INSIDE NETWORK PERIMETER SECURITY 207 (2003).

7. Matwyshyn, *supra* note 5, at 370–71. In the language of economics, these risks are properly termed negative externalities.

the creators or operators of code. This Article addresses this information disparity.[8]

1. Functionality Harms

Functionality harms occur, for example, when code unexpectedly changes settings and preferences,[9] cripples other programs on the machine,[10] and communicates information about the consumer to remote third-parties[11] without the consumer's awareness of the broadcast information. Although license agreements that accompany products sometimes disclose a portion of these activities and risks, the disclosure is frequently incomplete and incomprehensible.[12] Part of this ambiguity may be intentional on the part of the drafters of these agreements; some of them may believe that by providing transparency to the consumer regarding the code and its function on the consumer's system, the consumer may be provided the knowledge to circumvent the code.

How do these code harms happen in practice? They happen when a user interacts with code that has been intentionally degraded, improperly written, or compromised. For example, a doctor is preparing for surgery and notices that the x-ray images he needs to review appear strangely degraded on his computer.[13] He is not sure why; he later reads

---

8. It is true that perhaps the larger, more difficult and more sizable component of the problems set forth in this Article are the questions concerning the Internet criminality generating the risks. However, both parts of the equation need to be addressed—both the underlying criminality and the issues involving conduct of legal organizations and individuals that exacerbate the risk. This Article starts with the easier of the two.

9. For example, code may change registry keys. Glossary, Antispyware Coalition, Oct. 27, 2005, http://www.antispywarecoalition.org/documents/20051027definitions.pdf.

10. *See, e.g.*, Kyle Orland, *Vista DRM to Slow Down High-End Graphics?*, JOYSTIQ, Dec. 25, 2006, http://www.joystiq.com/2006/12/25/vista-drm-to-slows-down-high-end-graphics.

11. *See, e.g.*, Eric Bangeman, *Microsoft Admits Windows Genuine Advantage Phones Home*, ARS TECHNICA, June 8, 2006, http://arstechnica.com/old/content/2006/06/7017.ars.

12. For example, Sony described its DRM which contained a rootkit to contain "a small proprietary software program" in its end user license agreement. Ed Felton, *SonyBMG and First4Internet Release Mysterious Software Update*, FREEDOM TO TINKER, Nov. 3, 2005, http://freedom-to-tinker.com/blog/felten/sonybmg-and-first4internet-release-mysterious-softwa re-update. Sony did not explain any of the numerous information security risks that accompanied it. *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/. "'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://msl1.mit.edu/furdlog/docs/2005-11-18_apwire_pulling_a_sony.pdf.

13. This example is based on a Windows Vista content protection specification. Andrew Thomas, *Vista Security Spec 'Longest Suicide Note in History,'* INQUIRER, Dec. 24, 2006, http://www.theinquirer.net/inquirer/news/183/1029183/vista-security-spec-longest-suicide-note-in-history.

online that, in order to make it harder to copy movies, his operating system intentionally "downgrades" the quality of all video and audio using code (DRM) if they were not output through certain approved connections.[14] Or perhaps a consumer plays a new CD in her work computer. The consumer does not realize that code (DRM) accompanied the digital music files. In a preemptive step to prevent the consumer from being able to copy the digital files should she attempt to do so, the DRM disables all products on her hard drive with known capability of copying music files. Later that day when she attempts to copy a recording of a meeting she attended in order to distribute it to the attendees, she is unable to operate her sound editing software and cannot understand why. Both of these consumers lost use of their systems for reasons unclear to them but clear to the creators of the code.

2. Information Security Harms

From a consumer perspective, two primary information security harms can arise from the code. First, a consumer's data can be stolen and used for fraudulent activity, including identity theft.[15] Second, a consumer's machine can be harnessed into an organized crime zombie bot army of commandeered computers that can be used to attack targets, including critical infrastructure.[16] Organized crime syndicates have

---

14. *See Vista Copy Protection Is Defended*, BBC NEWS, Jan. 22, 2007, http://news.bbc.co.uk/2/hi/technology/6286245.stm.

15. Identity theft threatens not only individual consumers' finances but also threatens to undermine various social systems for administering benefits in the United States. For example, approximately one in seven adult social security numbers has already been compromised due to data breaches. Press Release, Gartner, Gartner Says Rash of Personal Data Thefts Shows Social Security Numbers Can No Longer Be Sole Proof of Identity for Enterprises (June 5, 2006), http://www.gartner.com/press_releases/asset_153141_11.html [hereinafter Gartner Press Release]. Consequently, these numbers will soon become an unusable method of authenticating U.S. residents for obtaining social services. *See id.*

16. For example, one Polish spam group uses over 450,000 compromised systems, "most of them home computers running Windows high-speed connections" all over the world. *See, e.g.*, Ciphertrust, http://www.ciphertrust.com/resources/statistics/zombie.php (last visited August 16, 2006). The black market in security-compromised machines is an international market. *See, e.g.*, John Leyden, *Phatbot Arrest Throws Open Trade in Zombie PCs*, THE REGISTER, May 12, 2004, http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/. "The price of these BotNets (DoSNets) was roughly $500 for 10,000 hosts [during Summer 2004] when the MyDoom and Blaster (the RPC exploit worm) first appeared on the scene." *Id.* Non-exclusive access to compromised PCs sold for about five to ten cents each. *Id.* The greatest incidence of zombies is in the EU (26.16 per cent); the United States is second in incidence (19.08 per cent) and China is third (14.56 per cent). *CipherTrust's Zombie Statistics*, CIPHERTRUST, http://www.ciphertrust.com/resources/statistics/zombie.php (last visited Oct. 6, 2009) [hereinafter *CipherTrust's Zombie Statistics*]; *see also, Rise of Zombie PCs 'Threatens UK'*, BBC NEWS, March 22, 2005, http://news.bbc.co.uk/1/hi/technology/4369891.stm. Approximately 250,000 new zombies are identified per day, *see CipherTrust's Zombie Statistics*, *supra*, with approximately 100–150 million total zombies currently in operation, by

begun launching extortion rackets against businesses, threatening them with attacks from zombie drones.[17] In fact, an army of zombie drones could be used to carry out an attack on electrical power infrastructure, disrupting service. According to the CIA, several power outages in multiple cities have been traced to cyberattacks.[18] Therefore, machines within agencies and machines with critical infrastructure roles can inadvertently become controlled as part of a zombie drone army.[19]

For example, perhaps our beleaguered consumer with the new CD with DRM also does not realize that the DRM in question is well-known in the security community to compromise computers. By playing the CD, she also gives hackers access to her employer's network to steal information and control her computer.[20] Perhaps a consumer follows a banner advertisement to a job-seeker website that encourages consumers to deposit their resume in the website's database. Meanwhile, the job-seeker website's operator, unlike the consumer, knew that using the website was not safe because hackers were actively harvesting data from the database with the likely intention of committing information crimes.[21] Or perhaps an email arrives from a

---

some expert estimates, see Tim Weber, *Criminals 'May Overwhelm the Web,'* BBC NEWS, Jan. 25, 2007, http://news.bbc.co.uk/1/hi/business/6298641.stm.

17. Joseph Menn, *Deleting Online Extortion*, L.A. TIMES, Oct. 25, 2004, at A1. This trend is concerning particularly because numerous U.S. federal agencies, including the Department of Homeland Security, have repeatedly failed cybersecurity review of the Government Accounting Office. Declan McCullagh, *Homeland Security Flunks Cybersecurity Prep Test*, ZDNET NEWS, May 27, 2005, http://news.zdnet.com/2100-1009_22-142993.html. According to FBI sources, the Eastern European mafia views sending out emails as its "9 to 5 job." Special Agent Thomas X. Grasso, Jr., Fed. Bureau of Investigation, Address at DefCon 14: Fighting Organized Cyber Crime—War Stories and Trends (Aug. 3, 2006) (audio available at http://www.defcon.org/html/links/dc-archives/dc-14-archive.html).

18. Tom Espiner, *CIA: Cyberattacks Caused Multicity Blackout*, CNET NEWS, Jan. 22, 2008, http://www.news.cnet.com/2100-7349_3-6227090.html.

19. For example, a vulnerability in one software program required only that a consumer visit the attacker's website to allow the attacker to exploit a hole in Internet Explorer and remotely compromise the consumer's machine. Osdir/mail archive, *Vulnerability in Step-by-Step Interactive Training Allows Remote Code Execution (MS05-031)*, *available at* http://osdir.com/ml/security.securiteam/2005-06/msg00062.html.

20. *See* Bruce Schneier, *Real Story of the Rogue Rootkit*, WIRED, Nov. 17, 2005, http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601. US-CERT, part of the U.S. Department of Homeland Security advised consumers not to install software from an audio CD. *See* US-CERT, http://www.us-cert.gov/current/current_activity.html#xcpdrm (last visited May 2, 2006).

21. This example is based on a breach experienced by Monster.com and a compromised banner ad run by The Register. For a discussion of the Monster.com compromise, see, for example, Amado Hidalgo, *A Monster Trojan*, SYMANTEC CONNECT, Aug. 17, 2007, http://www.symantec.com/connect/blogs/monster-trojan. For a discussion of The Register's compromised banner ad, see, for example, Laura Rohde & Paul Roberts, *Worm Hidden in UK Site's Banner Ads*, COMPUTER WEEKLY, Nov. 23, 2004, http://www.computerweekly.com/Articles/2004/11/23/206959/worm-hidden-in-uk-sites-banner-ads.htm.

senator asking for financial support to appeal the result in a contested senatorial election; a consumer follows a link provided in the email to read more about the candidate and donate online. On the day the campaign sent the email, it, unlike the consumer, knew that the website was under attack[22] and compromised. Because consumers visited the campaign website and donated, their credit card data may have been stolen[23] and information criminals may have harnessed their computers into a network of remotely-controlled computers used for organized information crime.[24]

3. A Framework for Risks of Code Harm

This knowledge imbalance between consumers and the creators and operators of code about functionality and information security harms hidden in code can be encapsulated by borrowing a framework from early information theorists Claude Shannon and Warren Weaver.[25] Any information transmission, in this case data tethered to code, includes six elements: 1) a source; 2) an encoder; 3) a message; 4) a channel or

22. Three types of attacks are possible: breaches of confidentiality, integrity, and availability. As used in this example, "attack" refers to a breach of confidentiality. Confidentiality violations refer to breaches where private data is accessible to unauthorized consumers. Integrity violations refer to violations where data is altered by unauthorized parties. Both confidentiality and integrity violations can result in the types of attacks leading to user harm. Availability attacks cannot. An example of an integrity attack was the recent alteration of John McCain's MySpace page by someone unaffiliated with the campaign in which an "official" message reversing the Senator's position on gay marriage was posted. Michael Arrington, *John McCain's MySpace Page "Enhanced,"* TECHCRUNCH, Mar. 27, 2007, http://www.techcrunch.com/2007/03/27/john-mccains-myspace-page-hacked/; *see also Lieberman Campaign Website Hacked?*, HOTLINE, Aug. 7, 2006, http://hotlineoncall.nationaljournal.com/archives/2006/08/lieberman_campa.php. Attacks against availability refer to rendering a service or system inaccessible. For a discussion of availability attacks, see, for example, Eric Cole & Sandra Ring, INSIDER THREAT: PROTECTING THE ENTERPRISE FROM SABOTAGE, SPYING, AND THEFT 357 (2006).

23. This example is based on the data breach experienced by the campaign of former Senator Norm Coleman in his attempt to contest the election of Senator Al Franken. *See, e.g.*, Elinor Mills, *Coleman Senate Campaign in Donor Data Leak Mess*, CNET NEWS, Mar. 12, 2009, http://news.cnet.com/8301-1009_3-10195434-83.html.

24. This network of computers is comprised of "zombie drones." Zombie drones are security-compromised machines that can be controlled remotely without the user's knowledge for sending spam or other malicious purposes. Thomas M. Dailey, Chair and President, U.S. Internet Service Providers Ass'n, General Counsel, Verizon Online, Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (June 16, 2004), *available at* http://www.usispa.org/pdf/USISPAPutnam.pdf; *Primer: Zombie Drone*, WASH. POST, Feb. 1, 2004, at F3.

25. ALEXIS TAN, MASS COMMUNICATION THEORIES AND RESEARCH 55 (2d ed. 1985) ("[A]n information source selects a message from a set of messages available to him or her. This message is changed by the transmitter into a signal, which is then sent over the channel to the receiver, which changes the transmitted signal back into the message and then sends it on to the destination.").

medium; 5) a decoder; and 6) a receiver.[26]

Source pertains to the creator or operator of the digital product. A source chooses whether to implement functionality limitation in a digital product. Functionality limitation is a popular business strategy for digital product producers, with the DRM industry alone earning around $1 billion in 2007.[27] Similarly, any information security deficits in the creator's or operator's organization—the overall condition of information security of the speaker's websites, databases, and operations—may impact the consumer.[28] Source information risks are prevalent;[29] in 2008, a 47% increase in data breaches occurred,[30] bringing the number of unique consumer records exposed in data breaches to more than 263,000,000.[31] The encoding and decoding processes include risks consumers face related to code[32] chosen by a creator or operator to convey data. If creators or operators choose to employ vulnerable code in data transmission, this choice can exacerbate security risks for consumers.[33]

---

26. CLAUDE E. SHANNON & WARREN WEAVER, THE MATHEMATICAL THEORY OF COMMUNICATION 18–26 (1949). Multiple types of information risks can coexist and overlap simultaneously.

27. Bharat Book Bureau: DRM Market Analysis—Future Directions, *available at* http://www.bharatbook.com/detail.asp?id=70004 (last visited Oct. 5, 2009).

28. Speakers who engage in vigilant information security monitoring of their systems are more likely to catch and patch vulnerabilities quickly in their systems when they occur.

29. More than 300 unique incidents of data compromise in 2006 alone resulted in exposure of more than 74,000,000 individual records of personally identifiable consumer information. *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches, www.privacyrights.org/ar/ChronDataBreaches.htm#2006 (last visited Oct. 5, 2009) [hereinafter A Chronology of Data Breaches]. For example, the list of entities known to have suffered information security breaches in 2006 alone included more than thirty universities, approximately 100 government agencies, more than twenty financial institutions, and two data brokers. *Id.* In particular, data was compromised in 2006 at the Department of Defense (DoD) and a DoD weapons research facility, the State Department, the Federal Trade Commission, the Department of Agriculture, the Department of Veterans Affairs, the Department of Energy, the Navy, the Marines, the Army, the election boards, the Government Accountability Office, the Internal Revenue Service, the Department of Transportation, the Department of Commerce, and the Transportation Safety Administration. *Id.*

30. Peter Dinham, *Data Loss a Growing Concern Says CSC*, ITWIRE, Mar. 15, 2009, http://www.itwire.com/content/view/23823/598/.

31. A Chronology of Data Breaches, *supra* note 29.

32. When I speak of code here, I refer to the choice of a digital medium or format and particular applications.

33. For example, unencrypted communication through a website or email is usually more easily intercepted and corrupted than encrypted transmissions, and courts have found that using certain browser protocols for data transmission exposes sensitive data to greater risk than necessary. In *In re Pharmatrak, Inc.*, the First Circuit determined that the "get method of data" query and transmission exposed consumers of a medical search engine to unnecessary data risks because sensitive data was generated in the URL transmitted by the website to the consumer. 329 F.3d 9, 16 (1st Cir. 2003). For example, email communications written in rich media

Three major consumer security risks are message risks, medium risks, and receiver risks. Message risks describe a defect in a particular message such as sending malicious attachments. An imprudent creator or operator can damage a consumer through unintentionally sending viruses and other forms of malicious code attached to legitimate data.[34] New vulnerabilities are also frequently discovered in code associated with popular file formats,[35] and these vulnerabilities in many cases require little action by the consumer to be harmful.[36] Therefore, medium risks relate to vulnerabilities that arise at the interaction of the message and the network transmitting it. For example, a consumer can click on a link in an email and be redirected to an attacker's website. On that website, the consumer may be tricked into entering information or otherwise harmed.[37] Finally, receiver risks relate to the interaction of

---

formats such as HTML mean that merely opening or reading such an email presents an increased potential for system compromise or at least for significant data collection without the consumer's consent. *See generally* Press Release, Microsoft, Goodbye, Spam: MSN Employs Innovative Technologies, Education to Reduce Unwanted E-Mail (May 8, 2003), *available at* http://www.microsoft.com/presspass/press/2003/may03/05-08msnspamfilterpr.mspx.(discussing the privacy invasive potential of merely opening an email because of web beacons).

34. Even knowledgeable consumers may wrongly believe that a security compromise cannot result from opening an attached Microsoft Word document or an Adobe PDF file. For a description of one possible vulnerability in Microsoft Word, see, for example, United States Computer Emergency Readiness Team, *Vulnerability Note VU#996892*, http://www.kb.cert.org/vuls/id/996892 (last visited Oct. 5, 2009). For a description of one possible vulnerability in Adobe PDF reader, see United States Computer Emergency Readiness Team, *Vulnerability Note VU#689835*, http://www.kb.cert.org/vuls/id/689835 (last visited Oct. 5, 2009).

35. For example, code connected to viewing the .jpg format has been compromised. *See, e.g.*, Microsoft, *Security Bulletin*, *supra* note 3, at Executive Summary. These formerly "safe" attachments now expose consumers to heightened security risks. In other words, merely viewing an image in an email can cause the code associated with the image to take control of a consumer's machine and allow a remote party to use the machine to commit information crimes invisibly to the consumer. Thus, the process of opening .jpg image files has been compromised. *Id.*

36. In fact, although most malicious attachments require that a consumer open a malicious attachment to be compromised, this is not always the case. In some instances, merely opening an email without opening a malicious attachment could trigger a virus. If, for example, a bug in the email application existed or if the email client was configured to execute script automatically, simply viewing a message without opening a malicious attachment could be enough to trigger a virus. *See, e.g.*, *Microsoft Outlook Virus Gripes*, COMPUTER GRIPES, http://www.computergripes.com/Outlook.Viruses.html (last visited Oct. 5, 2009).

37. Hijacking is a common technique used in phishing attacks. This type of attack may be either a URL redirection or a DNS hijacking. For a discussion of why consumers fall victim to phishing attacks, see, for example, Rachna Dhamija, J. D. Tygar & Marti Hearst, *Why Phishing Works*, *available at* http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf (Apr. 27, 2006). Similarly, attacks such as cross-site scripting and cross-site request forgery vulnerabilities, client-side state manipulation, and SQL injections present the next generation of attacks in Web 2.0 where consumers do not realize that the text before their eyes is engaged in invisible conduct behind their backs. Currently, it is estimated that almost 30% of websites try to push malware onto the machines of visitors. Wolfgang Gruener, *29% of Web Pages Host*

the prior elements with the consumer's system—whether information vulnerabilities exist on the consumer's system[38]—and the interactions of the functionality limitations built into the digital product by the source.

Through both their websites and their online advertising, websites and online services subject users to source, encoding and message risks in their code.[39] Shrinkwrap digital products that have an online component[40] or online digital products that require a consumer to also download code locally expose consumers to these same risks as websites, plus additional receiver risks. Even shrinkwrap digital products with no Internet component subject consumers to receiver risks. In each case, an information imbalance exists in favor of the creator or operator: the creator or operator is in the best position to know the risks associated with their digital products *at the point in time when harm to the consumer can be avoided*.

B. *Lack of Transparency*

In addition to the direct risks of code harm set forth above, it can be argued that another less obvious systemic legal risk has arisen due to code harms—a risk to the "white box" system model created by law to warn consumers about dangerous conditions. In software engineering, "white box" and "black box" refer to the level of transparency at the

---

Malware, Says Sophos, TG DAILY, July 25, 2007, http://www.tgdaily.com/content/view/33076/108/.

38. For example, some senders choose to use security vulnerabilities as a means of pushing their communication to consumers. IBM Internet Security Systems, *Security Alert: Vulnerability in Microsoft Windows Messenger Service*, Oct. 15, 2003, http://www.iss.net/threats/156/html [hereinafter IBM, *Security Alert*]. In 2003, a vulnerability was discovered in an application installed by default in all Windows machines that permitted third parties to access an application on the computers of consumers with always-on Internet connections but no firewalls. *Company Fights for Its Pop-Up Rights*, WIRED, Dec. 9, 2003, *available at* http://www.wired.com/techbiz/media/news/2003/12/61532 [hereinafter *Company Fights for Pop-Up Rights*]. Creator or operators began to push communication in the form of pop-up windows to such vulnerable consumers at unspecified times and regardless of whether a browser window was open. *Id.* Apart from consumers' feelings of invasion, harm resulted from highlighting the existence of the vulnerability on these consumers' machines. It allowed for compilation of a list of vulnerable consumers, a list that would have been desirable to information criminals. *See, e.g.*, *id.*; Complaint for Injunctive and Other Equitable Relief at 4, FTC v. D Squared Solutions, LLC, No. 03CV3108 (D. Md. Oct. 30, 2003), *available at* http://www.ftc.gov/os/2003/11/0323223comp.pdf; Robert Lemos, *Spammers Slip Ads Through Windows*, CNET NEWS, Oct. 17, 2002, http://news.cnet.com/2100-1001-962438.html; *see also* IBM, *Security Alert*, *supra*. Windows Messenger Service, which is distinct from Microsoft Corp.'s MSN instant messaging, is an application in Windows 95, 98, NT, 2000, and XP that enables spontaneous network communications from network administrators. *See, e.g.*, Carnegie Mellon University, *Cert Advisory CA-2003-27: Multiple Vulnerabilities in Microsoft Messenger and Exchange*, Oct. 16, 2003, http://www.cert.org/advisories/CA-2003-27.html.

39. *See, e.g.*, *Company Fights for Pop-Up Rights*, *supra* note 38.

40. For example, some shrinkwrap software requires online registration, "phones-home," or includes Internet-based updating features.

processing point, the point where the analysis of input occurs to generate an output.[41] A white box refers to a subsystem where the internal components are visible to the consumer, and the process of input analysis to generate output is clear.[42] Most importantly, the internal processes are fully transparent to the user, and the user understands how everything works.[43] A black box, on the other hand, refers to a process opaque to its consumer.[44] It is a subsystem where no ability to monitor input analysis exists, and the way that the input generates the output is a mystery.[45] In other words, the workings of the black box are not understood by the user.[46]

The traditional legal conception of assessing consumer risk is predicated on transparency to consumers—a "white box". Borrowing First Amendment terminology, this white box model can be called a "marketplace of ideas"[47] where the consumers of products and services assess data regarding these products and services in a process where risks are fully transparent to them. Where these transparencies have not been adequate, the law has created additional duties of disclosure to enable better processing and risk assessment.[48] Securities regulation disclosure,[49] food and drug labeling,[50]dangerous product warnings,[51] "sin" product warnings,[52] real estate settlement disclosure,[53] and notice

41. For a discussion of white versus black box processes, see, for example, Brian Bryson, *Bridging the Gap Between Black Box and White Box Testing*, IBM, June 28, 2003, http://www.ibm.com/developerworks/rational/library/1147.html.

42. *Id.*

43. *Id.*

44. *Id.*

45. *See id.*

46. *Id.*

47. *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting). John Stuart Mill justified free speech by its greater likelihood of generating "the truth." *See, e.g.*, JOHN STUART MILL, ON LIBERTY 45–47 (Oxford Univ. Press 1952) (1859). Alexander Meiklejohn's "democratic self-governance" argument defends free speech as essential to collective self-governance. *See, e.g.*, ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM 118 (Harper & Bros. 1960) (1948). Further evidence of this thinking is found in Justice Brennan's statements where he suggested that the ability to receive information and ideas is "an inherent corollary of the rights of free speech and press" because "the right to receive ideas is a necessary predicate to the *recipient's* meaningful exercise of his own rights of speech, press, and political freedom." Bd. of Educ. v. Pico, 457 U.S. 853, 867 (1982).

48. *See infra* notes 74–91 and accompanying text.

49. For a discussion of securities disclosure regulation, see, for example, Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 155 (2005).

50. For a discussion of food and drug labeling, see, for example, Krista Hessler Carver, *A Global View of the First Amendment Constraints on FDA*, 63 FOOD & DRUG L.J. 151, 152–59 (2008).

51. For a discussion of labeling of potentially dangerous products, see, for example, John C. Monica, Jr., *FDA Labeling of Cosmetics Containing Nanoscale Materials*, 5 NANOTECHNOLOGY L. & BUS. 63, 69 (2008).

52. For a discussion of cigarette labeling, see, for example, Robert K. Hur, *Takings, Trade*

of nonobvious hazards in property[54] are all examples of commercial situations where the law has corrected for information imbalances by requiring additional disclosure. This additional disclosure maintains the consumer's ability to accurately process risks and rewards of potential transactions.[55]

However, this calculus changes when data is accompanied by code. Because the ability of most consumers to obtain information about code is limited and the information is not readily available,[56] the consumer can no longer accurately assess the risks of the data plus code combination. Yet, the two are packaged together or "tethered."[57] Stated another way, the system is shifting toward an opaque "black box"

Secrets, and Tobacco: Mountain or Molehill?, 53 STAN. L. REV. 447, 471–72 (2000).

53. For a discussion of disclosures in the context of real estate settlement procedures, see Todd J. Zywicki & Joseph D. Adamson, *The Law and Economics of Subprime Lending*, 80 U. COLO. L. REV. 1, 60 (2009).

54. For a discussion of the disclosures a land possessor must make to visitors, see Mike Steenson, Peterson v. Balach, *Obvious Dangers, and the Duty of Possessors of Land in Minnesota*, 34 WM. MITCHELL L. REV. 1281, 1283 (2008).

55. Putting this framework in First Amendment terms, because of the transparent, agentic construction of white box information processing we want to preserve, regulating certain topics of speech as inherently too controversial offends our understanding of free speech. *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 391 (1992) (holding unconstitutional a city ordinance banning certain categories of speech when based solely upon the subjects the speech addressed); *see also* Eugene Volokh, *Speech as Conduct: Generally Applicable Laws, Illegal Courses of Conduct, "Situation-Altering Utterances," and the Uncharted Zones*, 90 CORNELL L. REV. 1277 1284 (2005) (arguing that "the distinction [between speech and conduct] . . . should be the one suggested by United States v. O'Brien and the other cases that distinguish content-neutral from content-based speech restrictions: Expression can generally be regulated to prevent harms that flow from its noncommunicative elements (noise, traffic obstruction, and the like), but not harms that flow from what the expression expresses.").

56. Code is protected by copyright, in particular the anti-circumvention provisions of the Digital Millennium Copyright Act. Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323, 331–32 (2004). Further, most users lack skill for circumvention. For a discussion of DMCA and DRM, see *id.* at 326–31 (2004) (arguing statutory limitations to the different means of DRM protection seem necessary); Dan L. Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 538–39 (2005) (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, 609 (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, 6–8 (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, 116–17 (2005) (setting forth a new administrative complaints 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).

57. For a discussion of tethered products, see, for example, JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET: AND HOW TO STOP IT 101 (2008).

model from the consumer's perspective, where consumers can no longer control or fully understand the risks involved in their commercial decisions about digital products. Currently no disclosure regime exists to correct this information imbalance. Nothing warns consumers about potential functionality harms and information security harms of the code before they use the data associated with the code.

In other words, a transparency loss has occurred in the context of digital products.[58] Whereas consumers could previously understand their information risk management end-to-end relatively well, consumers are now limited in their ability to do so because of code.[59] Explaining the shift a different way, using the language of communication theory, this shift represents the arrival of additional "noise" on the channel of communication.[60] On the same channel, the consumer must now process not only the data but also the "noise" of the functionality risks and information security risks in the code tethered to the data.[61]

C. *Lack of Feedback Loops*

Borrowing an insight from systems theory and cybernetics theory about the importance of feedback loops in systems for self-correction,[62]

---

58. For a discussion of transparency, see generally Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885 (2006).

59. For a discussion of the risks of data security breaches, see, for example, Matwyshyn, *supra* note 49, at 136–46. For example, merely opening an email written in HTML can result in security compromise of a machine. For a discussion of various information security risks of data exchanges, see, for example, Andrea M. Matwyshyn, *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy*, 98 NW. U. L. REV. 493, 512 (2004).

60. For a discussion of Claude Shannon and noisy communication channels generally, see, for example, Yochai Benkler, *Some Economics of Wireless Communications*, 16 HARV. J.L. & TECH. 25, 41 (2002) (discussing inverse correlation between the signal to noise ratio and the width of the band of frequencies of electromagnetic radiation that encodes information); Kevin Werbach, *Supercommons: Toward a Unified Theory of Wireless Communication*, 82 TEX. L. REV. 863, 874 (2004) (discussing the relationship between signal spread and interference on other signals and Shannon's capacity theorem, which states that capacity of a communication channel is proportionate to the width of the channel and the transmission power used).

61. *See generally* Jim Chen, *Webs of Life: Biodiversity Conservation as a Species of Information Policy*, 89 IOWA L. REV. 495 (2004); Ellen P. Goodman, *Spectrum Rights in the Telecosm to Come*, 41 SAN DIEGO L. REV. 269 (2003) (discussing government spectrum regulation); C.E. Shannon, *A Mathematical Theory of Communication*, 27 BELL SYS. TECH. J. 379 (1948), *available at* http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf (discussing consumer noise in the channel). For a discussion of Claude Shannon and the role of bits in communication theory, see, for example, Henry E. Smith, *The Language of Property: Form, Context, and Audience*, 55 STAN. L. REV. 1105, 1109–10 (2003).

62. Feedback loops provide essential information to a system to allow for evolution and self-correction. For a definition of and discussion of cybernetics, see ARVID AULIN, THE CYBERNETIC LAWS OF SOCIAL PROGRESS 2–3 (1982); NORBERT WIENER, CYBERNETICS OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE 19–20 (John Wiley & Sons,

one might argue that a feedback loop has already been created to address functionality harms and information security problems. Functionality is presumably described adequately in the end user license agreement accompanying the code, and many states have now passed data breach notification laws requiring notice to consumers whose data has been compromised in an information security breach.[63]

Even assuming that consumers are capable of understanding the legal language of end user license agreements, an assumption which is not entirely clear,[64] the goal of an end user license agreement is to protect the creator or operator, not to provide disclosure and warning to a consumer. One might similarly argue that data breach notices create an adequate feedback mechanism through compelled disclosure[65] and already address the concerns regarding identity theft and information crime highlighted in previous sections of this Article.[66] However, such arguments are incorrect; data breach notification statutes do not create a meaningful feedback loop for system self-correction. Data breach notifications currently cannot address two deficiencies. First, data breach notices come too late to prevent information security harm and do not prevent functionality harm. Second, they cannot teach a consumer how to avoid future harm.

A data breach notification is a notice of potential harm that has already occurred. However, not all breaches of consumer information are discovered. The discovery of a breach may occur months or years after the creator or operator's interaction with the consumer—or never.[67] But assuming a data breach is discovered, statutory time frames

---

Inc. 1950) (1948); American Society for Cybernetics, Definitions of Cybernetics, http://www2.gwu.edu/~asc/cyber_definition.html (last visited Oct. 5, 2009).

63. For a discussion of state data breach laws, see, for example, Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 919–25 (2007) (arguing in favor of creation of a coordinated response architecture and develops the elements of such an approach with a coordinated response agent that oversees steps for automatic consumer protection and heightens mitigation).

64. *See* Matwyshyn, *supra* note 1, at 535.

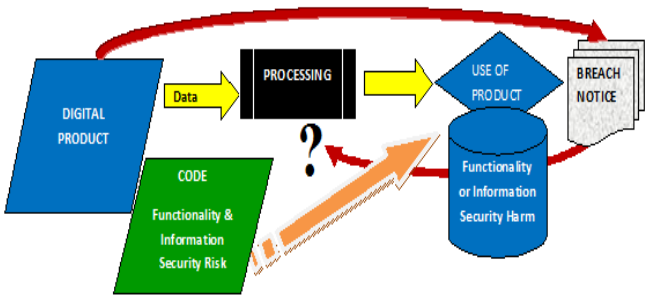
65. For a discussion of forced speech, see generally Martin Guggenheim, *Stealth Indoctrination: Forced Speech in the Classroom*, 2004 U. CHI. LEGAL F. 57 (2004).

66. No specific avenues of legal recourse are available to harmed individuals to create incentives for speakers to implement better security practices in the future. Prior lawsuits have failed due in part to the difficulty in establishing legally adequate causality and damages in connection with a particular data breach leading to a particular incidence of identity theft. *See, e.g.*, Kim Zetter, *ID Theft Victims Could Lose Twice*, WIRED, Feb. 23, 2005, http://www.wired.com/politics/security/news/2005/02/66685. An FTC prosecution or state attorney general prosecution may occur; however, the frequency of such prosecutions is low due to limited agency resources. For a list of recent FTC prosecutions for weak information security practices, see Federal Trade Commission, Commission Actions, http://www.ftc.gov/os/action s.shtm (last visited Oct. 5, 2009).

67. For example UCLA has suffered data breaches which have included data of applicants from at least the previous eight years. *See, e.g.*, Dawn Kawamoto, *UCLA break-in puts data on*

for notice of a security breach give a creator or operator that collects personally identifiable information as much as ten days or longer[68] to report a breach from the time of discovery of a breach. Similarly, although the identity of the creator or operator is irrelevant from the standpoint of analyzing whether a communication will expose the consumer to additional information security risks, a portion of data breach notification statutes cover only for-profit entities.[69] As discussed previously, some of the most severe data breaches involve governmental entities.[70] Although this information is useful in mitigating information security damage after the fact, it does not help to prevent the consumer from unknowingly assuming the risk of harm beforehand, at a point when harm can be avoided. As pictured in *Figure 1*, increased security risks occur simultaneously when interacting with code.

Figure 1: Current Data Breach Feedback Loop Without Additional Warning



800,000 at risk, CNET NEWS, Dec. 12, 2006, http://news.cnet.com/UCLA-break-in-puts-data-on-800,000-at-risk/2100-1029_3-6143003.html.

68. *See, e.g.*, P.L. 1997, c.172, Assem. Comm. Sub. for Assem. No. 4001, 211th Leg. (N.J. 2005), *available at* http://www.njleg.state.nj.us/2004/B.lls/A3500/4001_R1.PDF.

69. *See, e.g.*, GA. CODE ANN. § 10-1-911

70. A case study of a recently compromised jobseeker website provides a clear illustration of the dynamics at issue. Monster.com was aware that hackers using stolen credentials were harvesting data from the Monster jobseeker database. *See Monster.com Admits Keeping Data Breach Under Wraps*, FOX NEWS, Aug. 24, 2007, http://www.foxnews.com/story/0,2933,294471,00.html. These stolen credentials were then used, among other things, to send messages to the harmed jobseekers that purported to be from Monster.com and contained a malicious attachment. *Id.* Monster chose not to notify the impacted consumers until five days after the discovery of the security problem. *Id.*

First, data breach notifications are focused on solely source-related information theft harm; they do not address the information security source harms involving botnet capture, nor do they address functionality harms. Similarly, they do not consider the other points of risks, especially receiver risks. For example, if DRM code attached to a digital product disables anti-virus software and creates a backdoor on a consumer's system, data breach notifications are inapposite.

Second, security breach notifications do not teach consumers how to assess information risk prior to choosing business partners in the future. They also do not empower consumers to protect themselves against future code harms.[71] As set forth in *Figure 1*, even presuming that sophisticated consumers are aware that they make information security decisions when they choose to access data, consumers are currently unlikely to connect the feedback from data breach notices with their ongoing decisions about the safety of interacting with code in the future. Although consumers may sever relationships with breached entities, consumers feel powerless in protecting themselves against data mishandling by other entities; they may begin to suffer from "notification fatigue" as numerous security notices describing past breaches arrive.[72]

However, research indicates that consumers increasingly view creators and operators as having an obligation of stewardship to them.[73] A new approach is needed to buttress the data breach notification regime, one which provides disclosure at a point when consumers can make wiser choices about code risks to functionality and information security.

---

71. Security breach notifications do, however, allow a consumer to sever a relationship with a creator or operator who has exposed the consumer's information in this instance, and other consumers may choose to also avoid that company. *See Three of Four Say They Will Stop Shopping at Stores That Suffer Data Breaches; Most of Those Surveyed Blame a Merchant When They Hear About a Data Breach*, INFO. WEEK, Apr. 12, 2007, http://www.informationweek.com/software/showArticle.jhtml?articleID=199000563&cid=RSSfeed_TechWeb.

72. For a discussion of the possibility of national data breach notification legislation, see, for example, Grant Gross, *Analysis: US Data Breach Notification Law Unlikely This Year*, IDG NEWS SERVICE, May 8, 2006, http://www.macworld.com/article/50709/2006/05/databreach.html.

73. Andy Greenberg, *If Security Is Expensive, Try Getting Hacked*, FORBES.COM, Nov. 28, 2007, http://www.forbes.com/home/technology/2007/11/27/data-privacy-hacking-tech-security-cx_ag_1128databreach.html.

III. HOW TO WARN ABOUT CODE RISKS

As the previous parts of this Article have explained, an information imbalance exists between consumers and the creators and operators of code. This imbalance is not new; it has existed in varying degrees from the early days of the Internet and has, in part, been the subject of several legislative efforts in the area of technology regulation. Although these regulatory efforts have correctly focused on improving information parity and consumer control, they have left gaps.

One way to fill these gaps is by looking to other areas of law for models improving information parity. For example, tort law has crafted a "reasonable expectation of safety" to remedy the information imbalance in the relationship between possessors of the land and business visitors on the land. This reasonable expectation of safety involves a possessor's duty to warn and protect the public and business visitors on land, as well as to promptly repair known conditions that may cause harm.

A. *Lessons from Prior Technology Regulation*

Legislators have struggled with regulating digital products and the Internet. The law has never resolved whether digital products are goods or services, and the tension over this distinction has plagued regulatory efforts.[74] Despite this, regulatory efforts in the realm of digital products to date have focused on improving two areas of concern regarding digital products—(1) improving information parity through data warning or "labeling" approaches and (2) improving consumer control over digital product relationships through data/code prohibitions driven by the identity of the creator or operator.

1. Improving Information Parity

The data warning/labeling model[75] has also been employed in the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the CAN-SPAM Act),[76] the Children's Online Privacy Protection

74. U.C.C. § 2B (Draft 1999), *available at* http://www.law.upenn.edu/bll/zrchives/ulc/ucc2b/2b299.htm.

75. This assumes data that was not itself criminal. Examples of criminal Internet content include content regulated under the Child Online Protection Act, 47 U.S.C. § 231 (2006).

76. 15 U.S.C. § 7705 (2006). It was passed by Congress in 2003, in the wake of perceived technological failure to curb the increasing amounts of email. *Id.* § 7701(a)-(b). A primary goal was to create national uniformity in legal regulation of email. *Id.* As of December 2003, thirty-one states had laws regulating the transmission of email. *See, e.g.*, Paul Queary, *Redmond Man Wins Big in Spam Case*, SEATTLE TIMES, Sept. 11, 2003, at E2, *available at* http://community.seattletimes.nwsource.com/archive/?date=20030911&slug=spam11; Paul Roberts, *EarthLink Wins $16 Million in Spam Case*, PC WORLD, May 7, 2003, http://www.pcworld.com/news/article/0,aid,110627,00.asp. For a discussion of the preexisting relationship exemption of the CAN-SPAM Act, see, for example, Matthew B. Prince & Patrick

Act (COPPA)[77] and the Gramm-Leach-Bliley Act (GLBA),[78] and, most recently, state level spyware[79] and data breach notification statutes.[80] Efforts to improve information parity in digital products began with attempts to create a Uniform Commercial Code (U.C.C.) Article 2B[81] and the Uniform Computer Information Transactions Act (UCITA).[82] UCITA seeks to ensure that all material terms of a digital product transaction are disclosed to a consumer,[83] and it is intended to complement consumer protection law.[84] In general, the CAN-SPAM Act compels truthful sender, subject, and content labeling by requiring that commercial email include the letters "ADV" in the subject line of the email[85] and that sexually explicit materials are clearly labeled as such to warn a recipient about their prurient nature.[86] COPPA, a corporate statute addressing child data collection, and GLBA, a corporate financial data handling statute, also both compel additional data labeling. For example, both statutes require that an operator of a website warn the consumer of the operator's data practices through a notice of privacy practices. Specifically, the statutes require that a

---

A. Shea, *After CAN-SPAM, How States Can Stay Relevant in the Fight Against Unwanted Messages: How a Children's Protection Registry Can Be Effective, and Is Not Preempted, Under the New Federal Anti-Spam Law*, 22 J. MARSHALL J. COMPUTER & INFO. L. 29, 44–45 (2003).

77. 15 U.S.C. §§ 6501–6506 (2006).

78. *Id.* §§ 6801–6809 (2006).

79. For a discussion of spyware, see, for example, Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433, 1434 (2005).

80. For a discussion of state data breach notification statutes, see, for example, Schwartz & Janger, *supra* note 63, at 915.

81. These attempts failed.

82. UNIF. COMPUTER INFO. TRANSACTIONS ACT (UCITA) Prefatory Note (Proposed Official Draft 2001). The approach adopted by UCITA focuses on creating default licensing rules in line with the other provisions of the U.C.C., but it goes beyond Article 2 in buttressing public policy grounds for nonenforcement, prohibiting electronic self-help and excluding enforcement of prohibitions on reverse-engineering in some cases. *Id.*

83. *See id.* §§ 113, 114.

84. *See id.* § 104. However, despite its attempt to eliminate a portion of the information imbalances between creators and operators of digital products and consumers through disclosure and warning of material license terms, UCITA has not gained widespread adoption. Maryland and Virginia are the only states to have adopted UCITA. Ajay Ayyappan, *UCITA: Uniformity at the Price of Fairness?*, 69 FORDHAM L. REV. 2471, 2500 (2001). For a discussion of UCITA, see *id.* at 2472–74.

85. 15 U.S.C. §§ 7704(a)(5)(A), 7710(2) (2006).

86. *Id.* § 7704(d)(1). Similarly, each commercial email must contain information about how the consumer can opt-out from future mailings, in essence warning them that more email will arrive unless they opt out. *Id.* § 7704(a)(5)(A). Each of these requirements represents a type of labeling. The CAN-SPAM Act created a private right of action for Internet service providers (ISPs), but because the CAN-SPAM Act preempts most state spam statutes, in whole or at least in substantial part, it removed private rights of action granted by some state anti-spam statutes. *Id.* § 7707(h).

website collecting child[87] and financial data,[88] respectively, provide a link to a privacy policy which warns consumers about how data is collected, how it is used, with whom it is shared, and contact information for consumer questions.[89] State level spyware statutes require obtaining consumer consent and prohibiting deceptive means when encouraging downloading.[90] Finally, state level data breach notification laws also employ a model based on warning consumers about possible harm arising from a security breach: data breach notification laws require that an entity which suffers a security breach must notify potentially impacted consumers.[91]

2. Improving Consumer Control Over Digital Products

CAN-SPAM,[92] COPPA, and GLBA have additionally adopted an

87. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006). For a discussion of COPPA, see, for example, Andrea M. Matwyshyn, *Technology, Commerce, Development, Identity*, 8 MINN. J.L. SCI. & TECH. 515, 541–48 (2007); Charlene Simmons, *Protecting Children While Silencing Them: The Children's Online Privacy Protection Act and Children's Free Speech Rights*, 12 COMM. L. & POL'Y 119, 120 (2007).

88. For a discussion of GLBA, see Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230, 1241 (2002).

89. *See, e.g.*, 15 U.S.C. § 6803(a) (2006).

90. For a list of spyware legislation by state, see Benjamin Edelman, *State Spyware Legislation*, http://www.benedelman.org/spyware/legislation/ (last visited Oct. 5, 2009).

91. Currently, more than forty states, Puerto Rico, and the District of Columbia have data security breach notification statutes on their books. *Id.*; National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Oct. 6, 2009) [hereinafter NCSL, State Security Breach Notification Laws]. These notification statutes compel speech from entities who have suffered "data breaches" by mandating written notice to the consumers whose data has been impacted. Schwartz & Janger, *supra* note 63, at 915. The legislative intent driving data breach notification statutes involves preventing identity theft and generating a modicum of external accountability for data care. In requiring breached entities to warn consumers that their data has been compromised, legislatures have aimed to mitigate effects of identity theft. *Id.* at 917. By warning likely victims to check their credit reports more zealously, some instances of identity theft can be detected early. These state statutes vary in their definition of what constitutes a breach warranting notice, leaving discretion in some cases to the entity itself to determine whether the breach triggers the statute. For a list of state data breach notification statutes, see NCSL, State Security Breach Notification Laws, *supra*. For a discussion of state data breach notification statutes, see Schwartz & Janger, *supra* note 63.

92. *See, e.g.*, Elizabeth A. Alongi, *Has the U.S. Canned Spam?*, 46 ARIZ. L. REV. 263, 265 (2004) (arguing that because of the international nature of spam, an international approach is most promising and that the efficacy of individual national measures is, as yet, unknown); J. Brian Beckham, Case Note, Intel v. Hamidi: *Spam as a Trespass to Chattels—Deconstruction of a Private Right of Action in California*, 22 J. MARSHALL J. COMPUTER & INFO. L. 205, 226 (2003) (arguing that an exception should be recognized by courts in actions sounding in trespass to chattels involving spam); Shelley Cobos, *A Two-Tiered Registry System to Regulate Spam*, 2003 UCLA J.L. & TECH. 5, 13 (2003) (arguing for a National Registry of Businesses to "serve as a single tracking source for businesses/individuals sending out mass commercial e-mail

approach partially rooted in data/code prohibitions. CAN-SPAM explicitly prohibits dictionary attacks,[93] for example, and consumers can receive unsolicited communications only if the recipient has provided express prior authorization,[94] if the communications are part of an ongoing transaction or relationship,[95] or if the communications are not commercial.[96] Similarly, COPPA prohibits a website operator from engaging in some[97] digital communications[98] with a child[99] without prior, verifiable parental consent. GLBA limits a financial institution[100] from digitally communicating with consumers except to the extent required for completion of a transaction initiated by the consumer or as otherwise authorized by the consumer.

In both legal scholarship and in the courts, digital products' data and the commercial or noncommercial identity of the digital product creator or operator have been the primary focus of the debate, not the code underlying the visible data. In other words, digital products have usually

---

mailings"); Ben Dahl, *A Further Darkside to Unsolicited Commercial E-mail? An Assessment of Potential Employer Liability for Spam E-mail*, 22 J. MARSHALL J. COMPUTER & INFO. L. 179, 180 (2003) (arguing that "the proliferation of unsolicited commercial e-mail in the workplace means extra risk for businesses").

93. Dictionary attacks are a type of attack where all possible combinations of passwords or randomly generated email addresses are used to attempt to gain access to a protected resource or an existing email account. *See* James Grimmelmann, Note, *Regulation by Software*, 114 YALE L.J. 1719, 1743 (2005).

94. For a discussion of the prior authorization in CAN-SPAM, see, for example, Edwin N. Lavergne, *FCC Gives Teeth to the CAN-SPAM Act of 2003*, 1 N.Y.U. J. L. & BUS. 861, 869 (2005).

95. *See* 15 U.S.C. §§ 7702 (2), (17) (2006).

96. *See* Chris Ulbrich, *Spam Law Generates Confusion*, WIRED, Jan. 26, 2004, http://www.wired.com/print/techbiz/media/news/2004/01/62031. To date, the Act has not been challenged on First Amendment grounds, in part because its restrictions are perceived to be easily circumventable and rarely enforced.

97. COPPA and its rules include exceptions to the prior parental consent requirement. It is not required in the following circumstances: when "an operator collects a child's or parent's e-mail address to provide notice and seek consent;" when "an operator collects an e-mail address to respond to a one-time request from a child and then deletes it;" when "an operator collects an e-mail address to respond more than once to a specific request" and subsequently notifies the parent and gives the parent the opportunity to stop the communication before sending another communication to the child; when "an operator collects a child's name or online contact information to protect the safety of a child who is participating on the site" and notifies the parent to provide the opportunity to prevent further use of the information; and when "an operator collects a child's name or online contact information to protect the security or liability of the site or to respond to law enforcement, if necessary, and does not use it for any other purpose." FEDERAL TRADE COMMISSION, DIRECT MARKETING ASSOCIATION, & INTERNET ALLIANCE, HOW TO COMPLY WITH THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT 1, 3, *available at* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.pdf.

98. COPPA covers operators of websites targeting children. *See, e.g.*, 15 U.S.C. § 6502.

99. A child is statutorily defined as a person under the age of thirteen. *Id.* § 6501(1).

100. A "financial institution" is defined broadly in GLBA. *See* 16 C.F.R. § 313.3(k) (2009) (explaining the definition of a financial institution by giving examples).

been analyzed as static data, similar to postal mail advertisement. Although debate over the constitutionality[101] and desirability[102] of restrictions on data has arisen in the scholarly community, the U.S. legal literature has primarily conceptualized the issues around digital products as a limited problem of commercial speech.[103] Meanwhile, courts[104] have addressed challenges to both data labeling and data/code prohibitions cautiously and primarily in a First Amendment context, either failing to find state action[105] or adopting an analysis under

101. *See generally* Credence E. Fogo, *The Postman Always Rings 4,000 Times: New Approaches to Curb Spam*, 18 J. MARSHALL J. COMPUTER & INFO. L. 915 (2000) (arguing that amending the junk fax law to cover Internet solicitations, or providing civil and criminal penalties for spamming will be the most effective method of curbing spam and the least vulnerable to First Amendment challenges); Seth Grossman, *Keeping Unwanted Donkeys and Elephants Out of Your Inbox: The Case for Regulating Political Spam*, 19 BERKELEY TECH. L.J. 1533 (2004) (arguing that political spam can and should be regulated as part of a general measure restricting the use of all unsolicited bulk emails); Joshua A. Marcus, Note, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245 (1998) (arguing that regulating spam comports with the Central Hudson test and is needed because spam is not only annoying commercial speech but is also shifts the advertising cost to the consumer); Marc Simon, *The CAN-SPAM Act of 2003: Is Congressional Regulation of Unsolicited Commercial E-Mail Constitutional?*, 4 J. HIGH TECH. L. 85 (2004) (arguing CAN-SPAM will be upheld as constitutional in light of First Amendment challenges); Mark Sweet, *Political E-Mail: Protected Speech or Unwelcome Spam?*, 2003 DUKE L. & TECH. REV. 1 (2003) (arguing that regulation of commercial spam provides little precedent for regulation of political spam).

102. *See generally* Michael A. Fisher, Note, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUMBIA J.L. & ARTS 363 (2000) (arguing that it is likely that regulation of spam will ultimately take the form of rules regarding the labeling of electronic messages); Eric Goldman, *Where's the Beef? Dissecting Spam's Purported Harms*, 22 J. MARSHALL J. COMPUTER & INFO. L. 13 (2003) (arguing that "most purported harms [of spam] are illusory [and are] already adequately addressed by existing laws or best left to market solutions").

103. *See generally* Richard C. Balough, *The Do-Not-Call Registry Model Is Not the Answer to Spam*, 22 J. MARSHALL J. COMPUTER & INFO. L. 79, 79 (2003) (arguing that the "differences between Internet spam and telephone telemarketing make an 'opt-out' Do-Not-Spam registry an impractical model"); Matthew B. Prince & Patrick A. Shea, *After* CAN-SPAM*, How States Can Stay Relevant in the Fight Against Unwanted Messages*, 22 J. MARSHALL J. COMPUTER & INFO. L. 29 (2003) (arguing in favor of a child protection registry against spam); Cindy M. Rice, Comment, *The TCPA: A Justification for the Prohibition of Spam in 2002?*, 3 N.C. J.L. & TECH. 375 (2002) (arguing that amending the TCPA to incorporate spam is not the most effective method of spam regulation). In the EU, on the other hand, spam has frequently been conceptualized as a privacy question, pitting notions of individual privacy against freedom of trade. For a discussion of EU approaches to spam, see, for example, Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23 (2006).

104. Few communication cases have been fully litigated on First Amendment grounds. At least one settled during FTC prosecution. Ted Bridis, *Small Company Fights Government Claims Over Ad-Blocking Software*, INFO. WEEK, Dec. 10, 2003, *available at* http://www.infor mationweek.com/story/showArticle.jhtml?articleID=16700049.

105. *See, e.g.*, Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 456 (E.D.Pa. 1996).

commercial speech[106] standards set forth in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York.*[107] However, code that causes harm is not a problem limited to commercial creators or operators. As the list of entities who have suffered large scale data leakages set forth in Part II demonstrates, it is frequently nonprofit and governmental creators or operators who expose consumers to additional code harms.[108]

Ultimately, the statutes that currently exist do not explicitly prohibit entities from knowingly or recklessly exacerbating consumer harm from digital products. The three hypothetical situations set forth in Part II involved three situations where a consumer is likely to experience information harm. In the cases of the doctor with strangely degraded x-ray images and the consumer playing a CD at work, a creator or operator does not warn consumers about the risk of functionality harm and information security compromise associated with a shrinkwrap product. In the case of the jobseeker website and the political candidate's website, a creator or operator encourages additional visitors during a time when it has actual knowledge hackers are stealing data from visitors. In still other cases, a creator or operator knows that merely accessing its website will compromise user machines.[109]

---

106. White Buffalo Ventures, LLC v. Univ. of Tex. at Austin, 420 F.3d 366, 374 (5th Cir. 2005); State v. Heckel, 93 P.3d 189, 190 (Wash. Ct. App. 2004).

107. 447 U.S. 557, 566 (1980) (holding that a regulation which completely banned an electric utility from advertising to promote the use of electricity violated the First and Fourteenth Amendments and setting forth a four part test). For example, in *White Buffalo Ventures*, the Fifth Circuit performed a careful *Central Hudson* analysis and held that a state university's anti-solicitation policy prohibiting unsolicited emails was a permissible regulation of commercial speech based on the university's interest in protecting "*user* efficiency." 447 U.S. at 374–76. On the other hand, the court held that the university had no adequate interest in "server efficiency" to warrant a restriction on commercial speech. *Id.* at 376. Consequently, the perspective adopted by the court was that these communications were unwanted speech that nevertheless potentially warranted some First Amendment protection as commercial speech; states were not free to restrict communication without careful consideration and justification. *See id.* at 378. The policy at issue in *White Buffalo* was deemed not preempted by the CAN-SPAM Act. *Id.* at 369. As other cases fall outside the CAN-SPAM Act, it is likely courts will follow the lead of the Fifth Circuit in its *Central Hudson* analysis. In another case, a sender of communication sued AOL alleging that AOL's blocking of communication constituted an infringement of First Amendment rights. Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 438 (E.D. Pa. 1995) The court found in favor of AOL, based on the reasoning that AOL was neither an instrumentality of the government nor performed a traditional government function. *Id.* at 456.

108. For a recent compilation of breached entities, see A Chronology of Data Breaches, *supra* note 29.

109. For example, the Register.com security breach where a banner advertisement contained a malicious payload spread through merely through accessing the Register.com website would provide a possible Tier 3 situation. For a discussion of The Register's compromised banner ad, see, for example, Laura Rohde and Paul Roberts, *Worm Hidden in UK Site's Banner Ads*, COMPUTER WEEKLY, Nov.23, 2004, http://www.computerweekly.com/Artic

Currently, none of these situations are adequately addressed in legislation,[110] and in none of these situations would a reasonable consumer consider the actions he or she was undertaking to be imprudent. But, in each situation, there was a harmful information imbalance between the creator or operator and consumers about the behavior of the code that could prove harmful to the consumer. Therefore, to prevent greater harm to the unassuming consumer, the law must remedy this information disparity lurking in the code underlying digital products.

B. *Lessons from the Duty to Warn About the Condition of Land*

> Once land ownership and agrarian production were primary sources of wealth and income in our economy . . . . Following the industrial revolution, manufactured goods assumed center stage . . . . Our economy has experienced another fundamental change, with information products and services now driving increased productivity and growth. Accompanying this change is a widely diverse and rich array of methods for distributing and tailoring digital information to the modern marketplace . . . .[111]

As the quote above demonstrates, three distinct phases of commercial evolution have occurred in our legal history. The agrarian phase introduced a bundle of regulation connected to land and relationships around land and agrarian products; the second phase addressed manufactured goods; and we have now entered the phase of digital products. In each of the first two contexts—land and manufactured goods—duties to warn have been explicitly created by law to remedy information imbalances. Meanwhile, as discussed previously, technology regulation to date has tried to adopt an iterated approach, focusing on regulating information parity and improving consumer control in digital product relationships. However, information and control imbalances continue to exist between consumers and creators and operators of digital products.

Part of the regulatory challenge arises because digital products exist in somewhat of a hybrid position between the first two legal contexts and contributes new risks. Similar to manufactured products, shrinkwrap digital products and Internet-based digital products such as

---

les/2004/11/23/206959/worm-hidden-in-uk-sites-banner-ads.htm.

110. At most, the jobseeker and political website hypotheticals may trigger a data breach notification several days after the compromise, at a time when the impacted consumers can neither protect themselves nor understand a clear connection between their behavior and the harm.

111. UCITA Prefatory Note (Proposed Official Draft 2001).

websites are used in locations physically remote from the original place of production. However, dissimilar to manufactured products in the stream of commerce, digital products increasingly retain an ongoing connection with the creator or operator. Even many shrinkwrap products require a registration process online to allow the consumer to receive ongoing updates. Website-based digital products involve returning to the same place—a website—repeatedly. Similarly, both land rights and digital product rights simultaneously involve tangible and intangible elements: land rights include visible land and invisible air and underground water; digital product rights include visible data and invisible code. In this way, it can be argued that digital products are now becoming more like land than manufactured products in some, but clearly not all,[112] respects.

The two foci of previous technology regulation—a focus on improving information parity and a focus on consumer control—gain potency when blended with an approach based on the tort duty to warn and protect visitors on land. The insights from the tort rules regarding visitors on land are three-fold. First, possessors of land must provide a reasonable expectation of safety on land held open to the public. Second, possessors have a duty to warn and protect visitors both before they enter and while they are on the land, especially if risks to their safety are not apparent. Third, possessors of land have a duty to repair their land from harming both their invitees and the adjoining land.

1. Reasonable Expectations of Safety: A Duty to Inspect

The law involving both digital products and land includes the legal concept of licensees—people with a limited right to use. In tort law, the term "licensee" includes a subcategory of "invitees."[113] An invitee is a licensee to whom extra care is owed—either a member of the public[114] or a business visitor who is invited to enter, usually for a purpose connected with the business of the possessor of the land.[115] For example, customers in stores are considered invitees.[116] The possessor

112. For example, unlike land, digital products are perfectly duplicable.

113. RESTATEMENT (SECOND) OF TORTS § 330 cmt. a (1965).

114. When premises are held open to the public, those who enter for the purpose for which they are held open are invitees, even though their entry involves no possibility of business dealings with the possessor or of actual or potential economic benefit to the possessor. *See, e.g.*, Price v. Cent. Assembly of God, 356 P.2d 240, 241 (Colo. 1960); Bunnell v. Waterbury Hosp., 131 A. 501, 504 (Conn. 1925); Guilford v. Yale Univ., 23 A.2d 917, 918–19 (Conn. 1942); Howe v. Ohmart, 33 N.E. 466, 467 (Ind. App. 1893); Davis v. Cent. Congregational Soc'y, 129 Mass. 367, 371–72 (1880); Geiger v. Simpson Methodist-Episcopal Church of Minneapolis, 219 N.W. 463, 465 (Minn. 1928); Weigel v. Reintjes, 154 S.W.2d 412, 416 (Mo. Ct. App. 1941); Napier v. First Congregational Church of Portland, 70 P.2d 43, 44 (Or. 1937).

115. RESTATEMENT (SECOND) OF TORTS § 332 (1965).

116. RESTATEMENT (SECOND) OF TORTS § 332 cmt. a (1965). Courts may vary regarding whether customers are classified as invitees who are members of the public or invitees or are

does not need to initiate an official invitation;[117] the mere existence of a store gives the public reason to believe that the shopkeeper desires them to enter for the purpose of looking at goods and potentially buying them.[118]

An invitee enters land and the premises upon it with an implied assurance of reasonable care in preparation for the protection and safety of the invitee[119]—a reasonable expectation of safety. Therefore, an invitee is not required to be on the alert to discover defects. The reasonable expectation of safety obligates the possessor not only to ensure reasonable protection for invitees[120] against possible dangers of which the invitee is unaware,[121] but it also includes a duty to protect the invitee against the risk of harm from activities about which the invitee knows but against which he may reasonably fail to protect himself.[122]

2. Reasonable Expectations of Safety: A Duty to Warn and Protect from Hidden Dangers

As set forth above, a possessor of land is liable to his invitees for harms that violate the invitees' reasonable expectation of safety.[123] The possessor's duty includes inspection[124] of the premises to discover

---

business visitors. *See id.*

117. RESTATEMENT (SECOND) OF TORTS § 342 cmt. b (1965).

118. Whether an invitation has been extended turns on whether a reasonable person would understand the possessor to have expressed, through words or conduct, willingness for the public or a business visitor to enter. RESTATEMENT (SECOND) OF TORTS § 332 cmt. c (1965). The use of the land is often sufficient to determine the possessor's willingness for the public and business visitors to enter. *Id.* Merchants generally believe that the presence of the public for any of these purposes tends to increase their business. *Id.*

119. RESTATEMENT (SECOND) OF TORTS § 332 cmt. a (1965).

120. Invitees are entitled to a heightened duty as compared to other licensees. RESTATEMENT (SECOND) OF TORTS § 343 cmt. d (1965). Other licensees are entitled to expect that they will be placed upon an equal footing with the possessor by disclosure of any dangerous conditions known to the possessor. *Id.*; RESTATEMENT (SECOND) OF TORTS § 343A cmt. B (1965).

121. RESTATEMENT (SECOND) OF TORTS § 341A (1965).

122. *See, e.g.*, Bearman v. Univ. of Notre Dame, 453 N.E.2d 1196, 1198. (Ind. Ct. App. 1983) (finding that the plaintiff who was knocked down by an intoxicated fan in the parking lot after a football game was owed a duty of safety from the university, which was aware that alcoholic beverages were available at football games and that people became intoxicated and threatened the safety of others).

123. RESTATEMENT (SECOND) OF TORTS § 343 (1965).

124. In *Guin v. Brazos Education*, for example, the court focused on the fact that the defendant had followed the proper "process" through written security policies, had done current risk assessments, and had implemented proper safeguards as required by the GLB Act and found no liability for a breach that did occur. Guin v. Brazos Higher Educ. Serv. Corp., Civ. No. 05-668, 2006 U.S. Dist. LEXIS 4846, at *18–19 (D. Minn. Feb. 7, 2006). In the same vein, in *Bell v. Michigan Council*, the court imposed liability where the defendant was aware of the security risk, but did nothing to address it. Bell v. Mich. Council 25, No. 246684, 2005 Mich. App. LEXIS 353, at *12, *15 (Mich. App. Feb. 15, 2005).

possible unknown defects,[125] and, even in the case of a business visitor on residential premises, a duty to warn of these dangers.[126] Similarly, this duty to warn[127] and to reasonably protect invitees against physical harm extends to acts caused by the accidental, negligent, or intentionally harmful acts of third persons[128] or animals.[129]

For example, if a possessor expects or should expect from past experience that it is likely a third-party—either a careless actor or a criminal[130]—may endanger the safety of the invitee, the possessor may be under a duty to take precautions against it and provide reasonable safety, even if it means hiring additional staff.[131] The manner in which

---

125. *See* Dickey v. Hochschild, Kohn & Co., 146 A. 282, 283 (Md. 1929); Stark v. Great Atl. & Pac. Tea Co., 133 A. 172, 173 (N.J. 1926); Maehlman v. Reuben Realty Co., 166 N.E. 920, 921 (Ohio Ct. App. 1928); Durning v. Hyman, 133 A. 568, 570 (Pa. 1926); Kallum v. Wheeler, 101 S.W.2d 225, 229 (Tex. Comm'n App. 1937).

126. *See* Jobe v. Smith, 764 P.2d 771, 771 (Ariz. Ct. App. 1988) (finding liability where a refrigerator repairman was seriously injured in a client's home when he was assaulted by the homeowner's estranged boyfriend and stating that the homeowner had a duty to warn about a condition of the property and rejecting the homeowner's assertion that she had no duty to warn because a business visitor on residential premises is not included among the special relationships imposing a duty to exercise care to protect against harm from others).

127. Even in the case of licensees, rather than invitees, a possessor duty to warn exists regarding hidden perils. *See, e.g.*, Hicks v. Superstition Mountain Post No. 9399, Veterans of Foreign Wars of U.S., 601 P.2d 281, 284 (Ariz. 1979).

128. *Restatement (Second) of Torts* § 344 defines

> [t]hird persons" to "include all persons other than the possessor of the land, or his servants acting within the scope of their employment. It includes such servants when they are acting outside of the scope of their employment, as well as other invitees or licensees upon the premises, and also trespassers on the land, and even persons outside of the land whose acts endanger the safety of the visitor. The Section also applies to the acts of animals which so endanger his safety.

RESTATEMENT (SECOND) OF TORTS § 344 cmt. B (1965).

129. *Restatement (Second) of Torts* § 344 states:

> A possessor of land who holds it open to the public for entry for his business purposes is subject to liability to members of the public while they are upon the land for such a purpose, for physical harm caused by the accidental, negligent, or intentionally harmful acts of third persons or animals, and by the failure of the possessor to exercise reasonable care to (a) discover that such acts are being done or are likely to be done, or (b) give a warning adequate to enable the visitors to avoid the harm, or otherwise to protect them against it.

RESTATEMENT (SECOND) OF TORTS § 344 (1965).

130. The possessor does not have to have a particular third party in mind for the duty to pertain—a general category of individual is enough. Similarly, the possessor does not have to be able to foresee a particular time for the harm to occur; a general knowledge that harm is likely to occur at some point is enough for the duty to pertain. RESTATEMENT (SECOND) OF TORTS § 344 cmt. f (1965).

131. *Id.* The Restatement comment provides the following example:

the harm occurs does not need to be foreseeable; the only question that matters is whether the source of the harm was foreseeable.[132] For example, at least one court has held that a university must provide extra security after sporting events where alcohol is consumed because inevitably drunks will harm people in the parking lot.[133]

In the case of suit for a failure to warn, a plaintiff invitee has the burden of proving that the defendant possessor either knew or had reason to know of the condition, or that by the exercise of reasonable care he would have discovered it. Where the condition is temporary, this burden may require proof that it has existed for a sufficient length of time that exercise of reasonable care would have led to its discovery.[134]

3. Reasonable Expectations of Safety: A Duty to Repair Promptly

The possessor's duty to warn and protect the invitee exists both before the invitee's entry and during the entire time the invitee is on the land. Even after the invitee has entered, a possessor must also warn the invitee about any changes in the condition of the land that will create a risk of harm to the invitee. Invitees are entitled to expect safety not only in the conditions that exist before their arrival but also in the present condition and use of the land.[135]

> At rush hours the passengers upon the A Street Railway Company are accustomed to crowd into the cars in a manner likely to cause injury to some one in the crowd. The A Company fails to provide a sufficient staff of guards to prevent this practice. B, a passenger, is hurt in such a rush, after a single guard has warned him of the danger. The A Company is subject to liability to B.

RESTATEMENT (SECOND) OF TORTS § 344 cmt. f, illus. 1 (1965).

132. For example, in *Carey v. New Yorker of Worcester, Inc.*, the court held that the plaintiff, a patron in defendant's bar, was entitled to recovery when a boy known to be underage and a troublemaker shot him. 245 N.E.2d 420, 422 (Mass. 1969). The court found the defendant to have violated the duty to warn the plaintiff, which existed even though the harm occurred in an unforeseeable manner. *Id.*

133. Bearman v. Univ. of Notre Dame, 453 N.E.2d 1196, 1198 (Ind. Ct. App.1983).

134. *See* J.C. Penney Co. v. Norris, 250 F.2d 385, 386 (5th Cir. 1957); Parks v. Montgomery Ward & Co., 198 F.2d 772, 775 (10th Cir. 1952); Oldenburg v. Sears, Roebuck & Co., 314 P.2d 33, 37 (Cal. Dist. Ct. App. 1957); Frank v. J.C. Penney Co., 283 P.2d 291, 293 (Cal. Dist. Ct. App. 1955); Gold v. Ariz. Realty & Mortgage Co., 55 P.2d 1254, 1254 (Cal. Dist. Ct. App. 1936); Moran v. Gershow's Super Mkts., Inc., 143 N.E.2d 723, 725 (Ohio Ct. App. 1956); F.W. Woolworth Co. v. Goldston, 155 S.W.2d 830, 831–32 (Tex. Civ. App. 1941).

135. *See, e.g.*, Schwartzman v. Lloyd, 82 F.2d 822, 827 (D.C. Cir. 1936); Johnston v. De La Guerra Props., Inc., 170 P.2d 5, 8–9 (Cal. 1946); Donahoo v. Kress House Moving Corp., 153 P.2d 349, 355 (Cal. 1944); Greeley v. Miller's, Inc., 150 A. 500, 501 (Conn. 1930); Rowell v. Wichita, 176 P.2d 590, 597 (Kan. 1947); Dean v. Safeway Stores, Inc., 300 S.W.2d 431, 434–35 (Mo. 1957); Philpot v. Brooklyn Nat'l League Baseball Club, Inc., 100 N.E.2d 164, 167 (N.Y. 1951); Cejka v. R.H. Macy's Co., 155 N.Y.S.2d 565, 568 (Sup. Ct. 1956), *rev'd on other grounds*, 162 N.Y.S.2d 207 (App. Div. 1957), *aff'd*, 149 N.E.2d 525 (N.Y. 1958); Kmiotek v. Anast, 39 A.2d 923, 924–25 (Pa. 1944); Lee v. Nat'l League Baseball Club of Milwaukee, 89 N.W.2d 811, 816 (Wis. 1958).

Similarly, a possessor is not allowed to condone disrepair of the property caused by invitees or even trespassers.[136] Harm that occurs to adjacent properties because of disrepair on the possessor's property is a basis for liability for the possessor.[137] For example, in one case the defendants acquiesced in the use of diversion banks on their land as a raceway for motorcyclists.[138] During heavy rainfall, neighboring land was damaged by a mudslide due to the failure of the damaged diversion banks.[139] Although the harm to the diversion banks on the defendants' property was caused by third parties, the defendants' failure to repair provided a basis for an Iowa court to deem the defendants liable for harm caused on an adjoining property.[140]

These three insights from the relationship between possessors of land and invitees—a reasonable expectation of safety, a duty to warn, and a duty to promptly repair—may prove useful additions to the way we conceptualize harms from digital products. This type of blended approach must start from the premise of mitigating digital harms as consumers experience them, rather than from a focus on the identity of creators or operators or how the harm is technically caused.[141]

C. *Reasonable Expectation of Code Safety: A Three-Tiered Duty to Warn and Repair*

In the subsections that follow, this Article proposes and defends a "reasonable expectation of code safety"—a three-tiered regulatory approach inspired by systems theory[142] and the land-based duty to warn.

---

136. *See* RESTATEMENT (SECOND) OF TORTS § 365 (1965) ("A possessor of land is subject to liability to others outside of the land for physical harm caused by the disrepair of a structure or other artificial condition thereon, if the exercise of reasonable care by the possessor or by any person to whom he entrusts the maintenance and repair thereof (a) would have disclosed the disrepair and the unreasonable risk involved therein, and (b) would have made it reasonably safe by repair or otherwise.").

137. *See, e.g.*, Young v. Marlas, 51 N.W.2d 443, 448 (Iowa 1952); Crow v. Colson, 256 P. 971, 973 (Kan. 1927); Bernard v. Brownell, 173 N.E. 434, 435 (Mass. 1930); McCarthy v. Thompson Square Theatre Co., 150 N.E. 170, 170 (Mass. 1926); Mullen v. St. John, 57 N.Y. 567, 572 (1874); Pearson v. Ehrich, 133 N.Y.S. 273, 274 (App. Div. 1912); Restaino v. Griggs Motor Sales, Inc., 193 A. 543, 544 (N.J. 1937); Smith v. Claude Neon Lights, Inc., 164 A. 423, 425 (N.J. 1933); Klein v. Price, 65 P.2d 198, 199 (Okla. 1936); Pope v. Reading Co., 156 A. 106, 109 (Pa. 1931); Sakach v. Antonoplos, 148 A. 58, 60–61 (Pa. 1929); Hester v. Hubbuch, 170 S.W.2d 922, 927 (Tenn. Ct. App. 1942).

138. Schropp v. Solzman, 314 N.W.2d 413, 414 (Iowa 1982).

139. *Id.*

140. *Id.* at 415.

141. As discussed in Part II.C., data breach notification statutes fall short in part because they are primarily focused on commercial entities, ignoring the identical problems caused by nonprofit and government speakers.

142. Systems theory examines the dynamic information processing and evolution of systems. All systems have common elements of input, output, throughput or process, feedback, control, environment, and goal. *See, e.g.*, Institute for Systems Theory and Automatic Control,

Similar to the land-based duty to warn, the reasonable expectation of code safety remedies the information imbalance between the "invitee" consumers, on the one hand, and the "possessor" creators/operators of digital products, on the other. The reasonable expectation of code safety entails three duties: a duty to inspect, a duty to warn of digital harm, and a duty of code repair.

1. The Reasonable Expectation of Code Safety

As discussed in Part II, data today presents serious non–expressive, incidental risks for the consumer because of tethered code, and these functionality and information security risks arise invisibly when a consumer accesses the data. A serious information imbalance about this code exists between the creators and operators of code and consumers. By creating a preemptive duty to warn, such as the one that exists in the relationship between possessors of land and invitees, consumers can access a strong feedback loop. Thus, consumer protection legislation or regulatory action is needed to address the relationship between consumers and the creators and operators of code who knowingly[143] expose consumers to increased functionality and information security risks.

Borrowing the idea of crafting a reasonable expectation of safety from the land-based regulatory approach explained in the previous section, it is easy to extrapolate the idea of a "reasonable expectation of code safety." Like the reasonable expectation of safety connected with invitees on land, the reasonable expectation of code safety would be composed of three component parts—a duty to inspect code prior to release, a duty to warn of any hidden risks in the code both before purchase and after purchase, and a duty to repair problems with the code promptly.

Prior to the release of code, creators or operators should be prepared to attest that to the best of their knowledge and in accordance with reasonable levels of care, the code is safe for consumer use. This duty to inspect does not require creators or operators to represent and warrant that their code is error-free, only that they have inspected the code to the best of their ability and in accordance with reasonable industry norms. Numerous code tools are available, many at no cost, that enable creators and operators to better inspect their code for obvious flaws.[144] Some

---

Universität Stuttgart, Systems Theory, http://www.ist.uni-stuttgart.de/research/projects/SystemsTheory/ (last visited Oct. 6, 2009).

143. "Knowingly" here can refer to any standard of knowledge determined by a state, provided that liability is not imposed without fault.

144. For example, Microsoft recently released a free tool to help detect and prevent SQL injections. Posting of Ryan Naraine to Zero Day, http://blogs.zdnet.com/security/?p=1336 (June 24, 2008, 13:34 EST).

creators and operators simply choose not to take the time to use these tools in order to "ship" product more quickly.[145] Further, creators and operators should ensure that their code does not contain "legacy" problems of prior versions of code that are known to contain exploitable vulnerabilities, which may have gone undetected and unfixed.

Second, the reasonable expectation of code safety includes a duty by the creators or operators of code to warn of hidden risks and vulnerabilities about which they know or should know in their code, both before the consumer uses it and even after the consumer's first use. Consumers cannot assess the safety of the code before interacting with it, nor can they tell if the code has become unsafe after they have purchased it and started to use it. Most importantly, the creator or operator is in the best position to warn consumers of functionality risks and vulnerabilities and other information risks. This type of warning would dramatically improve the information imbalance between consumers and the creators and operators of code. Conversely, a lack of warning presents a serious policy concern: much like a possessor who encourages invitees, without informing them of the crumbling stairs inside, to enter into his condemned building where no one will hear their cries for help, a creator or operator who encourages consumers to interact with dangerous computer code draws consumers into a situation likely to harm them.

Finally, just as a duty to repair land during the stay of invitees pertains to possessors, so too a duty of code repair can mandate prompt correction of problems in code. Some creators or operators of code wait until the last possible (legal) moment before notifying consumers about data breaches, even if others are harmed in the interim.[146] Similarly, some creators and operators are lackadaisical about fixing vulnerabilities in their code and ignore consumer requests for information about the status of security vulnerabilities.[147] Sometimes they even release patches that exacerbate rather than fix problems.[148] No

145. For a discussion of the pressure to ship, see, for example, CEM KANER, SPECIAL LIBRARIES ASS'N, BAD SOFTWARE 2 (1999), *available at* http://www.kaner.com/pdfs/SLAbadSW.pdf.

146. For a discussion of the Monster.com compromise, see, for example, Hidalgo, *supra* note 21.

147. For example, American Express has been slow to correct security problems on its consumer-facing website and was taken to task by the press. *See, e.g.*, Dan Goodin, *American Express Bitten by XSS Bugs (Again): Card Accounts Still Naked*, THE REGISTER, Dec. 20, 2008, http://www.theregister.co.uk/2008/12/20/american_express_website_bug_redux/. Requests for more information from cardholders regarding the status of the security corrections to the website were ignored by the company. *See* Communication Between Andrea Matwyshyn, American Express Cardholder, and American Express (Jan. 11, 2009) (on file with author).

148. *See* Team Register, *SonyBMG Backtracks on Buggy Bug Fix: Wearing Out the Rewind Button*, THE REGISTER, Dec. 9, 2005, http://www.theregister.co.uk/2005/12/09/sony_mediamax_problems/.

uniform legal approach or business norm exists on the point of fixing vulnerabilities.[149] Through creating a duty to repair code promptly, the risks faced by consumers who continue to use the digital product in question are mitigated.

2. A Three-Tiered Approach

To operationalize the reasonable expectation of code safety proposed above, a state legislature[150] or perhaps the Federal Trade Commission, pursuant to its authority under § 5 of the Federal Trade Commission Act,[151] may adopt an approach composed of three tiers of responses to code that is likely to expose consumers to functionality or information security risk:[152] (1) a labeling approach for known functionality limitations and periods of low-risk vulnerabilities; (2) a hybrid approach of labeling and code prohibition during periods of medium risk vulnerabilities; and (3) a code prohibition approach during the time between discovery and patching of high-risk, critical vulnerabilities.

For information security harms, the tier categorization of vulnerabilities and responses would be determined on a sliding scale basis using an "information security code risk scale" modeled on threat

149. *See, e.g.*, Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7, ¶ 3 (2004) (discussing the application of laws and business standards to hacking).

150. Implementing the information security risk scale approach on the state level brings pragmatic benefits. First, state legislatures tend to work more quickly than Congress in addressing novel problems of law and technology. When Congress acts, harmonization of state statutes results in a lower level of consumer statutory recourse, as demonstrated by the CAN-SPAM Act. *See* 15 U.S.C. §§ 7701–13 (2006) (discussing regulations regarding email). Second, as the history of data breach notification statutes demonstrates, if a large state such as California passes a consumer protection statute impacting online communications, it is likely that this higher level of care will become the new norm of conduct. For example, maintaining a separate website for all California residents and a second website for all residents of other states would generate additional costs and inefficiencies. Finally, waiting for common law to emerge to address information harms is a losing proposition. Even assuming the glacial pace of common law development in this area could be tolerated, unresolved doctrinal questions regarding causation in data harm contexts and calculating damages for information harms would present courts with potentially intractable problems certain to cause disagreements among judges.

151. *See* 15 U.S.C. § 45(a) (2006) (discussing the authority of the Federal Trade Commission).

152. For companies with a *de minimis* number of consumers using their digital products, an exemption should be considered. Similarly, this framework is intended to apply to all creators or operators who receive consideration for their digital products. In other words, an open source product would not fall under this approach, but a "free" software product that comes tethered to advertising software that tracks users would be covered: the tracking in question generates information which constitutes a thing of value obtained in a bargained-for exchange. Further, companies can choose to discontinue products and thereby no longer be held to a reasonable expectation of code safety for that product. However, so long as copies are sold by the creator or operator, the expectation remains and clear notice of impending end of life must be included as a functionality limitation on the product to provide consumers with opportunity to adjust.

model[153] factors derived from norms of the information security industry. These factors would include: (1) the sophistication of the attack, (2) the severity of harm resulting from compromise, (3) the extent of user interaction required for triggering compromise, (4) the extent to which an attack is currently being leveraged or a commoditized exploit is available in the opinion of information security experts, and (5) the number of consumers potentially impacted. During periods of known vulnerability, a creator or operator can be statutorily required to perform an information risk calculus[154] prior to engaging in technology mediated code. For example, assigning a ten point scale to each of the five elements set forth above, the creator or operator would generate a risk score by obtaining an average score of the values for these five categories.[155] An average score under three may trigger a Tier 1 labeling response, an average score between three and six may trigger a Tier 2 hybrid response, and an average score over six requires a Tier 3 code prohibition response until the security vulnerability is fixed.

a. Tier 1: Labeling

The lowest level of protection, warning, and repair involves labeling through a "safety notice." Safety notice labeling should occur in a situation where (1) a digital product is known to cause or is likely to cause functionality harms to other digital products that a consumer may use or (2) information security problems or other risks exist in code, but the threat modeling indicates that the situation is low-severity and does not place consumers in imminent danger. The perspective adopted in the safety notice should be that of the consumer: the information in the notice should enable a consumer using the digital product to reasonably protect herself against known or possible harms.[156] Thus, the key

153. For an in-depth description of threat modeling process, see, for example, Microsoft Security Developer Center, *Threat Modeling*, http://msdn.microsoft.com/en-us/security/aa570411.aspx (last visited Oct. 6, 2009).

154. Statutorily requiring that an individual or entity engage in a risk calculus is not a novel approach. For example, under federal and state securities regulation, public companies are regularly asked to conduct analyses of "materiality" of events and the likelihood of events to impact future earnings. For a discussion of materiality determinations see, for example, Richard C. Sauer, *The Erosion of the Materiality Standard in the Enforcement of the Federal Securities Laws*, 62 BUS. LAW. 317, 317 (2007).

155. The ten point scale for each of the five elements would consist of: sophistication (1 = low, 10 = highly complicated), severity (1 = low, 10 = remote compromise), triggering (1 = extensive interaction, 10 = minimal), urgency (1 = as soon as feasible, 10 = immediately above all other priorities), impact (1 = a negligible number of consumers, 10 = 100% of consumers).

156. For example, if a security issue exists in a browser and a website expects that a sizable portion of their visitors use this browser, the website's safety notice should provide a brief explanation of the urgency of patching the browser and provide a link to assist the consumer in doing so. Or, for example, a website knows that it has become a favorite target of phishing attempts on its customers. This safety notice would also be a place to explain phishing to

question the safety notice answers is: "what would a reasonable consumer want to know about this digital product and its impact on her system and the security of her information?" The presentation of the safety notice should be as consistent as possible across all digital products[157] to help consumers observe and read the notice more readily.[158] It can be divided into two sections—one on source risks and one on receiver risks.

The source risks section would describe information the consumer needs to know about the status of the security of the source. Specifically, two pieces of information are critical: the number of known data breaches the organization experienced in the last year, and whether there is an active patching underway for a vulnerability. In practice, all websites will likely carry safety notices on a permanent basis. Because information security is an ongoing process, websites and the organizations behind them commonly engage in regular system updates and security improvements for noncritical issues.[159] For example, security patches to Microsoft products are released on the second Tuesday of every month.[160] Provided the patches on a particular Tuesday relate to unsophisticated, hard to trigger vulnerabilities that are likely to impact only a small portion of consumers and cause minimal damage, a security notice on a website during the updating period would state "We are currently patching our system." Email, website pages, and other communication should provide clear and conspicuous notice to the consumer that by choosing to interact with the creator or operator prior to completion of these regularly scheduled or other updates, the consumer may be exposed to additional risks. Seeing this notice, a cautious user may choose not to interact with the code and the digital product until such time as the fix is completed.

The receiver risks section of the security notice would explain to consumers the possible consequences to their system of using the digital product, such as degraded images in other programs as the doctor incurred with degraded x–rays, and advise them of any prudent

---

consumers, its dangers, and how to best avoid falling victim.

157. Part of the reason behind consumers' failure to read privacy policies may stem from their extreme levels of heterogeneity in content and presentation.

158. On websites, for example, the presentation could be a link in a yellow box in the upper right hand corner of a website that says "Safety Notice" and links to a notice that informs the consumer why a security issue exists in the way that the consumer may be using the website. The format should be consistent across all websites to enable consumers to train themselves to notice and review these notices. On a shrinkwrap product, a sticker explaining the functionality limitations should be placed in the upper right hand corner of the product.

159. *See, e.g.*, Brian Krebs, *Monthly Microsoft Patch Release Won't Include Word Fix*, WASHINGTON POST, Dec. 8, 2006, http://blog.washingtonpost.com/securityfix/2006/12/monthly_microsoft_patch_releas.html.

160. *Id.*

protections, such as newly released patches to common products. In the context of shrinkwrap products, any product with DRM would carry a safety notice. For example, some shrinkwrap products may create a permanent "phone home" link with their creators and operators after installation. This type of constant data transfer uses the consumer's Internet connection, usurps memory by running constantly in the background, and is likely to increase the likelihood that the computer's machine will run more slowly and that her operating system will crash more frequently. These reasonably predictable interactions should be listed on a safety notice warning sticker on the front of the product; the consumer should be able to review this information prior to purchase.[161]

b. Tier 2: Hybrid Labeling and Code Prohibition

In a situation where the operative threat modeling factors indicate a security problem of medium severity, the creator or operator should refrain from all "pushed" communications. Meaning the creator or operator should operate under a prohibition on reaching out to consumers through new advertisements, email campaigns and the like. Additionally, the creator or operator should conspicuously label with the safety notice described above all "pulled" communications and digital products, such as websites or compact discs, that a consumer may seek out independently. In this way, no new consumers are encouraged into a potentially dangerous situation and those consumers who choose to interact without encouragement are suitably warned of the risks.[162]

c. Tier 3: Code Prohibition

In a situation where threat modeling reveals a critical, severe security issue or an active exploit underway,[163] all communication should stop immediately and the digital products should be removed from consumer access.[164] For example, if merely visiting a website results in immediate compromise of user machines, the website should be taken down until such time as a consumer can safely interact with it. Until the security problem is remedied, allowing consumers to interact

161. This approach is also similar to the requirement that pharmaceutical companies disclose known negative side-effects of various drugs on warning labels.

162. For example, the Monster.com security breach would provide a possible Tier 2 situation. For a discussion of the Monster.com compromise, see, for example, Hidalgo, *supra* note 21.

163. An active exploit usually triggers a need for a "hot fix." A hot fix is an information security term for a security vulnerability correction that needs to be done immediately due to the severity of the threat. *See, e.g.*, Yahoo! Answers, *What Is Hotfix Why Are There So Many Installed in My Programs Do I Need Them??*, http://answers.yahoo.com/question/index?qid=20060723191022AAzC1bE (last visited Oct. 4, 2009).

164. In the case of a website, if the exploit is limited to a containable section of the site, the remainder of the site can continue to operate.

with the website exposes these consumers to information harm. The site should be replaced with a non-interactive notice: "Safety Notice: Please return another time." Similarly, if a digital rights management application on a shrinkwrap product results in immediate compromise of consumer machines, it should be pulled off the shelves. Advertising and all other communications connected to the website should be tabled until the information security problem is resolved.[165] For example, turning to the case of the jobseeker website described in Part II, this type of a code prohibition would be appropriate. Because hackers are actively pillaging information from the contents of the website databases, any visitor who deposits a resume is at risk of being victimized by an exploit in progress simply by using the website as intended. At a minimum, the sophistication of the attack was high, urgency was high, and a large portion of consumers was impacted.

3. The Consequences to Code Creators and Operators

The reasonable expectation of code safety embodied in the three-tiered model is itself modeled directly on corporate best practices for handling information security issues. Therefore, a regulatory approach constructed in this manner would not generate excessive burdens for organizations already engaged in rigorous information risk management. The only creators or operators burdened would be those who offer digital products that do not comport with industry best practices.

Creating a duty of code inspection by adopting this framework into law would grant legal validation to the efforts of organizations already proactively including strong consumer transparency and information security processes into their risk management planning and product development.[166] Minimizing functionality disruption of other code and ensuring effective information security are increasingly viewed as a competitive advantage by major technology companies;[167] however, especially the importance of rigorous information security is not universally understood at this juncture. In particular, market forces will not dramatically improve security in the public sector.

---

165. For example, the Register.com security breach, where a banner advertisement contained a malicious payload that spread merely through accessing the Register.com website, would provide a possible Tier 3 situation. For a discussion of The Register's compromised banner ad, see, for example, Rohde & Roberts, *supra* note 21.

166. The organizations most likely to object vociferously would be those seeking to hide the inadequacies of their existing information security management structures and the extent to which they carelessly put consumers at risk of information security harms.

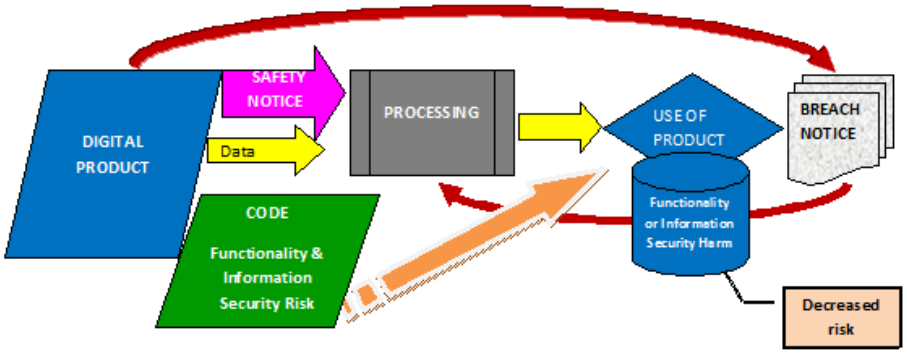
167. *See, e.g.*, Microsoft Corporation, *Windows Vista: Learn About the Features: Safer*, http://www.microsoft.com/singapore/windows/products/windowsvista/features/safer.mspx (last visited Oct. 6, 2009).

Creating a duty to warn of code harm would immediately improve the information parity between consumers and the creators and operators of code. Useful information would arrive at a point in time when the consumer can still choose not to interact with the code. This type of a real-time feedback loop would put consumers on notice of the existence of possible functionality or security risks or other problems involved with choosing to use the creator or operator's code. Public disclosure of ongoing functionality and information security problems through an additional information feedback loop will encourage creators or operators to engage in more careful code creation and to fix security problems more quickly to avoid public embarrassment.

Particularly if coupled with a mandatory audit regime, creating a duty of code repair would ensure that errors exposing consumers to information risk would not be ignored. A repeated code problem would carry consequences for the creator or operator through legal action, either from an agency or the public. Further, because repairs are always more costly than creating good code on the front end, financial incentives would be put in place for better quality code writing in the first instance.

As shown in *Figure 2*, functionality limitations and information security concerns are likely to be better incorporated into overall consumer processing where multiple sources of feedback concurrently exist to help the consumer assess the safety of digital products. The safety notice information will assist consumers in determining whether a digital product is safe before the consumer's initial interaction. As such, consumer decision-making would begin to shift back toward a white box model.

Figure 2: Data Breach Notice Feedback Loop with Prior Information Security Status Information



In particular, with the addition of a real-time feedback loop about creator or operator security, data breach notices would become more effective. Consumers would be able to more easily cognitively connect the information about a previous breach with their decision-making about future information security behaviors. They may learn to consider security in their communication interactions prior to exposing themselves to additional information security risks in the future.[168] Consequently, consumers may become better able to prevent their own future data compromises.

Part IV, which follows, addresses the primary objection associated with the approach proposed in Part III—a potential tension with the First Amendment. However, as Part IV explains, a regulatory approach focused on the incidental effects of data tethered to code comports with *United States v. O'Brien*[169] and does not offend the First Amendment. Where the data at issue, regardless of content, through its tethered code increases functionality harms and information security risk to the consumer, restrictions of that data and its tethered code will survive intermediate First Amendment scrutiny.

IV. CODE WARNINGS AND THE FIRST AMENDMENT

Perhaps the primary objection that would arise in connection with an approach such as the one set forth in Part III would involve First Amendment concerns regarding content neutrality of regulation, liability for data/code without knowledge of fault, and chilling of speech, particularly as it relates to the identities of certain creators or operators. This part addresses each of these First Amendment concerns in turn. Fundamentally, in instances where the data with tethered code increases the likelihood that the consumers will lose control of their machines and become victims of information crime, regulation of this data tethered to code should be and will likely be deemed to comport with the First Amendment. Although some risks of chilling speech may exist, regulation targeting nonexpressive incidental effects of this data tethered to code does not violate the First Amendment. This approach is theoretically rooted in *O'Brien*, buttressed by knowledge standards from *Gertz v. Robert Welch, Inc.*[170] In particular, the critical state of information security threatens continued efficacy of key social systems. This situation warrants First Amendment paradigms that create incentives for creators and operators to act with due care and diligence in connection with their code.

---

168. For a discussion of how changing the learning context changes the process of learning, see, for example, ALBERT BANDURA, SELF-EFFICACY IN CHANGING SOCIETIES (1995).

169. 391 U.S. 367, 370–71, 386 (1968).

170. 418 U.S. 323, 334 (1974).

A. *Content Neutrality*

Should states wish to regulate communication with regard to its information security impact, these regulations would constitute a content-neutral approach.[171] Borrowing a content neutrality test from Professor John Hart Ely, a content-neutral regulation is one where it becomes irrelevant whether the consumer understands English.[172] Here, this test is met: the content of data is not relevant to its regulation; data in any language poses the same functionality and information security risks as long as it is tethered to compromised code. The risk arises from the information security outcome triggered by the code behind the content.

Content-neutral regulations are not necessarily problematic from a First Amendment perspective; regulations targeting incidental effects of speech, avoiding content, are not unprecedented and have been upheld by the Court as comporting with the First Amendment. In *O'Brien*, the Supreme Court addressed the issue of whether a regulation prohibiting the burning of draft cards constituted a prior restraint on speech that violated the First Amendment.[173] The Court determined that "when 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms."[174] Consequently,

> a government regulation is sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.[175]

Turning to another similar intermediate scrutiny First Amendment context, time, place, manner restrictions have been upheld in numerous contexts, including restricting placement of tobacco advertisements,[176]

---

171. Prohibiting speech simply on the content or viewpoint expressed is facially unconstitutional. *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 381–83 (1992); Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd., 502 U.S. 105, 124 (1991) (Kennedy, J., concurring); Police Dep't of Chi. v. Mosley, 408 U.S. 92, 95 (1972).

172. John Hart Ely, *Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis*, 88 HARV. L. REV. 1482, 1483–90 (1975).

173. 391 U.S. at 370. For a discussion of *O'Brien*, see, for example, Volokh, *supra* note 55, at 1286.

174. *O'Brien*, 391 U.S. at 376.

175. *Id.* at 377.

176. *See generally* Lorillard Tobacco Co. v. Reilly, 533 U.S. 525 (2001) (holding that

restricting use of sound trucks[177] and amplified music,[178] restricting use of automatic dialing-announcing devices,[179] restricting parades,[180] and restricting locations of adult theaters.[181] Limiting data tethered to code and the communications about these digital products which exacerbate consumers' functionality and information security risks is consonant with the theory behind these restrictions—it serves an important government purpose[182] that is not related to suppression of speech.[183] Although the approach proposed in Part III may not be the only way of achieving the desired goal, it is not mandatory as a matter of First Amendment doctrine that the proposed approach be the least speech-restrictive alternative.[184]

Just as the Court in *O'Brien* found a vital interest in the continued functionality of the Selective Service System,[185] identity theft and zombie botnets harm both society as a whole through undermining key social systems and individual consumers in their economic reputations.[186] Identity theft and zombie botnets run by organized cybercrime threaten the continued functionality of the Social Security System and threaten other national interests. Because social security numbers (SSNs) are a disproportionately useful piece of personally identifiable information for an identity thief, they are a primary target for information criminals. As many as one in seven adult SSNs has already been compromised as a result of data breaches in the last several years.[187] As the trajectory of compromise currently stands, SSNs will

---

Massachusetts had demonstrated a substantial interest in preventing access to tobacco products by minors and certain provisions had employed appropriately narrow means to advance that interest).

177. *See generally* Kovacs v. Cooper, 336 U.S. 77 (1949) (upholding restrictions on use of sound trucks).

178. *See* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (restricting amplified music and emphasizing that the time, place, and manner regulation must be narrowly tailored to serve a legitimate government interest).

179. *See, e.g.*, Van Bergen v. Minnesota, 59 F.3d 1541, 1556 (8th Cir. 1995) (acknowledging that a Minnesota regulation on the use of automatic dialing-announcing devices triggers First Amendment review but upholding the law as a legitimate time, place, or manner regulation).

180. *See* Cox v. New Hampshire, 312 U.S. 569, 576 (1941) (finding a parade permit ordinance constitutional).

181. *See* Young v. Am. Mini Theatres, Inc., 427 U.S. 50, 62–63 (1976) (concluding that the city's interest supports the different treatment of adult theatres, limiting "the place where [adult] films may be exhibited," even though based on distinguishing content).

182. *See, e.g.*, Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180, 180–81 (1997).

183. *See, e.g.*, Barnes v. Glen Theatre, Inc., 501 U.S. 560, 570 (1991).

184. *See, e.g.*, *Turner*, 520 U.S. at 217–18.

185. *United States v. O'Brien*, 391 U.S. 367, 381 (1968).

186. For a discussion of a possessor of land's duty to warn and protect entrants from physical harm, see *supra* notes 126–39 and accompanying text.

187. Gartner Press Release, *supra* note 15.

soon become an unusable method of authenticating U.S. residents for obtaining social services. Some experts believe that the level of compromise of SSNs has already reached the point where they can no longer be used as a primary means of authenticating identity.[188] As described in Part II, large numbers of businesses, nonprofits, and government agencies appear to suffer data breaches on a regular basis. These numbers do not bode well for the survival of the Social Security System as a means of authenticating U.S. citizens for purposes of government benefits. This negative trajectory becomes particularly apparent when the statistics of SSN compromise are coupled with the Government Accountability Office's annual findings of failing or inadequate information security practices in most federal agencies[189] and the lack of meaningful improvements to leakage of social security numbers by private entities.[190]

Compromising communication is fast becoming a method of choice for Internet criminals. They seek to efficiently cause damage or steal consumer information from consumer systems and to turn such systems into zombie drones[191] for attacking other consumers by sending malicious communication as part of a zombie botnet network.[192] An inadequately protected personal computer can be "owned" by an attacker in under four minutes. [193] Approximately 250,000 new zombies are identified per day[194] with approximately 100 to 150 million total

188. *Id.*

189. *See, e.g.*, Alice Lipowicz, *DHS Still Remiss on Cybersecurity: GAO*, WASH. TECH., Mar. 3, 2007, http://washingtontechnology.com/articles/2007/03/21/dhs-still-remiss-on-cybersecurity-gao.aspx; Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk: Testimony Before Cong. Subcommittees, Comm. on Oversight and Government Reform, H.R., 110th Cong. 2 (2007) (statement of Gregory C. Wilhusen, Director, Information Security Issues), *available at* http://www.gao.gov/new.items/d07935t.pdf (finding that federal agencies do not maintain acceptable information security practices); Grant Gross, *VA Ignores Cybersecurity Warnings*, PCWORLD, June 14, 2006, http://www.pcworld.com/article/id,126093-page,1/article.html.

190. For example, 50,000 General Electric employees' social security numbers were compromised in September 2006. *See* Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Oct. 6, 2009).

191. Zombie drones are security-compromised machines that can be controlled remotely without the consumer's knowledge for sending communication or other malicious purposes. *See Primer: Zombie Drone*, *supra* note 24.

192. Botnets are organized networks of remotely compromised machines, harnessed by criminals for the purpose of sending spam, conducting denial of service attacks, and other nefarious purposes. Botnets are frequently part of organized criminal operations. The changing character of spam toward primarily a criminal enterprise also drives spam internationalization in production. *See* Clive Thompson, *The Virus Underground*, N.Y. TIMES MAG., Feb. 8, 2004, at 28, 79, 82.

193. *Clean System to Zombie Bot in Four Minutes*, SLASHDOT, http://slashdot.org/article.pl?sid=04/11/30/1932245.

194. For example, one Polish spam group uses over 450,000 compromised systems, "most

zombies currently in operation, by some expert estimates.[195] Eastern European organized crime syndicates have begun launching extortion rackets against businesses in other countries, threatening them with attacks from zombie drones.[196] The threat to international critical infrastructure posed by this international market in zombie drones is severe.[197] For example, an army of zombie drones could be used to carry out an attack on electrical power infrastructure, disrupting service. According to the CIA, power outages in multiple cities outside the United States can be traced to cyberattacks where extortion demands were ignored.[198] Similarly, vital national security interests are implicated when machines within agencies and machines with critical infrastructure roles become owned as part of a zombie drone army because an employee imprudently, for example, clicked on a link in an email which led to a compromised website.[199]

Finally, digital products' current black box system threatens trust in the Internet as a viable communication and commercial medium.[200] One

---

of them home computers running Windows high-speed connections" all over the world. *See, e.g.*, *CipherTrust's Zombie Statistics*, *supra* note 16.

195. Weber, *supra* note 16.

196. Menn, *supra* note 17. This trend is concerning particularly because numerous U.S. federal agencies, including the Department of Homeland Security, have repeatedly failed cybersecurity review of the Government Accounting Office. McCullagh, *supra* note 17. According to FBI sources, the Eastern European mafia views sending out emails as its "9 to 5 job." Grasso, *supra* note 17.

197. David Bank, *New Virus Can Turn You into a Spammer*, WALL ST. J., Jan. 29, 2004, at D1. A black market also has developed for zero-day exploit code to be included in or used in connection with spam. Zero-day exploit code is code which exploits a security vulnerability for which there is no known patch and of which the vendor is not aware. George V. Hulme, *Zero-day Attacks Expected to Increase*, INFO. WEEK, Mar. 24, 2003, at 32; Comments of Simple Nomad, Stanford University, Cybersecurity, Research and Disclosure Conference, Nov. 22, 2003; s*ee also The Beagle Has Landed*, WIRED, Jan. 23, 2004, http://www.wired.com/print/techbiz/it/news/2004/01/61976; Ron Hale, Intrusion Crackdown, http://www.itsecurity.com/papers/telenisus.htm (last visited Oct. 6, 2009).

198. *See* Tom Espiner, *CIA: Cyberattack Caused Multiple-City Blackout*, CNET NEWS, Jan. 22, 2008, http://www.news.com/2100-7349_3-6227090.html.

199. *See supra* note 18.

200. The primary real space comparison used for first generation of digital products and communication was postal mail. Email has proven itself in its developmental trajectory to be a fundamentally different medium than postal mail. In 2001, only 8% of U.S. email traffic was spam. Luiz Henrique Gomes et al., *Characterizing a Spam Traffic* (2004), *available at* http://www.imconf.net/imc-2004/papers/p356-gomes.pdf. However, by comparison, in 2003, 40% of traffic was spam, and by 2004, this figure rose to 73% of traffic. By comparison, approximately only 40% of U.S. postal service mail is commercial in nature. Also, 25% of Internet consumers have already diminished their use of email because of spam. A parallel cut has not been noted for postal mail, due to the presence of commercial communications. *See* DEBORAH FALLOWS, PEW INTERNET AND AMERICAN LIFE FOUNDATION, SPAM: HOW IT IS HURTING EMAIL AND DEGRADING LIFE ON THE INTERNET i, 12 (2003), *available at* http://www.pewinternet.org/~/media//Files/Reports/2003/PIP_Spam_Report.pdf.pdf.

in every sixteen emails has been found to carry a virus.[201] The pervasiveness of these risks has impaired consumers' sense of control over their own systems to the extent that consumers have started to use the Internet less as a consequence.[202] If consumers determine that they cannot use the data of even trusted speakers without putting themselves at risk for identity theft because of the attached code, they may lose faith in the medium as a whole for communication.

B. *Liability for Knowledge of Risk and Failure to Warn*

Although protecting consumers and preserving critical systems are core concerns with regard to information security risk, creator and operator side concerns also exist. A regulatory approach which imposes, in essence, a strict liability approach to punishing speech will inevitably result in chilled speech—speakers speaking less for fear of punishment. Creators and operators may worry that they will bundle data with code that harms consumers unknowingly. However, particularly in the context of data tethered to code which exacerbates functionality or information security risk, regulation should temper liability with a knowledge qualification. Even information security experts cannot foresee all possible security issues before they arise.[203] The operative

---

201. Michael Binder, Assistant Deputy Minister, Spectrum Info. and Telecomms. Tech., Lecture to ICT Standards Advisory Council of Canada (Mar. 22, 2005) (presentation available at http://www.isacc.ca/isacc/_doc/Book19-2005/ISACC-05-33300.pdf).

202. *See* FALLOWS, *supra* note 200, at 12. To date, the FTC has prosecuted under 100 individuals and entities for spam fraud. *See Prepared Statement of the Federal Trade Commission on "Unsolicited Commercial Email": Statement Before the Comm. on Energy and Commerce, Subcomm. on Commerce, Trade and Consumer Protection, Subcomm. on Telecommunications and the Internet*, 108th Cong. 1 (2003), *available at* http://www.ftc.gov/os/2003/07/spamtest.htm. Most of these enforcement actions involved false content and were brought under § 5 of the Fair Trade Act, alleging that the defendants in question engaged in unfair trade practices. *See, e.g.*, Complaint for Civil Penalties, Permanent Injunction, and Other Relief at 2, United Statesv. Global Mortgage Funding, Inc., No. SACV 07-1275 DOC (C.D. Cal. Oct. 30,2007); Stipulated Final Judgment and Order for Permanent Injunction at 1, FTC v. Westby, No. 03 C 2540 (N.D. Ill. Mar.. 4, 2004); FTC v. NetSource One, No. 022-3077 (W.D. Ky. filed Nov. 2, 2002); FTC v. Cyber Data, No. CV 02-2120 LKK (E.D. Cal. filed Oct. 2002); FTC v. Internet Specialists, No. 302 CV 01722 RNC (D.Conn. filed Oct. 2002); Stipulated Judgment and Order for Permanent Injuction at 2, FTC v. Patrick Cella, No. CV-03-3202 (C.D. Cal.Nov. 20, 2003); Stipulated Final Judgment and Order for Permanent Injuction and Other Equitable Relief at 2, FTC v. K4 Global Publ'g, Inc., No. 5:03-CV-0140-3-CAR (M.D. Ga. Oct. 14, 2003); Complaint for Permanent Injunction and Other Equitable Relief at 1, FTC v. Clickformail.com, Inc., No. 03-C-3033 (N.D. Ill. May 7, 2003). A more apt comparison might be a person with a possibly contagious illness entering a room full of people. The illness may spread simply because the person shook hands with someone in the room. If the person obtains a reputation as someone who spreads disease, people will become unwilling to shake hands with him.

203. *See, e.g.*, comments of Prof. Ed Felton, Computer Law Section panel on information

question is whether once a vulnerability is discovered or should have been discovered[204] that all reasonable steps are expeditiously taken to remedy the problem. Information risks will always exist; the operative inquiry is into how they are handled after discovery. Responses and the levels of care vary dramatically, and many organizations feel adequate economic and legal incentives do not exist to warrant vigilance and immediate fixes to information security problems.[205]

In situations where creators or operators know or should know that their data is tethered to code that exposes a consumer to additional functionality or information security risks, a legitimate state interest in regulation and consumer protection exists. States can properly impose liability. Regarding the standard of knowledge that might pertain to the speaker under an analysis using the *O'Brien*-inspired framework proposed above, the cases of *Gertz v. Robert Welch, Inc.*[206] and *New York Times v. Sullivan*[207] provide possible guidance.

In *Gertz*, the Supreme Court considered the liability of a magazine publisher for libel in connection with an article alleging that the plaintiff was part of a communist conspiracy to frame a policeman convicted of murder.[208] The Court held that in the case where defamation of a private individual is at issue rather than a public figure, the First Amendment does not prevent liability for the publisher and that the plaintiff is not required to prove knowledge of falsity or reckless disregard for the truth.[209] In situations where private individuals are made more vulnerable to injury and substantial danger is apparent, the state interest in protecting them is correspondingly greater, and states are at liberty to set lower burdens of proof of fault.[210] Consequently, where some degree of fault exists, liability can be deemed appropriate by state law for speech. Therefore, following the logic of *Gertz*, states can be free to impose liability for data tethered to code that magnifies functionality and information security risks for consumers so long as they do not

---

security, AALS ANNUAL MEETING, New York, New York, Jan. 4, 2008.

204. A vulnerability should be known by a vulnerable speaker if the vulnerability is known generally in the information security community.

205. For example, in the recent TJX data breach, the company was using substandard encryption to protect millions of consumers' data. Most home routers employ stronger encryption than that which was employed by TJX. For a discussion of the TJX breach, see, for example, Mark Jewell, *TJX Data Breach Now Called World's Largest: 45.7 Million Cards Were Compromised*, SAN DIEGO UNION TRIBUNE, Mar. 30, 2007, *available at* http://www.signonsandiego.com/uniontrib/20070330/news_1b30tjx.html.

206. 418 U.S. 323, 340 (1974).

207. 376 U.S. 254, 271–80 (1964).

208. *Gertz*, 418 U.S. at 326–27.

209. *Id.* at 347.

210. *Id.* at 344–46.

impose liability without fault.[211] Such regulation is intended to protect consumers from identity theft, among other things, and constitutes a "protection of private personality . . . left primarily to the individual States under the Ninth and Tenth Amendments."[212] Similarly, there is a "strong and legitimate state interest in compensating private individuals for injury to reputation," [213] such as the economic reputation damage caused by identity theft. Data tethered to code that exposes consumers to additional information security risk represents a "careless error"[214] that does not "materially advance[] society's interest in 'uninhibited, robust, and wide-open' debate on public issues,"[215] and "belong[s] to [a] category of utterances which '. . . any benefit that may be derived from them is clearly outweighed by the social interest in order.'"[216]

However, even presuming that this *Gertz* standard may not be optimal, a more difficult standard of reckless disregard for the information security impact of the data with code that is modeled after *New York Times v. Sullivan*[217] would still provide a workable standard.[218] In *New York Times v. Sullivan*, an elected official sued the *New York Times* in connection with an advertisement he alleged to be libelous.[219] In finding the speech at issue to be protected by the First Amendment, the Court articulated a standard of actual malice required to negate the presumption of Constitutional protection for the speech: the Court found that a "statement . . . made with 'actual malice'—that is, with knowledge . . . or with reckless disregard" is not protected First Amendment speech.[220] In the context of data tethered to a flawed code, where the creator or operator can be shown to have had actual knowledge or reckless disregard of increasing the risk of functionality

211. In instances where an aggrieved consumer cannot demonstrate reckless disregard for her information security by a speaker, recovery should be limited to actual injury, as broadly defined by the *Gertz* Court to include out-of-pocket loss, impairment of reputation and standing, personal humiliation, and mental anguish and suffering, all of which frequently arise in cases of identity theft. According to *Gertz*, states may not permit recovery of presumed or punitive damages when liability is not based on knowledge of falsity or reckless disregard for the truth, and a plaintiff who establishes liability under a less demanding standard than the *New York Times* test may recover compensation only for actual injury. *Id*. at 349.

212. *Id.* at 341.

213. *Id.* at 348–49.

214. *Id.* at 340.

215. *Id.*

216. *Id.* (quoting Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942)).

217. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964).

218. However, adopting the *New York Times v. Sullivan* standard would eliminate the option for suits on the basis of negligent speech about code—a failure to warn. Suits for negligent functionality limitation or information security conduct would remain a viable option, of course.

219. *Id.* at 256.

220. *Id.* at 279–80.

or information crime for the consumer, the speech at issue can, as a First Amendment matter, be regulated and provide a basis for liability.

C. *Chilling and Speaker Neutrality*

A core First Amendment concern is that of chilling speech and distorting public discourse.[221] It might be argued that by imposing equal obligations of care in connection with information security implications on all creators and operators, a disproportionate burden may be placed on small creators or operators holding unpopular positions. By imposing an affirmative obligation of information security care in connection with data bound with code, the proportional costs of compliance may be greater for these two groups than for a large, uncontroversial creator or operator and their speech may be chilled as a consequence. Although the proposed model may indeed result in greater proportional costs to these two groups, that is not necessarily the case in all instances. Through careful assessment of their code needs and through careful contracting, any additional costs can be minimized. Choices about code dictate choices about security. Because the standard for liability advocated here turns on actual knowledge or some degree of fault, exercising reasonable care in information risk management does not necessarily disproportionately burden these small or unpopular creators or operators. For example, the best information security outcome, if not the most efficient business outcome, may be encouraging creators and operators to outsource data management and information security services, while simultaneously considering it more aggressively in their own risk management and contracting practices. Those lacking expertise in information systems who attempt to manage their own information systems are likely to experience a greater number of information security problems and negative public relations consequences.[222]

---

221. *See, e.g.*, Geoffrey R. Stone, *Content Regulation and the First Amendment*, 25 WM. & MARY L. REV. 189, 198 (1983) ("[T]he [F]irst [A]mendment is concerned, not only with the extent to which a law reduces the total quantity of communication, but also—and perhaps even more fundamentally—with the extent to which the law distorts public debate."). *See id.* at 192–93 ("The Court's primary concern in the content-neutral realm is that such restrictions, by limiting the availability of particular means of communication, can significantly impair the ability of individuals to communicate their views to others. This is, of course, a central [F]irst [A]mendment concern, for to the extent that content-neutral restrictions actually reduce the total quantity of expression, they necessarily undermine the 'search for truth,' impede meaningful participation in 'self-governance,' and frustrate individual 'self-fulfillment.'").

222. Small entrepreneurial ventures may indeed have fewer resources to invest in information security processes and monitoring. However, small ventures sometimes engage in behaviors that exacerbate their own information security risks unnecessarily. For example, small ventures frequently have a tendency to engage in aggressive data collection and hoarding, including collecting personally identifiable data that is not needed for processing of any transactions authorized by the customer. By choosing to hoard information, these ventures make

Speakers holding unpopular positions on their websites, for example, may indeed be more likely to be the victims of information criminals seeking to harm their supporters through the Internet in order to silence them. This technological reality should push them to consider functionality and information security risks more aggressively, in much the same way that they expect hecklers in real space to attack them verbally with more zeal. In other words, it is not a regulation mandating care in speech that would disproportionately burden them; it is the combination of technology and the unpopularity of their speech, regardless of medium.[223] Meanwhile, if consumers begin to associate unpopular speakers with increased functionality and information security risks, they may become unwilling to listen to unpopular communication. A minimum statutory level of care may actually provide comfort to consumers while listening to unpopular communication.

From a First Amendment standpoint, the data implicated can encompass two distinct kinds of speech—commercial[224] and political.[225] However, from a functionality and information security standpoint, all data is essentially identical; all data potentially exposes consumers to significantly increased functionality and information security risks if

---

themselves more attractive to information criminals, thereby triggering a need for more rigorous security processes. Similarly, when hiring developers who write custom code for such ventures, small ventures may be less likely to use counsel and less likely to include information security requirements which can easily be negotiated into the specifications for the speech. Proactively considering ways to mitigate information risk may assist not only the consumers' of small companies, it may also assist the companies themselves. For example, teaching entrepreneurs to consider information security from the inception of the enterprise will assist them in obtaining trade secret protection to defend their proprietary information assets. Also, hiring a dedicated high-quality hosting company with strong information security standards may not only reduce risk of communications being compromised, but may also result in long term cost-savings over maintaining Internet communications in-house. Public relations damage can potentially be mitigated through shifting blame to an external services provider.

223. Through assessing the information risk structure associated with particular communication strategies, these speakers may realize they are gratuitously exposing themselves to certain types of information security problems. Careful contracting and choosing intermediaries such as hosts and ISPs can again alleviate much of the concern. In the context of unpopular speech in particular, because attacks on communication have become sophisticated, protecting the message and ensuring that consumers will not be victimized should rank as an organizational priority. As a practical matter, unless the speakers are information security experts, they will lack the expertise to do so effectively.

224. For a discussion of commercial speech, see generally Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557 (1980) (holding that a regulation completely banning an electric utility from advertising to promote the use of electricity violates the First and Fourteenth Amendments).

225. For a discussion of political speech, see generally Buckley v. Valeo, 424 U.S. 1 (1976) (ruling on the constitutionality of several provisions of the Federal Election Campaign Act).

tethered to code.[226] It is true that a First Amendment incongruity arises in connection with speaker identity—the proposed regulatory approach adopts an identity neutral approach while existing case law addressing communication adopts a commercial speech analysis. As discussed in Part III.A.2, the dominant analytical approach used by courts in connection with digital products has been analysis under the commercial speech standards of *Central Hudson*[227] and its progeny, which looks to the commercial or noncommercial identity of the speaker and the content of the speech. In contrast, the proposed statutory approach creates a mandatory real-time information security feedback loop that would apply to all content creators or operators, regardless of commercial or noncommercial motivation. As such, it can be argued that the approach proposed by this Article burdens noncommercial speakers in a way they have heretofore not been burdened in connection with their communication. This assertion is accurate; however, this identity neutral approach is driven by technological necessity. A commercial speech centered restriction is doomed to technological failure. Any successful functionality and information security speech regulatory regime must be inherently speaker neutral. Information security processes are only as successful as the weakest point in the information security chain. Commercial or noncommercial identity does not impact the functionality or information security risks code carries. Similarly, data content, commercial or otherwise, is not the source of concern. A compromised political website can cause the same information security damage to consumers as a compromised commercial website. Therefore speaker neutrality is mandated by the technological reality of the policy problem.[228]

D. *Compelled Speech*

As articulated by the Supreme Court in *Wooley v. Maynard*,[229] although "the right of freedom of thought protected by the First Amendment against state action includes both the right to speak freely and the right to refrain from speaking at all,"[230] in circumstances where

---

226. Both of these communications may have resulted in the theft of the consumer's identity and a consumer unknowingly becoming part of a remotely controlled organized information crime computer network. In the language of computer security, remote compromise of a machine can lead to the owned machine becoming part of a zombie network used for distributed denial of service (DDoS) attacks and information crime. For a discussion of zombie drones and remote compromise, see Matwyshyn, *supra* note 5, at 378–79.

227. *Central Hudson*, 447 U.S. at 566.

228. It can also be argued that this type of speaker neutral approach recognizes the Court's trend toward converging levels of constitutional protection for political and commercial speech. *See, e.g.*, 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 501–03 (1996).

229. 430 U.S. 705 (1977).

230. *Id.* at 714 (1977) (citation omitted); s*ee also, e.g.*, Rumsfeld v. Forum for Academic &

an ideologically neutral compelling state interest warrants compelling speech, such compelled speech is constitutionally permissible.[231] Compelled speech approaches are frequently used in consumer protection contexts; contexts such as securities disclosure,[232] food and drug labeling,[233] alcohol and tobacco labeling,[234] and real estate disclosures[235] provide examples of instances where compelled speech is

---

Institutional Rights, Inc., 547 U.S. 47, 69 (2006) (requiring universities to advertise presence of military recruiters on campus); Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74 , 86–87 (1980) (upholding free speech rights of individuals on private property of shopping mall); W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 633–34 (1943) (refusing to uphold West Virginia statute requiring saluting of the flag in schools). Additional cases have limited the government's ability to force one speaker to host or accommodate another speaker's message. *See, e.g.*, Hurley v. Irish-Am. Gay, Lesbian & Bisexual Group of Boston, 515 U.S. 557, 573–574 (1995) (holding that state law cannot require a parade to include a group whose message the parade's organizer does not wish to send); Pac. Gas & Elec. Co. v. Pub. Utils. Comm'n of Cal., 475 U.S. 1, 21 (1986) (ruling that a state agency cannot require a utility company to include a third-party newsletter in its billing envelope); Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974) (holding that a right-of-reply statute violates editors' right to determine the content of their newspapers).

231. For a discussion of compelled speech, see Martin H. Redish & Kirk J. Kaludis, *The Right of Expressive Access in First Amendment Theory: Redistributive Values and the Democratic Dilemma*, 93 NW. U. L. REV. 1083, 1113–23 (1999). For several scholarly articles about various aspects of commercial speech, see Larry Alexander, *Compelled Speech*, 23 CONST. COMMENT. 147 (2006); Mark Champoux, *Uncovering Coherence in Compelled Subsidy of Speech Doctrine:* Johanns v. Livestock Marketing Ass'n, 125 S. Ct. 2055 (2005), 29 HARV. J.L. & PUB. POL'Y 1107 (2006); *Government Speech Doctrine—Compelled Support for Agricultural Advertising*, 119 HARV. L. REV. 277 (2005); Lewis Michael Higgins, *Constitutional Law—First Amendment—Compelled Funding of Government Speech Through the Use of Targeted Assessments Does not Violate the First Amendment*, 36 CUMB. L. REV. 643 (2006); Robert Post, *Informed Consent to Abortion: A First Amendment Analysis of Compelled Physician Speech*, U. ILL. L. REV. 939 (2007); Robert Post, *Transparent and Efficient Markets: Compelled Commercial Speech and Coerced Commercial Association in* United Foods, Zauderer, *and* Abood, 40 VAL. U. L. REV. 555 (2006).

232. For a discussion of securities disclosure and speech, see Michael R. Siebecker, *Corporate Speech, Securities Regulation, and an Institutional Approach to the First Amendment*, 48 WM. & MARY L. REV. 613 (2006).

233. For example, in *Glickman v. Wileman Bros. & Elliott, Inc.*, 521 U.S. 457 (1997), the Court found that compelled subsidies for generic fruit advertising did not burden First Amendment rights, and instead evaluated the program "under the standard appropriate for the review of economic regulation . . . ." *Id.* at 469; *see also* Joseph Wilhelm, Comment, *Compelled Commercial Speech Under the Beef Promotion Act Should be Impermissible:* United States v. Frame, *885 F.2d 1119 (3d Cir. 1989)*, 59 U. CIN. L. REV. 1021 (1991) (discussing the speech involved under the Beef Promotion and Research Act of 1985).

234. For a discussion of labeling of "vice" products, see Kathryn Murphy, Note, *Can the Budweiser Frogs Be Forced to Sing a New Tune?: Compelled Commercial Counter-Speech and the First Amendment*, 84 VA. L. REV. 1195 (1998).

235. For a discussion of real estate disclosures, see Tanya D. Marsh & Robert G. Solloway, *Survey: Property Law: Let the Seller Beware: The Slow Demise of Caveat Emptor in Real Property Transactions and Other Recent Developments in Indiana Real Property Law*, 38 IND. L. REV. 1317 (2005).

used successfully to further a compelling state interest in consumer protection. In the context of consumer protection from the hidden engines of destruction in data tethered to code, the case is equally—if not more—compelling.

IV. CONCLUSION

This Article explored whether a duty to warn should exist in the context of digital products and argued in favor of creating a "reasonable expectation of code safety." Code will never be perfect, the same way that land is never perfect. New vulnerabilities are found every day in much the same way that the owner of an old house finds a new creaky step or a broken pipe. In both cases, perfection is not possible; the best approach is a process-based one which requires vigilant inspection, clear and ample disclosure and warning, and consistent monitoring with prompt repair.

Therefore, to adequately address these hidden engines of destruction, Congress or state legislatures should enact a three-tiered duty to warn and repair. Such legislation would improve information parity and consumers' control over the digital products they use. Existing data breach notification laws alone cannot solve the security problems that lurk in the code behind the digital content.