Loyola University Chicago Law Journal

Volume 48
Issue 4 *Summer 2017*

Article 9

2017

It Is Just Unfair Using Trade Laws to "Out" Security Software Vulnerabilities

Marian K. Riedy

Bartlomiej Hanus

It Is Just Unfair Using Trade Laws to "Out" Security Software Vulnerabilities

Marian K. Riedy & Bartlomiej Hanus***

In 2015, hackers gained access to hundreds of millions of consumer data records housed in the databases and systems of American businesses, and the number of records stolen climbed even higher the following year. Though businesses spend billions of dollars each year on security software and systems to protect data from unauthorized disclosure, those systems often fail because of vulnerabilities in the software that hackers exploit. All but the simplest software contains some vulnerabilities, including coding errors. Pursuant to the observations of previous legal scholarship, one of the reasons "bad code" (i.e., code vulnerable to hacking) persists in the consumer market is that software vendors insulate themselves from accountability using contractual disclaimers of warranties and limitations on liability. One might expect, by way of contrast, that in the commercial market for software and, in particular, for security software, companies would demand that the vendor share responsibility in the event of a data breach. But this Article's empirical analysis of end-user license agreements (i.e., agreements between the software vendor or developer and the software user) for such security products demonstrates a similar liability shield in the contractual terms. Therefore, companies cannot, or perhaps just will not, hold security software vendors accountable. The result is an unacceptable risk to consumers; therefore, this Article proposes that regulators should reduce the risk by using unfair trade laws. Specifically, this Article recommends that if a security software vendor knows of a vulnerability in its code and fails to notify its licensees of that vulnerability, it should be charged with committing an unfair trade practice.

---

* Associate Professor, Emporia State University, School of Business. Before her academic appointment, Dr. Riedy practiced law as a civil litigator in Washington, D.C. She is a graduate of Harvard Law School.

** Assistant Professor, Emporia State University, School of Business. He received his Ph.D. degree from the University of North Texas. His primary research interests revolve around information security.

INTRODUCTION

The title of a 2012 article in *The Atlantic* observed that "software runs the world," and then, chillingly, asked: "How scared should we be that so much of it is so bad?"[1] Referring therein to software errors that resulted in millions of dollars in losses in securities trading,[2] the same question might well be asked, however, in regard to the software and systems that large and small businesses use to protect against data compromise.

It has often been observed that software—the programs computer systems run on[3]—are vulnerable[4] to an information security breach. That is, one coding error in the software can give hackers unauthorized access to confidential information on a computer hard drive that is embedded in application software, passing from one networked computer to another, or residing on a remote server.[5] One technical solution to this problem is

1. James Kwak, *Software Runs the World: How Scared Should We Be That So Much of It Is So Bad?*, ATLANTIC (Aug. 8, 2012), http://www.theatlantic.com/business/archive/2012/08/software-runs-the-world-how-scared-should-we-be-that-so-much-of-it-is-so-bad/260846/.

2. *Id.*

3. Taiwo A. Oriola, *Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities*, 28 J. MARSHALL J. COMPUTER & INFO. L. 451, 452 (2011).

4. *See generally* Derek E. Bambauer, *Schrödinger's Cybersecurity*, 48 U.C. DAVIS L. REV. 791, 844 (2015) ("Complete prevention of inaccuracy is impossible . . . [s]oftware code displays extraordinary complexity, leading inevitably to bugs. Hackers are adept at finding and exploiting vulnerabilities . . . ."); Oriola, *supra* note 3, at 455 (explaining that most reported computer or network security issues result from software vulnerabilities); Kevin R. Pinkney, *Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43, 51 (2002) (stating that many hackers' strategies result from programmers and system administrators failing to address known security issues and vulnerabilities).

5. WHITE HOUSE, LEGISLATIVE LANGUAGE: DATA BREACH NOTIFICATION, § 1(g)(1); *see, e.g.*, Bambauer, *supra* note 4, at 844 ("Complete prevention of inaccuracy is impossible . . . [s]oftware

to enhance the security features of computer operating systems and other software.[6] Another is to employ data security software and related systems and services specifically designed to protect against breaches.

Hundreds of companies now sell such data security software and systems.[7] Their offerings range from antivirus software for installation on home computers[8] to enterprise systems designed to detect threats, secure networks, and otherwise provide security for some of the largest companies in the world.[9] Fortune 500 companies reportedly spent $71 billion on data security systems in 2014.[10] Cybersecurity Ventures recently projected worldwide spending on commercial cybersecurity products and services to eclipse $1 trillion for the period between 2017 and 2021.[11] But like the underlying software running computers and programs, security software is also vulnerable to attack.[12]

Vulnerabilities in software began to command the technical community's attention when the consumerization of the Internet gained speed around 2005,[13] and now, the magnitude and severity of the problem

---

code displays extraordinary complexity, leading inevitably to bugs."); Oriola, *supra* note 3, at 463 ("A faulty code or bug is the Achilles' heel of computer or network systems security, and one of the weakest links through which networked computers are traditionally breached.").

6. Emily Kuwahara, *Torts v. Contracts: Can Microsoft Be Held Liable to Home Consumers for Its Security Flaws?*, 80 S. CAL. L. REV. 997, 1006 (2007) (describing Microsoft's "Trust Worthy Computing Initiative" to improve the security of its operating systems).

7. Amanda N. Craig et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, 758 (2015). The Authors collected End User License Agreements ("EULA") available on the websites of three hundred seventy of such companies, ranging from industry giants providing complex, customized solutions—such as Lockheed Martin—to companies selling specific tools such as email filtering.

8. *E.g.*, *McAfee Total Protection*, MCAFEEA FOR CONSUMER, https://promos.mcafee.com/offer.aspx?id=1094031 (last visited Apr. 12, 2017) (offering McAfee Total Protection to consumers for purchase or thirty-day free trial).

9. *Protect Your Digital Enterprise*, HEWLETT PACKARD ENTERPRISE, https://www.hpe.com/us/en/solutions/protect-digital.html (last visited Apr. 12, 2017).

10. Seth Rosenblatt, *Modern Security Tactics Fail to Protect Against Malware, Study Finds*, CNET (Jan. 8, 2015), http://www.cnet.com/news/modern-security-tactics-fail-to-protect-against-malware-new-study-finds/.

11. *Cybersecurity Market Report*, CYBERSECURITY VENTURES, http://cybersecurityventures.com/cybersecurity-market-report/ (last visited Apr. 12, 2017) (noting the market for the second quarter of 2016).

12. *See generally* Stephen S. Gilstrap, *Shifting the Burden in Software Licensing Agreements*, 121 YALE L.J. 1271 (2012) (discussing the increasing potential liabilities associated with software security breaches).

13. In 2005, the number of publicly reported vulnerabilities increased significantly. Also around that time, a large number of easy-to-find bugs in web applications was discovered. The National Vulnerability Database was created, resulting in an increased number of flaws reported by large software companies. *See* Robert Lemos, *Security Flaws on the Rise, Questions Remain*, REGISTER (Jan. 6, 2006), http://www.theregister.co.uk/2006/01/09/computer_security_flaws_on_the_rise/ (discussing the increasing amount of vulnerabilities and software flaws).

is common knowledge in the IT community.[14] Paradoxically, while Moore's Law led to cheap computing power, which allowed for increased software complexity (i.e., lines of code, and consequently, the number of instructions that can be carried out), software quality has apparently declined.[15] Thus, presently, the pace at which coding errors are fixed and new code developed is about the same.[16] Software design and coding flaws may be due, in part, to the increasing modularization of software development[17] via, for example, service-oriented architecture ("SOA")[18], and the increased reliance on agile development methods.[19] Buyers may not demand high-quality software when purchased because updates and patches automatically push to software purchasers via the web.

While security software may not be as complex as operating systems (the latter containing a fair amount of security-related as well as functional features),[20] security software suffers from similar weaknesses and is prone to similar vulnerabilities. For example, antivirus software,

14. *Vulnerability Type Distributions in CVE*, NVD, https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on&cvss_version=3 (last visited Oct. 3, 2016).

15. Moore's Law states that "[t]he number of transistors incorporated in a chip will approximately double every 24 months." Arnab Hazari, *Electronics Are About to Reach Their Limit in Processing Power—but There Is a Solution*, QUARTZ (Jan. 6, 2017), https://qz.com/852770/theres-a-limit-to-how-small-we-can-make-transistors-but-the-solution-is-photonic-chips/ (quoting Gordon Moore, Intel cofounder).

16. *Verizon's 2016 Data Breach Investigations Report*, VERIZON, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/ (last visited Apr. 12, 2017) [hereinafter *Verizon's Report*].

17. Historically, software was written in-house which led to the creation of information silos—isolated applications with no common interfaces to share data with other packages. In contrast, modern-day software is designed with interoperability in mind, which basically means that it takes advantage of common interfaces to share data. Thus, a larger IT infrastructure can be built from building blocks coming from different vendors.

18. Service-oriented architecture ("SOA") is a methodology in which applications rely on the World Wide Web and other such services available in a network. Implementing SOA "can involve developing applications that use services, making applications available as services so that other applications can use those services, or both." Ed Ort, *Service-Oriented Architecture and Web Services: Concepts, Technologies, and Tools*, ORACLE (Apr. 2005), http://www.oracle.com/technetwork/articles/javase/soaterms-138190.html#soaterms.

19. Agile methods differ from traditional waterfall methods in that they favor iterative software design cycles. Such an approach tends to be more suitable for projects where the requirements are characterized by high volatility. Barry Boehm, *Get Ready For Agile Methods, With Care*, COMPUTER, Jan. 2002, at 64, 66.

20. Several categories of metrics for "complexity" exist. McCabe's cyclomatic complexity and Halstead metrics are among the most widely recognized. The former is based on the control of flow of the application. The latter uses program size and effort to evaluate measures like number of operators, operands, etc. ADITYA P. MATHUR, FOUNDATIONS OF SOFTWARE TESTING 29–30 (2008). In addition, simpler measures like source lines of code ("SLOC") may also be used to measure the complexity of a program.

as identified by vendors listed in the Cybersecurity 500 ranking,[21] is susceptible to a number of vulnerability categories, including bypassing access control and permissions, privilege elevation, denial of service (e.g., resource management errors and buffer overflow), code injections and execution, memory corruption, and others.[22] The more complex the software package, the greater the number of vulnerabilities. To make matters worse, different products can suffer from the exact same vulnerability, such that one type of hack can exploit all products simultaneously.[23] Notwithstanding the expenditure of an extraordinary amount of resources to prevent compromise, data comprised of millions of customer records containing personal information housed by a company (e.g., social security and credit card numbers, other financial information, and medical records) and confidential business information are still insecure.[24]

Hackers exploit that insecurity to steal or compromise the data.[25] Intentional hacking is by far the most common cause of stolen or compromised data.[26] Today, hacking is a lucrative business carried out by well-trained cybercriminals with malicious intent to exploit data for potentially enormous amounts of money. It is estimated that external actors—the majority of whom are motivated by direct or indirect financial gain—cause roughly 80 percent of data breaches.[27] Other motives, such as revenge, entertainment, or ideology, rarely play a role.[28] Personal information about individuals, such as names and addresses, may sell for as much as three dollars on the Dark Web (i.e., the

21. *Cybersecurity 500*, CYBERSECURITY VENTURES, http://cybersecurityventures.com/cybersecurity-500/ (last visited May 6, 2017). Some common vendors include: Avast Software, ESET, Malwarebytes, McAfee, Kaspersky, Symantec, etc. *Windows Anti-Malware Market Share Reports*, METADEFENDER, https://www.metadefender.com/stats/anti-malware-market-share-report#!/?date=2017-02-27 (last visited May 6, 2017).

22. *Vulnerabilities by Type*, CVE DETAILS, http://www.cvedetails.com/vulnerabilities-by-types.php (last visited May 6, 2017).

23. For example, in 2012, it was discovered that specially crafted archive files could fly under the radar and avoid malware detection by several major antivirus products on the market. *CVE-2012-1459 Detail*, NVD, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1459 (last visited May 6, 2017).

24. *See infra* notes 29–44 (recognizing personal information's high price tag).

25. *See generally* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011 (2014) (discussing various approaches to mitigating cyberattacks).

26. *Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breach (last visited May 6, 2017) (reflecting that more than 70 percent of record breaches were due to hacking or "unknown"). Other culprits include insiders and lost or stolen data storage devices, among others. Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data Is at Risk: Get Over It!*, 19 SMU SCI. & TECH. L. REV. 3, 12–13 (2016).

27. *Verizon's Report*, *supra* note 16.

28. *Id.*

underground Internet),[29] and social security numbers sell for a dollar.[30] The price of financial information, such as credit card numbers and PayPal or eBay account credentials, ranges from one to eighty dollars per record. The Dark Web markets where stolen data is bought and sold are often quite sophisticated. For example, those with a well-established reputation actually have a return policy, which allows the buyers to receive a refund if the purchased information is no longer active (i.e., a credit card has been blocked or login credentials have been changed or removed).[31]

All this stolen data can add up to a substantial profit. For example, three hackers caught and charged with, inter alia, committing securities fraud on individuals whose identities were stolen from JPMorgan Chase allegedly made hundreds of millions of dollars.[32]

This potential profit begets an astonishing number of data breaches and a massive number of corrupted files. It has been estimated that approximately one in five organizations will likely suffer from a material data breach in the next two years.[33] In January 2015, cybersecurity firm FireEye reported that 96 percent of the 1,600 computer networks that it monitored were breached in 2014.[34] Many of the big data breaches made headline news. For example, it is widely known that in 2014, North Korean hackers compromised Sony's computers and databases.[35] In the process, the hackers destroyed the company's servers and personal computers and wiped Sony's databases clean, resulting in a temporary disruption of business functions.[36] Millions of customer records

29. *Follow the Data: Dissecting Data Breaches and Debunking the Myths*, TREND MICRO (Sept. 22, 2015), http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data. A related source of illicit revenue, but not one specifically addressed herein, is the black market for information regarding software vulnerabilities—avenues for data theft—including the sale of information regarding so-called "zero day" attacks. Bambauer, *supra* note 25, at 1078.

30. Don Reisinger, *Here's How Much Your Social Security Number Is Worth on the Dark Web*, FORTUNE (Aug. 3, 2016), http://fortune.com/2016/08/03/social-security-dark-web/.

31. Omri Toppol, *The Industrialization of the Underground Economy*, BLOGDOG (Apr. 7, 2015), https://getlogdog.com/blogdog/the-industrialization-of-the-underground-economy/.

32. Aarti Shahani, *3 Charged in Hacking Case Against JPMorgan Chase, 11 Other Firms*, NPR (Nov. 11, 2015, 5:07 AM), http://www.npr.org/2015/11/11/455577683/3-charged-in-hacking-case-against-jpmorgan-chase-11-other-firms.

33. ONLINE TRUST ALLIANCE, 2015 DATA PROTECTION & BREACH READINESS GUIDE 6 (Feb. 13, 2015), https://otalliance.org/system/files/files/resource/documents/dpd_2015_guide.pdf.

34. FIREEYE, MAGINOT REVISITED: MORE REAL-WORLD RESULTS FROM REAL-WORLD TESTS 3 (2015), https://www2.fireeye.com/rs/fireye/images/rpt-maginot-revisited.pdf.

35. It was widely rumored, if not proven, that hackers targeted Sony because of Sony's pending release of a comedy show about the assassination of the North Korean leader, Kim Jong-Un. Ari Shapiro, *Sony CEO Reflects on Immobilizing Cyberattack 1 Year Later*, NPR (Nov. 20, 2015, 5:59 PM), http://www.npr.org/2015/11/20/456831542/sony-ceo-reflects-on-immobilizing-cyber-attack-1-year-later.

36. *Id.*

containing personal information were allegedly compromised,[37] as were personnel records dating back over a decade.[38] The hack of JPMorgan in 2015 resulted in the compromise of some seventy-six million client records containing personal and financial information.[39] Overall, in 2015 alone, hundreds of millions of data records housed in the databases and systems of American businesses were hacked,[40] and the numbers climbed even higher in 2016.[41] Government databases are, of course, another target for hackers. In June 2015, the Office of Personnel Management reported that hackers stole the background investigation records of an estimated 21.5 million current, former, and prospective federal employees.[42] These examples are from data breaches that were reported and confirmed, but the overall universe of data compromise is undoubtedly much larger.

The security software systems installed to protect against unauthorized data disclosure did not detect these breaches. Instead, either law enforcement agencies or other third-party entities unrelated to the breached organization discovered about 80 percent of breaches.[43]

The total cost of all this data compromise may be impossible to calculate, but from some specific examples and industry surveys, one can reasonably conclude that hacking exacts a steep price from businesses and consumers. In one case alone, Target, which suffered a massive data breach in 2013,[44] reportedly lost a total of about $236 million in breach-related costs,[45] pledged to spend $100 million upgrading its security,[46] and spent additional money defending against lawsuits brought on behalf of its 110 million customers whose credit and debit card information had been stolen[47] and by banks and credit unions that incurred costs replacing

37. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 955 (S.D. Cal. 2014).

38. Elena Kvochko & Rajiv Pant, *Why Data Breaches Don't Hurt Stock Prices*, HARV. BUS. REV. (Mar. 31, 2015), https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

39. Shahani, *supra* note 32.

40. David McCandless, *World's Biggest Data Breaches*, INFO. IS BEAUTIFUL, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks (last updated Apr. 25, 2017).

41. Paul Ausick, *2016 Data Breaches 10% Higher Than a Year Ago*, 24/7 WALL STREET (Apr. 21, 2016. 8:50 AM), http://247wallst.com/technology-3/2016/04/21/2016-data-breaches-10-higher-than-a-year-ago/.

42. *Cybersecurity Resource Center: Cybersecurity Incidents*, OPM.GOV https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last visited May 6, 2017).

43. *Verizon's Report*, *supra* note 16.

44. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).

45. Kvochko & Pant, *supra* note 38.

46. In re *Target*, 66 F. Supp. 3d at 1157.

47. *Id.* at 1157.

those cards and otherwise remediating the results of the breach.[48] Sony reportedly spent $53 million after its 2014 breach just in repairing its IT and financial systems.[49] The greater the number of records compromised, the greater the cost of remediating the breach. But, on average, the cost to any American company is estimated to be $7 million.[50]

Not every hack will be so costly to the breached company because insurance may cover some of the out-of-pocket losses,[51] and the net cost may be but a small percentage of the company's revenues.[52] But overall, companies spend billions of dollars dealing with the consequences of data breaches.[53] Consumers will presumably pay some portion of this cost as companies pass data breach remediation expenses into the price of goods and services, and consumers also incur costs directly as a result of the breach. One analysis found that consumers spent $13.3 billion in losses between 2005 and 2011,[54] and $13.1 billion in 2013 alone,[55] resulting from illegal purchases from stolen credit and debit cards,[56] lost time and money correcting account information, and other additional costs necessary to remediate the misuse of personal information.[57]

If all this money and time spent replacing computers, databases, and credit cards are not bad enough, the prospect of more pervasive and more dangerous consequences from data breaches in the future ought to give one pause. For individuals, consider all the personal data that is

48. Kvochko & Pant, *supra* note 38.

49. Shapiro, *supra* note 35.

50. *2016 Ponemon Cost of Data Breach Study: United States*, IBM, http://www-03.ibm.com/security/data-breach/ (last visited May 6, 2017).

51. Daniel Garrie & Michael Mann, *Cyber-Security Insurance: Navigating the Landscape of a Growing Field*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 379, 384 (2014) (noting that cybersecurity insurance is the "fastest growing segment of the industry"). Of course, insuring against the risk of a cyberattack is also a cost to the company: premiums for cybersecurity insurance totaled $1.3 billion in 2013. *Id.*

52. Robert Hackett, *How Much Do Data Breaches Cost Big Companies? Shockingly Little*, FORTUNE (Mar. 27, 2015), http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/.

53. *2015 Cost of Data Breach Study: Global Analysis*, IBM, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=SEW03053WWEN (last visited May 6, 2017).

54. LYNN LANGTON, U.S. DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS, IDENTITY THEFT REPORTED BY HOUSEHOLDS, 2005–2010, at 5 (Nov. 2011), http://www.bjs.gov/content/pub/pdf/itrh0510.pdf.

55. Al Pascual, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, JAVELIN (Feb. 20, 2013), https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters.

56. Erika Harrell, *Victims of Identity Theft, 2014*, BUREAU JUST. STAT. (Sept. 27, 2015), http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5410.

57. *Id.*

increasingly becoming available from "smart" homes and devices linked to the Internet. This "Internet of Things" ("IoT"), or "ubiquitous computing,"[58] is still in its infancy, but growing rapidly. "Over the past few years, practically every household item within reach has been technologically upgraded and rendered 'smart': toothbrushes, cutlery, baby monitors, refrigerators, thermostats, slow cookers, sprinkler systems, sex toys, even the locks in doors."[59] The makers of the smart devices collect and store that data.[60] Where we go, what we want, and what we do is all transmitted to company databases via Siri and Alexa.[61] Given that present-day devices belonging to the IoT family are still in their infancy, little doubt remains that new vulnerabilities will emerge and be exploited.[62]

What hackers could do with this data is anyone's guess, but a home break-in and serious blackmail come to mind, as does true identity theft—not just an illicit charge or two on a credit card—or the devices themselves could be turned against individuals. For example, if a hacker compromises a car's control system, that car could come to an abrupt stop on a busy freeway.[63] For a business, consider the possibility of a Stuxnet-like[64] attack in which commercial operations are hijacked and altered in ways imperceptible to and undetectable by the company, and which have the effect of reducing the company's competitive edge and ultimately, perhaps, its very survival.[65]

---

58. UBIQUITOUS COMPUTING (Mar. 17, 1996, 8:00 PM), http://www.ubiq.com/hypertext/weiser/UbiHome.html (last visited May 6, 2017).

59. Jacob Silverman, *Just How 'Smart' Do You Want Your Blender to Be?*, N.Y. TIMES MAG. (June 14, 2016), https://www.nytimes.com/2016/06/19/magazine/just-how-smart-do-you-want-your-blender-to-be.html.

60. *Id.*

61. *Id.* Such "personal assistants" respond to voice commands to access digital connections, including the internet and applications on computers and mobile devices.

62. Press Release, Gartner, Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor (Aug. 18, 2015), http://www.gartner.com/newsroom/id/3114217.

63. Brenda Craig, *First Car-Hacking Class Action Filed Against Ford, GM, and Toyota*, LAWYERSANDSETTLEMENTS.COM (July 25, 2015, 10:30 AM), http://www.lawyersandsettlements.com/articles/data-breach/interview-internet-lawyers-technology-lawyer-2-20800.html#.VjJKfUauzTp.

64. Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011, 7:00 AM), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1. In short, Stuxnet is a piece of malware affecting industrial control systems deployed over large industrial facilities. It allows the perpetrator to take control of such systems without authorization. The prevailing rumor is that it was a result of cooperation of the United States and Israeli governments targeting Iranian nuclear power plants (until it got out of control).

65. Threats to national security from terrorist or "rogue" government attacks are, of course, perhaps of even greater concern. How best to safeguard data housed and used by government

It is probably just a fact of a heavily digitized life that data cannot be made completely secure from unauthorized access. No software (other than perhaps the simplest of software) can feasibly be error free,[66] and so long as these crimes pay, hackers will search for and exploit those errors.[67] But in general, society has reached a consensus that the number and extent of data breaches can and should be reduced.[68]

One of the many legal measures aimed at improving data security[69] that legal scholars propose focuses on the particular issue of software vendors' limited responsibility for security vulnerabilities in the mass-market products they sell.[70] As discussed in more detail below, vendors of consumer software, in particular, almost universally shield themselves from liability in the event of a data breach through disclaimers in the sale or license agreement, thereby eliminating the threat of litigation as an

---

agencies is beyond the scope of this Article.

66. Bambauer, *supra* note 4, at 844.

67. *E.g.*, Trevor Ford, *Cybersecurity Legislation for an Evolving World*, 50 U.S.F.L. REV. 119, 121 (2016) ("Currently, both nation-state and criminal actors are conducting elaborate and persistent campaigns to compromise the security of their targets . . . .").

68. To that end, for example, in regard to the security of consumer data only, Congress and the states regularly consider new legislation designed to ensure consumer privacy and protect personal information stored in company databases. *E.g.*, Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. TIMES (Feb. 27, 2015), http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?_r=0 (discussing recent proposed legislation that would provide Americans with greater control over companies' access to their personal information). Regulators also propose new rules, standards, and guidance. *See generally* U.S. DEP'T OF JUSTICE, COMPUT. CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., *Best Practices for Victim Response and Reporting of Cyber Incidents* (2015), https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf (suggesting steps to take before, during, and after a cyber intrusion).

69. It would surely be impossible even to summarize all of these, given that hundreds, if not thousands, of scholarly articles have been published on the general topic of data security.

70. *E.g.*, T. Randolph Beard et al., *Tort Liability for Software Developers: A Law & Economics Perspective*, 27 J. MARSHALL J. COMPUTER & INFO. L. 199, 230–31 (2009) (discussing certain aspects of the consumer's experience with software that are within the consumer's control rather than the seller's); Michael A. Cusumano, *Who Is Liable for Bugs and Security Flaws in Software*, 47 COMM. ACM 25, 26 (Mar. 2004), https://pdfs.semanticscholar.org/4fa3/39da13b3fe84062778af73ed688ffc25bd20.pdf; Gilstrap, *supra* note 12, at 1272–73 (explaining that despite increasing potential liabilities associated with security breaches, software licensing agreements between vendors and businesses continue to limit vendors' liabilities); Oriola, *supra* note 3, a 514–16; Pinkney, *supra* note 4, at 46 (stating that the government has more than once protected software manufacturers from liability for harm caused by software failure); Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1558 (2005) (explaining that "those responsible for securing our personal data are rarely the ones who pay the cost of securing it"); Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?* 67 MD. L. REV. 425, 432–33 (2008) (listing the lack of significant risks to vendors in distributing insecure software as one reason why certain software is insecure).

incentive to produce better software.[71] But legal scholarship has paid less attention to this commercial market for security software and systems.[72] This Article attempts to fill that gap and its empirical analysis of an end-user license agreement ("EULA") (i.e., an agreement between the software vendor or developer and the software user) for such security systems demonstrates a similar liability shield in the contractual terms. On the face of these license agreements, the commercial user—the company that purchases the security software—bears the risk of loss in the event of a data breach. This contractual allocation of risk may be a perfectly reasonable choice for the licensee, for it can insure against that risk.[73] But to the extent the lack of accountability on the part of security software vendors undermines the goal of data security, this scenario should be unacceptable to the millions of consumers whose sensitive personal information, housed by the purchasers of commercial security systems, is consequently more vulnerable to theft and misuse.[74]

This Article proposes, as a solution, that the evolving role of consumer protection agencies in promoting information security can, and should, include a specific focus on commercial-security software. The Federal Trade Commission ("FTC"), in particular, has authority to protect consumers from "unfair" or "deceptive" conduct related to data security.[75] In regard to protecting data against unauthorized disclosure, the FTC mostly targets companies that fail to employ reasonable data security measures.[76] These failures, the FTC alleges, create a "substantial risk of harm" to consumers and constitute an "unfair trade practice."[77] A vulnerability in the security software used by a company to protect against data disclosure can also pose a "substantial risk of harm" to the consumers whose data is housed by that company, unless that vulnerability is detected and quickly patched.

This Article proposes, then, that regulators take the following

71. *See infra* Part I.A. (The "Unusual" Legal Cocoon Woven by Software Vendors).

72. Gilstrap's scholarship, for example, aims at security software, but not, specifically, the commercial market for such software. Gilstrap, *supra* note 12, at 1273.

73. *See generally* Garrie & Mann, *supra* note 51 (discussing the growing importance of cybersecurity insurance and related issues).

74. This is, of course, the classic "externalities" problem. *See* Bambauer, *supra* note 25, at 1030 ("Insecure [IT] users and providers do not suffer the full costs of the harms they generate.").

75. *See generally* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 963–66 (2016) (describing the common law approach of the Federal Trade Commission ("FTC")).

76. *Id.* at 957–58.

77. Amanda R. Moncada, *When a Data Breach Comes-a-Knockin', the FTC Comes A-Blockin': Extending the FTC's Authority to Cover Data-Security Breaches*, 64 DEPAUL L. REV 911, 919 (2015).

position:[78] if a commercial security software vendor knows or should have known of a vulnerability in its software, it could be subject to an "unfair" or "deceptive" trade practice claim if the vendor does not notify all of its licensees of that defect.[79] This proposal—a new take on "caveat emptor"—accomplishes at least two important objectives. First, it encourages information exchange, a strategy which is increasingly promoted as an effective weapon against cybercrime.[80] Not all software vulnerabilities would create such a significant risk of harm that the failure to disclose would qualify as an "unfair trade practice," but the risk of such a charge would presumably incentivize vendors to share vulnerabilities information. Second, to the extent commercial licensees are bound by contractual limitations on holding security software vendors accountable by filing suit, or are simply unwilling to bear the cost of litigation, regulatory agencies and consumers could step in and recover for the breach. Though new parties could recover for the breach, this limited definition of "unfair trade practice" would not unleash the floodgates to litigation and would account for the fact that software cannot be made wholly "secure." And surely the failure to disclose a known vulnerability would meet anyone's definition of "unfair."

This Article proceeds as follows: Part I begins with a discussion regarding the prevailing and persistent problem of software vendor immunity from responsibility for security failures, and proposed solutions. What follows is a summary, in broad strokes, of the functionality of a specific subset of software: commercial data security systems. This Article next describes its empirical analysis of commercial security software license agreements and observations regarding the respective liability of licensor and licensee in the event of a data breach, and discusses the reasons commercial buyers seem either unable or unwilling to hold the vendors responsible. Part II turns to this Article's proposal for breaking this impasse. First, it explains how encouraging "buyer beware" notifications fits well with the current legal trend promoting information exchange to combat cybercrime. Second, it discusses the FTC's current and evolving role in cybersecurity, explains why that role can readily encompass the regulation of commercial

78. Whether this position should be taken through rulemaking, or through "common law" development or other administrative means is beyond the scope of this Article.

79. Michael D. Scott proposes that the FTC can and should use its authority to take action against "unfair and deceptive trade practices" to prosecute vendors who distribute "insecure" software. Scott, *supra* note 70, at 482–83. The proposal herein is more specific and targeted—avoiding various troublesome issues such as defining "insecure"—and is based on a differing set of observations and arguments, including this Article's empirical analysis of commercial EULAs.

80. *See generally* Ford, *supra* note 67 (discussing the increase in frequency and sophistication of cyberattacks); *see infra* Part II.A. (discussing information sharing as a data-security measure).

software vendors who fail to notify of a vulnerability, and notes how state trade laws might also come into play. Third, it discusses why, in this context, targeted regulation with a limited option for private litigation is a better option than a pure liability regime.

I. DISCLAIMING RESPONSIBILITY

As this Part summarizes, scholars have well documented the fact that software vendors almost universally shield themselves from liability in the event of a breach of contract. One might expect, however, that in the commercial market for software and, in particular, for security software, a different pattern would emerge. Sophisticated companies purchasing billions of dollars of software and services to secure data would surely demand that the vendors of that software and those services share in the responsibility in the event of a data breach. But this Article's empirical analysis suggests otherwise.

A. The "Unusual"[81] Legal Cocoon Woven by Software Vendors

As has been observed through both qualitative[82] and empirical research,[83] software vendors almost universally employ standard form contract terms that disclaim warranties and limit liability in the event the software fails, resulting in a security breach.[84] Courts generally uphold contractual disclaimers of express and implied warranties in software license agreements.[85] Though a contractual disclaimer may be

81. Bambauer, *supra* note 25, at 1034 (referring to the prevailing use of contractual limitations on liability in software licenses).

82. *E.g.*, Michael L. Rustad, *Making UCITA More Consumer-Friendly*, 18 J. MARSHALL J. COMPUTER & INFO. L. 547, 579 (1999) ("One can read hundreds of click-wrap, Web site, shrink-wrap, and other mass-market transactions and have yet to find a single example of a software licensor willing to provide any warranty for its software.").

83. An analysis of standard form contracts licensing dozens of different types of software demonstrated that 90 percent disclaimed implied warranties and 89 percent disclaimed liability for consequential damages. Florencia Marotta-Wurgler, *What's in a Standard Form Contract? An Empirical Analysis of Software License Agreements*, 4 J. EMPIRICAL LEGAL STUD. 677, 703 (Dec. 2007). Express warranties were generally limited to conformance to specifications. *Id.* at 697. *See also* Robert J. Hillman & Ibrahim Barakat, *Warranties and Disclaimers in the Electronic Age*, 11 YALE J.L. & TECH. 1, 6 (2008–2009) (presenting empirical evidence of widespread use of disclaimers in consumer software license agreements).

84. *See generally* Marotta-Wurgler, *supra* note 81 (analyzing standard form contracts in software license agreements to document the prevalence of terms such as license scope and warranties); Rustad, *supra* note 82 (explaining the importance of the Uniform Computer Information Transaction Act, the statute which, among other things, enables expanding commercial practice in computer information transactions by commercial usage and agreement of the parties); Scott, *supra* note 70 (exploring why software vendors are not being held liable for distributing insecure code and why current laws regarding negligence and product liability do not concern insecure software).

85. Scott, *supra* note 70, at 437.

unenforceable because of fraudulent or negligent misrepresentations made by the vendor regarding the software's expected performance,[86] courts are generally reluctant to disregard a clear limitation of warranty in the terms of the contract.[87] The limited type of express warranty that is commonly found in the standard EULA is so "content-less" that, as one scholar observed, "[n]o reported decision has unequivocally held that a software vendor has breached an express warranty."[88] Though an "unconscionable" disclaimer may be unenforceable,[89] courts generally enforce limitations on liability in software license agreements[90] and infrequently find this exception applicable in the commercial context.[91] In a few jurisdictions the "failure of essential purpose" doctrine may be effective in overcoming a limitation of liability clause.[92] But for the most part, purchasers or licensees have no contractual recourse against the software vendor in the event of security failures.[93]

86. *See, e.g.*, J.C. Whitney & Co. v. Renaissance Software Corp., No. 99 C 3714, 2000 WL 556610, at *9–10 (N.D. Ill. Apr. 19, 2000) (denying a motion to dismiss based on disclaimer when the plaintiff sufficiently pled facts supporting fraud in the inducement claim).

87. *E.g.*, Lincoln Sav. Bank v. Open Solutions, Inc., No. C12-2070, 2013 WL 997894, at *3–5 (N.D. Iowa Mar. 13, 2013).

88. Scott, *supra* note 70, at 437.

89. U.C.C. § 2-302(1) (2004).

90. Bambauer, *supra* note 25, at 1034 ("End-user license agreements typically disclaim all liability on the vendor's part, and tort law has failed to impose a duty of care on software manufacturers.").

91. Scott, *supra* note 70, at 438.

92. *See generally* Gilstrap, *supra* note 12 (arguing that licensing agreements between vendors and businesses restrict vendors' liabilities, which allow them to avoid the liability following a security breach).

93. It has been noted that software vendors are effectively using the "risk allocation provisions of the [Uniform Commercial Code ("UCC")]" to shift liability for software failures to the users in the EULAs. Scott, *supra* note 70, at 427. Some, and perhaps the majority of courts apply the UCC to software transactions. *E.g.*, Holly K. Towle, *Enough Already: It Is Time to Acknowledge That UCC Article 2 Does Not Apply to Software and Other Information*, 52 S. TEX. L. REV. 531, 552–53 (2011) (explaining courts' evolution in applying article 2 of the UCC to software transactions). But many do not. *E.g.*, Lamle v. Mattel, Inc., 394 F.3d 1355, 1359 n.2 (Fed. Cir. 2005) (vacating the district court's grant of summary judgment on a claim against a licensing agreement for a board game); Architectronics, Inc. v. Control Sys., Inc., 935 F. Supp. 425, 432 (S.D.N.Y. 1996) (same); Attachmate Corp. v. Health Net, Inc., No. C09-1161 MJP, 2010 WL 4365833, at *2 (W.D. Wash. Oct. 26, 2010) (same). The emerging trend seems to be to consider the issue as being fact specific. Gabriela Rojas-Lozano v. Google, Inc., 159 F. Supp. 3d 1101, 1108–09 (N.D. Cal. 2016). Whether the UCC applies may be determinative in regard to various contract law issues. *E.g.*, Lorin Brennan, *Why Article 2 Cannot Apply to Software Transactions*, 38 DUQ. L. REV. 459, 465–66 (2000) (illustrating that the usual image of a software transaction as a customer who purchases pre-packaged software from a retail store falls within a "sale of goods" within article 2 of the UCC). But regarding risk-allocation provisions, it appears the distinction makes little difference. At common law, limitations of damages provisions, particularly a provision precluding recovery for consequential damages, in commercial contracts are generally enforceable, as are limitations on warranties.

These provisions pose a formidable obstacle against breach of contract liability in the event a hacker breaches a vulnerability in the software and compromises the user's data.[94] The lack of significant legal risk in the event of a security breach is one of the reasons insecure software is sold.[95] The solution, according to many scholars, is to mold traditional tort and contract law principles in such a way that software vendors can be held accountable notwithstanding the contractual disclaimers.[96] As most of these same scholars acknowledge, however, recovery based on a tort-based claim would encounter many, perhaps insurmountable problems, including, inter alia, the economic loss rule, which, in many jurisdictions, precludes recovery in tort where the injury does not produce pecuniary damages and there is no claim for physical injury, death, or other property damages.[97] And contractual limitations on liability are generally

94. *See generally* Gilstrap, *supra* note 12 (arguing that licensing agreements between vendors and businesses restrict vendors' liabilities, which allow them to avoid the liability following a security breach).

95. Scott, *supra* note 70, at 433 (exploring why software vendors are not being held liable for distributing insecure code and why current laws regarding negligence and product liability do not concern insecure software). There are other reasons, of course, including the cost and complexity of producing "error-free" code, as discussed above.

96. *E.g.*, Gilstrap, *supra* note 12, at 1280 (arguing for a broader adoption of the "failure of essential purpose" doctrine of contract law); Pinkney, *supra* note 5, at 69 (analyzing possible tort remedies); Michael L. Rustad & Thomas H. Koenig, *Cybersecurity Policy: Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 ISJLP 237, 239 (2007) ("We argue that companies have a duty to provide reasonable information security practices under the common law of torts."); Rustad & Koenig, *supra* note 70, at 239; Scott, *supra* note 70, at 441 (analyzing opportunities and barriers to the assertion of various tort claims); Daniel M. White, *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 FORDHAM L. REV. 369, 401 (2010) (arguing that government purchasers should demand "real" warranties from software vendors); Frances E. Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 746 (2005) ("[W]e argue for the adoption of a strict liability regime for software failure that produces physical injury and offer supporting arguments for why such a move is both necessary and sensible."). Aside from these private contractual issues, a related body of scholarship analyzes whether and to what extent software should be regulated. *E.g.*, Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 296–97 (2006) (explaining that most software programs are intricate and interrelated sequences of code, which create complex programs that might entice hackers); Peter Sloan, *The Reasonable Information Security Program*, 21 RICH. J.L. & TECH. 2, 25 (2014) (arguing that to establish a reasonable information security program, an organization should consider applicable legal requirements to implement security safeguards, including obligations to third-parties); David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 294 (2014) (discussing the efficacy of two modes of cybersecurity regulation using a mixed-methods empirical approach); *see generally* Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319 (2005) (exploring the increasing use of code and informational-technology architecture to deal with societal issues and problems).

97. *E.g.*, Scott, *supra* note 70, at 481 ("However, for the most common forms of injury caused by defective security software—loss of sensitive corporate and third party data—the economic loss rule will continue to bar most claims.").

enforceable.[98] As a result of all this, "[t]o date, despite an epidemic of computer security flaws, no plaintiff has recovered damages for cybercrimes enabled by flawed software under either a contract theory or under a tort theory."[99]

Though scholars, such as Stephen Gilstrap, specifically address security software, most scholarship regarding the lack of accountability for insecure software generically concerns mere "software."[100] Much of the data is drawn from consumer transactions.[101] The analyses of the reasons for the failure of the market to demand more secure software rest on principles applicable primarily in the consumer, "mass-market" setting.[102] For reasons discussed in these scholarly articles, it is perhaps not surprising that, in this particular market, the rule of *caveat emptor* generally rules.

One might expect, by way of contrast, that in the commercial market for software and, in particular, for security software, a different pattern would emerge. Sophisticated companies that purchase billions of dollars of software and services to secure data would surely demand that the vendors of that software and those services themselves share in the responsibility in the event of a data breach. But this Article's empirical analysis suggests otherwise.

B. Even More Unusual Commercial Security Software in the Same Cocoon

Information security for the commercial market ranges from desktop antivirus software used by a small law firm[103]—here overlapping with the consumer market—to complex beasts including cybersecurity

98. *E.g.*, *id.* at 437 (explaining that warranty disclaimers are presumed valid and construed strictly in favor of the buyer).

99. Rustad & Koenig, *supra* note 70, at 1567; *see also* Kuwahara, *supra* note 6 (describing Microsoft's "Trust Worthy Computing Initiative" to improve the security of its operating systems).

100. Gilstrap, *supra* note 12.

101. *E.g.*, Rustad, *supra* note 82, at 566. In Marotta-Wurgler's empirical study, over half of the standard form contracts were for "business" rather than consumer software, according to the author. Marotta-Wurgler, *supra* note 83, at 689. But given that the average cost of all products in the data set was $763, it does not appear that many of these contracts were for truly "commercial grade" software products.

102. *E.g.*, Bambauer, *supra* note 25, at 1033 (discussing the problem of externalities arising from the insecure use of "her" computer); Oriola, *supra* note 3, at 468 (arguing that the market can and does demand more secure software, using steps taken by Microsoft to reduce vulnerabilities in its Windows operating system as an example); Richard Warner & Robert H. Sloan, *Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access*, 2012 U. ILL. J.L. TECH. & POL'Y 45, 70–71 (discussing "Alice" and her decision regarding the purchase of secure versus insecure software).

103. This observation is based on the Authors' experience.

auditing services, data mining and analytics,[104] and various "proactive" measures intended to quickly detect and respond to attempted attacks such as software and hardware firewalls and intrusion detection and/or prevention systems.[105] Data security systems also include measures for "patching" leaks[106] and for otherwise minimizing the damage if a breach occurs.[107] The more complex data security system packages include a wide range of services including, inter alia, data security training[108] and various system and security support measures such as assistance in installation, maintenance, analysis, and response to security threats.[109] As with anything having to do with data, however, at the core of most, if not all, data security systems is software. Regardless of whether it is a simple script, or a complex data transformation procedure, software serves as the middleman between hardware and data. It handles the logic of how data is being processed and controls the access to hardware resources. Some information-security vendors offer software solutions only and others deliver so-called security appliances, which are basically dedicated stand-alone devices comprising of both hardware and software.[110]

Notwithstanding the variety of functions security software performs, the license agreements for that software are quite similar. The Authors of this Article performed text mining on the EULAs posted on the websites of close to 400 data security vendors, ranging from global conglomerates with data security divisions[111] to niche start-up companies,[112] which demonstrated a surprising similarity among the

104. *E.g.*, Craig et al., *supra* note 7, at 758–59 (discussing a survey of industry practices to show that more than 75 percent of firms offer data-mining, analytics, and detection systems).

105. *See generally id.* (explaining proactive cybersecurity measures to defend against "Advanced Persistent Threats").

106. *E.g.*, Oriola, *supra* note 3, at 468 (arguing that a "find-and-corrective" patch strategy to fend against unscrupulous groups or malicious hackers).

107. *E.g.*, Bambauer, *supra* note 25, at 1054 (explaining that in the event of an attack or a breach, using heterogeneous systems—like variegated code and hardware—as opposed to homogenous systems cause fewer parts of that system to be affected).

108. Craig et al., *supra* note 7, at 760.

109. *E.g.*, *Services Overview*, LOGRHYTHM, https://logrhythm.com/services/ (last visited Apr. 10, 2017) (offering security intelligence for private firms).

110. These devices offer features such as firewall, virtual private network ("VPN"), traffic shaping, content filtering, intrusion detection, network connectivity, packet inspection, etc. In essence, these are nothing other than specialized computers with a central processing unit, memory, storage, etc., that are designed and optimized to perform specific tasks.

111. *See, e.g.*, *Cyber Solutions*, LOCKHEED MARTIN, http://cyber.lockheedmartin.com/ (last visited May 10, 2017) (offering cybersecurity for private firms).

112. *See, e.g.*, *Open Source Application Security*, BLACK DUCK SOFTWARE, https://www.blackducksoftware.com/solutions/application-security (last visited May 28, 2017) (offering information security for private firms).

EULAs, and between these agreements and "mass market" consumer software license agreements.

Text mining is a semiautomated process aimed at extracting patterns from unstructured data sources, more specifically textual data.[113] Some of the most common applications of text mining include information extraction, topic tracking, summarization, categorization, and clustering. Like any analytical methodology, text mining follows a standardized process. In general, this process can be broken down into three sequentially organized steps: (1) establishing a corpus, (2) creating a term-document matrix ("TDM"), and (3) extracting knowledge.[114] Even though these steps are organized serially, the reciprocal relationships between them result in an iterative overall process. Before the TDM is created, the documents are preprocessed (i.e., cleansed) to eliminate as much "noise" from the documents as possible. The cleansing is iterative, and requires subject-matter expertise to identify relevant and redundant terms. The TDM relates the remaining terms to the documents based on selected measures, such as the frequency with which the term appears in the documents. The underlying assumption behind such an approach is that these frequencies can be used to illustrate (i.e., summarize) the essence of a given document.

The Authors of this Article obtained a corpus of 370 documents extracted from the vendor sites (the set contained only documents that were publicly available). The corpus contained a total of 1,444,017 words and 17,217 unique word forms. The EULAs varied in length from 170 words to almost 16,000 words. Because the documents significantly varied in length, the Authors computed a vocabulary density (i.e., a numerical value representing words commonly used in the documents in the corpus).[115] Here, the vocabulary density ranged from 0.120 to 0.571. Although one would expect software license agreements to contain common words because all contracts have core common elements (e.g., recitation of "consideration"), these figures demonstrate a very high degree of commonality. The Authors then cleansed the corpus and created the TDM by extracting the words "warranty," and "liability," and case/number variations of these words.[116]

---

113. GABE IGNATOW & RADA MIHALCEA. TEXT MINING: A GUIDEBOOK FOR THE SOCIAL SCIENCES 4 (2016).

114. Dursun Delen & Martin D. Crossland, *Seeding the Survey and Analysis of Research Literature with Text Mining*, 34 EXPERT SYSTEMS WITH APPLICATIONS 1707, 1711 (2008).

115. The number is obtained by dividing the total words by the unique words, which shows how many words will occur, on average, before a new word is encountered. Zachary Booth Simpson, *Vocabulary Analysis of Project Gutenberg* (May 2000), http://www.mine-control.com/zack/guttenberg/.

116. Specifically, first, we split the documents into sequences of tokens, which were identified

The TDM demonstrates the following regarding the warranty language of the 370 EULAs: 60 percent (225 EULAs) contained an "as is" phrase, including "as is and without warranty," "as is basis without warranty," or "as is without warranty/ies of any kind." 41 percent (152 EULAs) specifically stated "no warranty/ies" or "makes/provides no warranty of any kind." In the fifty EULAs that provided a warranty, the vendor guaranteed that the product "will perform substantially in accordance with the documentation." Almost half (177) of the EULAs, on the other hand, explicitly stated that the licensed products were not "error free."

66 percent (245 EULAs) limited the liability of the vendor in some regard. In these 245 agreements, the seller confirmed that "in no event shall/will [it] be liable" for various categories of damages. Specific disclaimers that appeared frequently included liability disclaimers for "loss of data" or "lost data" (145 EULAs), "loss of profits" or "lost profits" (197 EULAs), and "interruption of business operations" (76 EULAs). The seller's "entire liability" was often limited by the agreement to an amount not exceeding the amount paid for the software or services (171 EULAs).

On the face of these license agreements, then, the commercial user of security systems commonly used "as is" software, therefore at risk for bearing almost all costs—which, as discussed in the Introduction, can be considerable—in the event the software fails and a data breach occurs. And given the similarity of the EULAs' low vocabulary density, one could wonder how the buyer even knows what the phrase, "as is," really means. One would expect contracts or purchase orders for "mass-market" software, as with coffee pots or other standardized goods, to be boilerplate: neither the seller nor the buyer needs additional, contractual information to understand the nature of the exchange. This is also true for many services, ranging from lawn care (e.g., the grass will be cut when it reaches a certain height and buyer will pay a set fee) to a knee replacement (e.g., the natural joint will be removed and replaced and the insurance carrier billed for the surgeon's fee). But given the complexity

---

with non-letter characters (e.g., spaces between the words). Second, we transformed all the characters in our documents to lower case. Third, we filtered entity names (i.e., people, organizations, places, etc.) from the documents. Fourth, we generated n-grams (with n set to 7) from the document terms. An n-gram is essentially a series of consecutive tokens of length n, which are used fully to capture the terms of interest, which are "delivered" in the n-gram. Fifth, after creating the n-grams, we filtered the "stopwords" from our corpus. Stopwords are basically words that occur so frequently in text and speech that individually they do not add any specific meaning to the document, like "a." These may, however, have significance in conjunction with other terms, and that is why we created the n-grams first. The end product of these transformations was a term occurrence matrix that listed the total term (words and n-grams) occurrences, as well as document occurrences.

and variability of a "security system,"[117] and of each individual company's hardware, software, network, and business functions, it would seem that both the seller and the buyer would need additional, contractual language to effectuate a transparent exchange. Certainly, it is possible to employ a simple, formulaic contract for the exchange of complicated services. For example, a law firm retainer agreement is usually simple and somewhat "boilerplate." But the obligations and responsibilities of the attorney to the client need not be spelled out in detail in the contract: the applicable code of professional conduct contains a host of performance obligations the attorney must follow, and which the client is entitled to expect. The professional standard of care imposes its own set of performance requirements. But no such extracontractual professional standards exist in the security software world.[118] *Caveat emptor* appears to reign in this market, just as it does in the consumer market.

Of course, sophisticated commercial purchasers of enterprise security software and systems do not necessarily enter into these "boilerplate" license agreements. Some percentage of licensees surely negotiate more favorable terms, including more robust warranty provisions.[119] But for some reason—the disclaimers, limited warranties, limitations on recoverable elements of damages, and indefinite contractual description of expected performance in the EULAs being possible explanations—the software vendors are not being held accountable in the event of a data breach. Repeated searches of reported federal and state cases demonstrate a curious dearth of lawsuits by companies[120] against security

117. By "complexity," we mean here the variety in infrastructure configurations. No two corporate clients will have their computing infrastructure set up in the exact same way. The vendor will have tested its software performance in various simulated environments, but it cannot expect that the product will perform the exact same way in every environment. This complexity also increases due to the rate by which technologies come and go: customers may have legacy applications which are no longer compatible with current standards. In addition, as discussed earlier, new vulnerabilities surface all the time, which often means the vendors need to modify their products to accommodate for the new challenges. In short, security software functions in a complicated and dynamic environment.

118. *E.g.*, Rustad & Koenig, *supra* note 70, at 1590 ("It is theoretically possible that a software engineer could be held liable for computer malpractice but, to date, no court has held that a software engineer's failure to develop reasonably secure software constituted professional negligence."). Note that the company buying the software, on the other hand, may be subject to specific, regulatory standards for data security. Dana Rosenfeld & Donnelly McDowell, *Moving Target: Protecting Against Data Breaches Now and Down the Road*, 28 ANTITRUST 90, 90–93 (2014).

119. *See, e.g.*, Lockheed Martin Transp. Sec. Solutions v. MTA Capital Const. Co., No. 09 Civ. 4077 (PGG), 09 Civ. 6033 (PGG), 2014 WL 12560686, at *13 (S.D.N.Y. Sept. 16, 2014) (explaining that in a contract for the purchase of a $300 million security system for the New York metropolitan area transportation system, Lockheed warranted, inter alia, to provide equipment and software "fit for the MTA's intended use" and "free from defects in design, material and workmanship").

120. Consumers seem somewhat more apt to seek compensation from their security software

software and services vendors arising from a data security breach.[121] The occasional lawsuit between a purchaser and a security software vendor involves, instead, a dispute about contractual obligations other than securing data.[122] One could wonder why companies, collectively spending billions of dollars on security software and systems, are not fighting back.

C. Commercial Licensors: Unable or Unwilling to Hold Vendors Accountable?

Although identifying the many reasons any one company accepts the status quo is an impossible task, some common themes can be discerned. First, regarding those companies that accept the "boilerplate" terms which effectively shield vendors from liability, this contractual allocation of risk may, at first blush, seem to be a perfectly reasonable choice for the licensee, for it can insure against that risk.[123] But because of the "unpredictable probability and costs" of data breach, cybersecurity insurance is particularly expensive.[124] Because if insured, the policy premium may not come close to covering the entire loss to the

---

vendors when that software malfunctions in some way. *See generally* Boyd v. Avanquest N. Am. Inc., No. 12-cv-04391-WHO, 2015 WL 4396137 (N.D. Cal. July 17, 2015) (denying a software manufacturer's motion to dismiss a class action seeking damages from an alleged breach of contract); Haskins v. Symantec Corp., No. 13-cv-0183-JST, 2013 WL 6234610 (N.D. Cal. Dec. 2, 2013) (dismissing the plaintiff's suit for false representations by a computer security software manufacturer); Bilodeau v. McAfee, Inc., No. 12-CV-04589-LHK, 2013 WL 3200658 (N.D. Cal. June 24, 2013) (granting the plaintiff leave to amend the complaint against a computer security software manufacturer); Rottner v. AVG Technologies USA, Inc., 943 F. Supp. 2d 222 (D. Mass. 2013) (granting a software manufacturer's motion to dismiss a class action complaint claiming false representation); Gross v. Symantec Corp., No. 12-00543 CRB, 2012 WL 3116158 (N.D. Cal. July 31, 2012) (granting a software manufacturers' motion to dismiss a class action for fraudulent inducement, express warranty, breach of contract, and breach of implied covenant).

121. The few, related cases found include *National Union Fire Insurance Co. v. Trustwave Holdings, Inc.*, No. CN14C-10-160 MMJ (CCLD), 2016 WL 2354621 (Del. Super. Ct. May 3, 2016), in which the subrogee sued a qualified security assessor for allegedly failing to ensure compliance with standard measures for securing credit card transactions, resulting in a breach, and *Cotton Patch Café, Inc., v. Micros Systems*, No. MJG-09-3242, 2012 WL 5986773 (D. Md. Nov. 27, 2012), in which the defendant, vendor of Point-of-Sale systems to retailers, allegedly installed a server containing malware which hackers used to access data.

122. *See generally* i.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002) (granting a motion for summary judgment in favor of the defendant, reasoning that the plaintiff could not be awarded specific performance because the software was not irreplaceable); Piper Jaffray & Co. v. SunGard Sys. Int'l, Inc., No. 04-2922 (RHK/JSM), 2004 WL 2222322 (D. Minn. Sept. 30, 2004) (granting a motion to dismiss the plaintiff's breach of contract claims against a software manufacturer).

123. *See generally* Garrie & Mann, *supra* note 51, at 385 (arguing that one of the difficulties associated with the high costs of cybersecurity insurance is choosing between spending money on cybersecurity insurance or investing in cybersecurity technology).

124. *Id.* at 384.

company.[125]

Rather than insure against an uncertain risk, companies could negotiate more favorable terms with security vendors, demanding meaningful warranties and reallocations of the risk of loss. These are not, after all, individual consumers buying Microsoft operating systems with security flaws.[126] Presumably, as a consequence, vendors would provide more secure software, but this "better" software would come at a higher cost.[127] In the end, however, companies may simply be unwilling to pay this higher cost to ensure greater protection. Although the issue is a matter of some debate,[128] it would appear most observers believe companies underspend on cybersecurity overall.[129]

Compounding the issue is the fact that, for any one business, the risk of a large-scale data breach and resulting loss is small.[130] If a breach occurs, some portion of the loss to the company may be recouped through insurance coverage.[131] If the publicity of the breach causes a drop in the company's share price, that drop may be just temporary.[132] The net cost of the breach to the company may be a very small percentage of annual revenues.[133] Therefore, paying more for better security software is just not worth the cost for companies.[134]

---

125. *E.g.*, Hackett, *supra* note 52 (reporting information from Target's financial statements showing, for 2014, $191 million in losses caused by a data breach, offset by $46 million in insurance receivable).

126. *See generally* Kuwahara, *supra* note 6 (discussing impediments to liability and proposing various possible solutions).

127. *Cf.*, Oriola, *supra* note 3, at 472 (arguing that the lack of a demand for more secure, and presumably more costly, software in the consumer market is due, in part, to the fact that software cannot be wholly secure).

128. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1510 (2013).

129. *Id.* at 1511 ("Most observers believe that firms are underinvesting—and are missing the mark by a wide margin.").

130. *Verizon's Report*, *supra* note 16. Similarly, in 2016, pursuant to IBM's 2017 Cyber Security Intelligence Index Report, more than 54 million "security events" were detected by the clients' systems or networks, whereas the average client experienced only ninety-three attacks out of these events. 2017 IBM X-FORCE THREAT INTELLIGENCE INDEX, IMB SECURITY 3 (Mar. 2017), http://www-03.ibm.com/security/data-breach/cyber-security-index.html. In other words, only a fraction of a percent of the total security events represents a significant level of severity.

131. Garrie & Mann, *supra* note 51, at 380–81 (arguing that cybersecurity coverage is needed given the high cost of data breach). Thus, the risk allocation provisions of the EULA's would be acceptable: the buyer accepts the risk of loss and simply insures against it.

132. Kvochko & Pant, *supra* note 38 (illustrating the momentary stock declines of Home Depot, Sony, Target, and Sears following a publicized data breach).

133. Hackett, *supra* note 52 ("From Sony to Target, big companies that were hacked felt barely a dent to their bottom line.").

134. The valuation exercise may be greatly compounded by the externalities problem: "The fact that many costs of cyber-attacks are externalized is enormously significant." Sales, *supra* note 128, at 1526.

In any event, similar to consumers, those companies bound to the same types of vendor-protective licensees are unable to hold software vendors accountable. Contractual limitations on liability are generally enforceable, particularly in commercial transactions.[135] As with claims brought by individuals arising from data breach, tort claims by commercial buyers would encounter many, perhaps insurmountable problems, including, inter alia, the economic loss rule.[136] In many jurisdictions, the economic loss rule precludes recovery in tort where the injury is pecuniary and no claim exists for physical injury, death, or other property damages.

Even when a data breach occurred and the company that experienced the breach is not precluded by contract from seeking damages from a security vendor, realistically identifying that vendor as a culpable party to the breach is beset with a number of technical and legal difficulties. On the technical side, for the company to even investigate whether the breach may have implicated a specific software is often a trial-and-error game. Some evidence of what occurred can be collected through digital forensics, but only if the attackers have not removed all the traces of their activity by, for example, wiping the system event logs. But even if there is clear evidence that the attack came through a specific software package, the company itself can usually only examine the binaries of a given piece of software because the software is commonly purchased and installed in proprietary, closed-source code. In other words, symptoms of a suspected vulnerability may be detectable, but only the vendor can identify the root cause because it is hidden behind the code. In a potentially adversarial situation, obtaining the vendor's helpful intervention seems unlikely.

From the legal point of view, proving "cause in fact" will prove difficult because multiple access points to the data are likely[137] and multiple intervening actions between the coding of the software and the breach likely occurred.[138] Proximate cause is also a very sticky wicket,[139] particularly given the difficulty of ascribing foreseeability to the consequences of any particular software error. It might be reasonably

135. *E.g.*, Scott, *supra* note 70, at 437 (explaining that warranty disclaimers are presumed valid and construed strictly in favor of the buyer).

136. *Id.* at 481 ("However, for the most common forms of injury caused by defective security software—loss of sensitive corporate and third party data—the economic loss rule will continue to bar most claims.").

137. *E.g.*, Rustad & Koenig, *supra* note 70, at 252 (arguing that most data disasters have occurred because of weak access controls in "the terrestrial world" rather than through hacking in cyberspace).

138. Hahn & Layne-Farrar, *supra* note 96, at 316.

139. Rustad & Koenig, *supra* note 70, at 1602.

foreseeable that a breach might occur, given what is widely known about cybercrime today,[140] but the industry knows very little about what cybercriminals do with all the purloined data unless a criminal investigation brings it to light in a particular case.[141] Thus, defining what damages are "reasonably foreseeable" is problematic: "Even if the plaintiff establishes actual cause, there may not be recovery if the causal relationship between the defendant's breach and the plaintiff's losses is too remote."[142]

Despite all these hurdles, one would presume that if the lack of data security were untenable, sophisticated commercial buyers would take action. Buyers would demand favorable contract terms, notwithstanding some price increase, or corporate counsel would have brought viable claims in court (e.g., claims of negligent misrepresentation or fraud by nondisclosure),[143] notwithstanding restrictive contract terms. Sophisticated forensic experts would have identified software vulnerabilities and opined, in court, that that particular defect was a cause of the breach. Data would be more secure. But this hypothetical surely does not look like the security world today.[144]

None of this is happening because, apparently, for any or all of the reasons proposed above, the situation is tenable, insofar as business is concerned. Unless some external force propels a change, there is little reason to believe the commercial buyers are going to step up to the plate and demand better security software. The consumers whose data those companies house are therefore largely left out in the cold.[145] It has been observed: "The problem is that those responsible for securing our personal data are rarely the ones who pay the cost of securing it and in

140. *See generally* Meiring de Villiers, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 HASTINGS COMM. & ENT. L.J. 149 (2008) (presenting an analysis of civil liability for the failure to safeguard confidential information).

141. *E.g.*, Shahani, *supra* note 32 (reporting on a federal indictment naming three men who were believed to have hacked JPMorgan Chase).

142. Rustad & Koenig, *supra* note 70, at 1602.

143. Cotton Patch Café, Inc., v. Micros Sys., No. MJG-09-3242, 2012 WL 5986773, at *3 (D. Md. Nov. 27, 2012).

144. *Supra* Part I (recognizing that software vendors almost universally shield themselves from liability in the event of a breach of contract).

145. But in *Strautins v. Trustwave Holdings, Inc.*, a class of plaintiffs sued the data security vendor whose products and services were used by the South Carolina Department of Revenue after a breach of the department's records resulted in unauthorized access to taxpayer records. 27 F. Supp. 3d 871, 872–73 (N.D. Ill. 2014). The plaintiffs brought claims alleging violations of the Fair Credit Reporting Act, negligence, and invasion of privacy and contract (third-party beneficiary). *Id.* at 873–74. The court dismissed the case based on a finding of lack of an actual injury sufficient to support standing. *Id.* at 877–78. The court noted, in dicta, that Trustwave, the security software vendor, was not a "consumer reporting agency" subject to the Fair Credit Reporting Act. *Id.* at 882. It is unknown whether any of the other claims would have survived.

many cases are not the same people with whom we have entrusted our data in the first place."[146] Another problem is that those companies with which consumers have entrusted their data (i.e., retailers, hotels, and other consumer product and service providers) are not able, or perhaps not willing, to ensure those responsible for securing consumer data (i.e., security software vendors) actually secure it or to take any responsibility after that data is stolen. But should consumers just concede to this situation?

II. IT IS UNFAIR NOT TO TELL

This Article proceeds on the assumption that something should be done to alter the prevailing relationship between security software vendors and commercial licensees of security software and systems. Something must be done to incentivize the development of better commercial security systems, with or without the participation of the companies buying those systems, to better protect consumer and client data. This Article's proposal for accomplishing these objectives relies on a combination of required information disclosure from security software vendors and penalties based on existing unfair trade laws in the event of nondisclosure. Specifically, this Article proposes that regulators consider deeming it an "unfair trade practice" if a commercial security software vendor knows or should have known of a vulnerability in its software, but does not notify all of its licensees of that known defect.

Part II.A discusses the weaknesses of the existing, voluntary information-sharing programs and the benefits to be gained by disclosing cybersecurity information, including software-vulnerability information. Part II.B proposes that a required vulnerabilities disclosure fits well within existing jurisprudence defining "unfair trade practices" in the cybersecurity arena.

A. Information Sharing as a Data Security Measure

Cybersecurity information sharing ("CIS")[147] has its detractors, certainly,[148] but the prevailing view notes that by sharing information,

146. Mark Rasch, *How Much Does a Security Breach Actually Cost? And Who Pays for It?*, REG. (July 15, 2005, 6:02 AM), http://www.theregister.co.uk/2005/07/15/who_pays_for_security_breaches.

147. Cybersecurity information sharing ("CIS") can be defined as "the collection, analysis, distribution, and utilization of any information relevant to a cybersecurity threat." Ford, *supra* note 67, at 123.

148. *See, e.g.*, Derek E. Bambauer, *Sharing Shortcomings*, 47 LOY. U. CHI. L.J. 465, 468–78 (2015) (critiquing the current policy focus of CIS on information sharing). CIS that involves sharing information with the government also raises privacy concerns. For example, the Center for Democracy and Technology, a nonprofit think tank that advocates for online civil liberties, opposed

companies will be better able to counter a security problem that is otherwise, perhaps, virtually intractable.[149] In any event, CIS as a tool against cyberthreats has firmly arrived on the scene.

There are many reasons why CIS among data-theft targets is an effective deterrent. Attacks on networked computers continue to increase in number and in sophistication.[150] Large-scale breaches of corporate data are increasingly attributable to an advanced persistent threat ("APT"), not some opportunistic "hack."[151] An APT exists when the attacker (1) has an above-average expertise to carry out more sophisticated exploits, (2) is determined to achieve his or her goal, and (3) also has sufficient resources to support his or her actions. An APT family of threats usually identifies targeted attacks that take place over a prolonged period of time where the attacker will not give up before achieving his or her goal. In contrast, opportunistic attacks usually result from the attacker's consistent scan of the environment and an impulsive attack when the opportunity presents itself. Historically, APT was a term reserved for statewide cyberattacks. But recently, the industry identifies a hack as an APT when the primary goal of the hack is simply to steal data. The technical sophistication of an APT is often enhanced by adding social-engineering strategies, like spear phishing, to the mix.[152]

By sharing information about the nature and target of past attacks, companies may become aware of potential vulnerabilities of which they

---

the Consumer Information Security Act ("CISA") on the grounds that the statute would facilitate government surveillance and other individual privacy violations.

149. *E.g.*, Sales, *supra* note 128, at 1546 ("Effective cyber-security depends on the generation and exchange of information.").

150. *E.g.*, Ford, *supra* note 67, at 121 (surveying the incidence and cost of increased networked computer targeted attacks); Ariana L. Johnson, *Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation*, 20 N.C. BANKING INST. 277, 283 (2016) (explaining further why financial institutions are particularly vulnerable to attacks).

151. Advanced persistent threat ("APT") implies a targeted and systematic attack, whereas an "opportunistic" hack is not.

152. Phishing is a type of social engineering—a high-tech scam that uses e-mail or websites to deceive people into disclosing personal information useful in identity theft, such as credit card numbers, bank account information, social security numbers, passwords, or other sensitive information. Spear-phishing attacks target a smaller, more select group of individuals (e.g. users of a specific website, members of an organization, etc.) with the primary goal of bypassing the security perimeter of the target organization. Spear phishing is different from regular phishing in that it uses contextual information relevant to the recipient and spear phishing appears as if it was sent from somebody within the organization. FIREEYE, INC., SPEAR-PHISHING ATTACKS WHY THEY ARE SUCCESSFUL AND HOW TO STOP THEM 3 (2016), https://www2.fireeye.com/rs/fireye/images/fireeye-how-stop-spearphishing.pdf; *see generally* EUROPEAN LAW ENFORCEMENT AGENCY, INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2016 REPORT (2016), https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016 (identifying spear phishing as a key threat and recommending various protocols for future developments in spear phishing).

had no prior knowledge; gain understanding of the methods used by the hackers (the "tactics, techniques, and procedures" ("TTPs")); and be better able to design effective defenses against those TTPs.[153] Detecting threats and vulnerabilities and investigating the TTPs is costly and time consuming.[154] Any one company can afford only so much analysis. With widespread sharing of the results of cybersecurity analysis, every company, at a very low cost, can acquire a much more robust inventory of threat and vulnerability information than it could ever achieve with its own resources.[155] The same is true for effective response and mitigation actions: the exchange of information about these issues increases the speed and accuracy with which companies can react to attacks.[156] TTPs are constantly evolving, such that effective data security requires constant innovation. Measures that encourage companies to share information about perceived and actual security threats, and to cooperate in developing new technologies, are likely to improve data security for all.[157] Accordingly, a wide range of scholars argue that "intelligence dissemination" is likely one of the best tools for enabling an effective cybersecurity strategy.[158]

Many different varieties of CIS are certainly in use today. Government efforts to improve national security, including the security of critical industries, drive most of the CIS. These efforts include, inter alia, the provision by government agencies of cyberthreat and vulnerability information to industry about cyberthreats and vulnerabilities, and the encouragement of information exchange between government and private industries. Thus, for example, the Clinton administration encouraged the creation of industry-specific Information Sharing and Analysis Centers,[159] which share threat and mitigation information with

153. Ford, *supra* note 67, at 123.

154. *Id.* at 124.

155. *Id.* at 125.

156. Johnson, *supra* note 150, at 294.

157. *See* S. REP. NO. 114-32, at 2 (2015) ("The [CISA] believes that 'such increased sharing will drive public and private sector cybersecurity efforts to develop key new technologies and processes.'").

158. *See, e.g.*, Craig et al., *supra* note 7, at 726 (arguing that an effective proactive cybersecurity strategy should focus on real-time detection, attribution of threat actors, flexibility of response actions, and intelligence dissemination); Ford, *supra* note 7, at 131 (noting that attributing malicious attacks requires correlation with other intelligence sources); Hahn & Layne-Farrar, *supra* note 96, at 353 ("The best step policymakers could take immediately would be to encourage reporting of security breaches."); *see generally* Johnson, *supra* note 150 (suggesting that utilizing cyberintelligence may create better network monitoring and more effective detection and mitigation).

159. *E.g.*, WHITE PAPER: THE CLINTON ADMINISTRATION'S POLICY ON CRITICAL INFRASTRUCTURE PROTECTION: PRESIDENTIAL DECISION DIRECTIVE 63, at 10 (May 22, 1998), http://csrc.nist.gov/drivers/documents/paper598.pdf (noting that the creation of information

industry partners and with the government.[160] Late in 2015, President Obama signed the Computer Information Sharing Act, which directs the United States Department of Homeland Security ("DHS") and other government agencies to provide information to the private sector and allows private-sector companies to share "cyberthreat indicators" and defensive measures with each other and with the government in exchange for immunity from liability from antitrust and other laws.[161] Wholly private initiatives to promote CIS have also emerged, including, for example, the Cyber Threat Alliance, which welcomes "all organizations" to share in cybercrime threat intelligence.[162]

Information on software vulnerabilities is especially critical in improving data security.[163] To this end, DHS' United States Computer Emergency Readiness Team sponsors a national vulnerabilities database ("NVD") (i.e., a compilation of standards-based, or defined vulnerabilities, reported voluntarily).[164] Though the database currently contains almost 80,000 identified vulnerabilities,[165] by most accounts the list is wholly inadequate.[166] The efficacy of the program depends, to a large extent, on the willingness of software vendors to disclose vulnerabilities, or "bugs," of which they have become aware, but software vendors may be reluctant to publicly disclose vulnerabilities for many reasons.[167] Disclosure may cause a vendor to lose customers and

---

sharing and analysis centers in private sector industries is "strongly encouraged").

160. *About NCI*, NAT'L COUNCIL ISACS, http://www.nationalisacs.org/about-nci (last visited May 10, 2017).

161. THE DEP'T OF JUSTICE, THE DEP'T OF HOMELAND SEC., GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, at 4 (2016).

162. *McAfee and Symantec Join Fortinet and Palo Alto Networks as Co-founders of the Industry's First Cyber Threat Alliance*, CYBER THREAT ALLIANCE, https://cyberthreatalliance.org/pr/mcafee-and-symantic-join-fortinet-and-palo-alto-networks-as-co-founders.html. The founding members of Cyber Threat Alliance were Fortinet, McAfee, Palo Alto Networks, and Symantec. Whether, and to what extent, private CIS is discouraged or even prohibited by antitrust and other laws is outside the scope of this Article.

163. Oriola, *supra* note 3, at 481 ("It is sacrosanct that vulnerabilities detection research is invaluable to computer and network security, as it facilitates the discovery and disclosure of latent 'zero day' or new vulnerabilities that could be exploited by unscrupulous hackers if left uncorrected.").

164. NAT'L VULNERABILITY DATABASE, https://nvd.nist.gov (last updated Mar. 20, 2017).

165. *Current CVSS Score Distribution for All* Vulnerabilities, CVE DETAILS, http://www.cvedetails.com/ (last visited May 6, 2017).

166. Other vulnerability databases exist on the market as well. For example, the open source vulnerability database reports over 120,000 vulnerabilities. The exact number is unknown. For more information, see *The Duality of Expertise: Microsoft*, OSVBD (Feb. 28, 2017), https://blog.osvdb.org/ (last visited May 6, 2017) (providing information about security vulnerabilities in computerized equipment).

167. With some exceptions, reported vulnerabilities are disclosed to the public within forty-five

potential buyers,[168] whether the vulnerability is fixed, or patched.[169] Creating the patch can be expensive, which means there may be a disincentive to do so.[170] Disclosure may increase the risk that a hacker can exploit the code, whether or not the vulnerability is patched.[171]

The vendor is certainly not the only candidate who can report a vulnerability: users and "independent security researchers" of all types, including malicious hackers, also engage in vulnerabilities-detection research.[172] These individuals or entities may report the vulnerability to the NVD, make the information public,[173] report to the vendor, or sell the information to the highest bidder in the market for software vulnerabilities. Sellers in this market include, for example, brokers who legitimately buy and sell information, as well as criminal hackers. And buyers in this market range from software vendors or users (e.g., both Facebook and Mozilla have "bounty hunter" programs for vulnerabilities detection)[174] to government agencies.[175] This market raises many concerns, not the least of which is the threat of criminal blackmail by a hacker in possession of a "zero-day" vulnerability key to the preservation of national security.[176] For purposes of a user obtaining accurate information on software vulnerabilities, the concern is that these black markets are inefficient, because they are "unregulated, unstructured, and ill-defined."[177]

A number of the problems with existing information exchange programs would be solved, or at least alleviated, if the industry strongly encouraged—with the threat of an unfair trade practice charge—commercial security software vendors to report vulnerabilities to their

days after the initial report. *Vulnerability Disclosure Policy*, SOFTWARE ENGINEERING INST., http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm? (last visited May 10, 2017).

168. Rahul Telang & Sunil Wattal, *An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price*, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 544, 548 (Aug. 2007), http://www.heinz.cmu.edu/rtelang/tse.published.pdf.

169. *E.g.*, Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1063 (2011) (positing that vendors face reduced reputational or market pressures to improve security when vulnerabilities are disclosed).

170. *Id.* at 1065.

171. *Id.* at 1064.

172. *Id.* at 1065.

173. For example, Google, through its Project Zero, uncovers and reports previously undisclosed computer software vulnerabilities. Chris Evans, *Announcing Project Zero*, GOOGLE ONLINE SECURITY BLOG (July 15, 2014), https://googleonlinesecurity.blogspot.de/2014/07/announcing-project-zero.html.

174. Bambauer & Day, *supra* note 169, at 1066.

175. *Id.*; *see generally* Bambauer, *supra* note 25 (advocating for and proposing governmental regulation for known and unknown threats).

176. Bambauer & Day, *supra* note 169, at 1062.

177. Oriola, *supra* note 3, at 512.

licensees. This threat would reduce the ineffectiveness that stems from the "voluntariness" that plagues the NVD and other private information-exchange programs.[178] Although reputational damage may still result from disclosure to licensees, this limited disclosure would presumably reduce the risk that competitors could use vulnerabilities information to the disadvantage of the vendor, or that hackers could exploit the vulnerability. To the extent the vulnerabilities markets include vendors and software users, this regularized exchange of information would be a practical first step in regulating one corner of the vulnerabilities market, surely a beneficial result.[179]

B. Data Security and Unfair Trade Laws

The FTC is authorized to enforce section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits "unfair or deceptive acts" that affect commerce.[180] Between 2002 and 2015, the FTC exerted this regulatory authority in sixty enforcement actions against companies that "engaged in unfair or deceptive trade practices that put consumers' privacy at unreasonable risk."[181] Specifically, in these actions, the FTC protects the privacy of consumers' data.[182] Scholars argue about the proper administrative tools that the FTC should use (e.g., adjudication as opposed to rulemaking),[183] but agree that the FTC has a legitimate role in improving data privacy. Indeed, by some measures, the FTC has "evolved into the broadest and most powerful data protection agency in the United States."[184]

An act may be "unfair or deceptive," causing the privacy of consumer data to be put at unreasonable risk, if, for example, a company fails to follow its privacy policies by engaging in the unauthorized collection or

178. *E.g.*, *Become a Member*, CYBER THREAT ALLIANCE, http://cyberthreatalliance.org/membership/ (last visited May 10, 2017) (recruiting a diverse membership representative of the cybersecurity industry).

179. Oriola, *supra* note 3, at 514 ("[T]here is a good case for discouraging underground markets in software vulnerabilities due to their propensity for perpetuating malicious hacking activities.").

180. 15 U.S.C. § 45(a)(1) (2012).

181. FED. TRADE COMM'N, 2015 PRIVACY AND SECURITY UPDATE 4 (2015), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2015/privacy_and_security_data_update_2015-web_0.pdf. The FTC's authority in this regard was upheld in *FTC v. Wyndham Worldwide Corp.* 10 F. Supp. 3d 602, 612 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

182. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2236 (2015).

183. *See, e.g.*, Hurwitz, *supra* note 75, at 988 (noting that "the FTC's current approach is arguably the most aggressive use of adjudicatory procedures to develop a substantive area of law that any agency has embraced in the modern era of administrative law").

184. Hartzog & Solove, *supra* note 182, at 2236.

distribution of data,[185] or if a data-security measure fails. Thus, for example, the FTC claimed that Lifelock, Inc., an American identity theft protection company, made deceptive claims about its identity theft protection services, and investigated Oracle, a computer technology company, when the company failed to properly notify consumers of a known security risk in software updates.[186] Pursuant to FTC guidance, a company housing consumer data may engage in an "unfair" trade practice if it fails to provide reasonable security measures to protect that data against unauthorized disclosure.[187]

The FTC Act defines an "unfair" act as one that (1) causes actual or likely substantial injury to consumers; (2) consumers cannot reasonably avoid; and (3) is not outweighed by countervailing benefits to consumers or to competition.[188] The FTC's position is that "an injury may be sufficiently substantial . . . if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[189] The actual "act" that is alleged to be unfair, in regard to the security of consumer data housed in corporate files, is the failure of the company to take "reasonable" security measures.[190]

Thus, in *FTC v. Wyndham Worldwide Corp.*, for example, the agency charged that Wyndham, inter alia, "failed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess'" and "did not require the use of complex passwords for access to the Wyndham-branded hotels' property management systems and allowed the use of easily guessed passwords."[191] As charged by the FTC, Wyndham's "unfair acts" resulted in substantial, actual injury: three data breaches and the exposure of over 600,000 consumer card numbers, causing fraudulent, unreimbursed credit card charges, among other costs to the consumers.[192]

185. Moncada, *supra* note 77, at 918–19.

186. *Privacy and Security Update*, *supra* note 181, at 4.

187. Timothy E. Deal, *Moving Beyond "Reasonable": Clarifying the FTC's Use of Its Unfairness Authority in Data Security Enforcement Actions*, 84 FORDHAM L. REV. 2227, 2240 (2016) (noting that complaints frequently allege a defendant's failure to employ adequate data security measures); *Privacy and Security Update*, *supra* note 181, at 4.

188. 15 U.S.C. § 45(n) (2012).

189. Fed. Trade Comm'n, *Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction* (1980), *reprinted in* Int'l Harvester Co., 104 F.T.C. 949, 1072–88 (1984).

190. Deal, *supra* note 187, at 2240.

191. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 624 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015). Similar allegations of "failed" or inadequate data security measures were made in administrative actions against GMR Transcription Services, Inc., and LabMD, Inc., among others. *Privacy and Security Update*, *supra* note 181, at 4.

192. *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 623. On appeal, the Third Circuit rejected Wyndham's argument that "unfair" required something in addition to the specific statutory

Just as a company's deficient security measures can cause harm to hundreds of thousands of consumers, so, too, can vulnerabilities in the security software used by that company to protect consumer data.[193] According to one report, only as few as just ten vulnerabilities (among thousands known), in a company's infrastructure led to the theft of hundreds of millions of consumer records in 2015.[194] When a company's software vulnerability causes a substantial breach and data theft, it seems "unfair" if consumers suffer injury and are not subsequently remedied.

An act can also be "unfair" if it caused "likely substantial injury to consumers."[195] What is sufficiently probable to constitute "likely" injury is a bit murky, but the FTC Act clearly draws a distinction between substantial injury that "has" occurred and an injury that "may" occur.[196] In regard to data security, the FTC has utilized the definition of "unfair" to launch an investigation of Verizon arising from its shipment of routers with outdated encryption standards, leaving customers "vulnerable to hackers."[197] Pursuant to its statutory authority, the FTC could also investigate a security-software provider if a vulnerability in its software is likely to cause widespread injury to consumers. Not every software vulnerability is of a type or magnitude that poses a "likely" threat of substantial harm, but there is data available that the FTC could use to evaluate the risk of breach.[198]

What, specifically, the software vendor has done that is "unfair" when

---

elements, but did not otherwise rule on the lower court's findings regarding the sufficiency of the allegations. *Wyndham Worldwide Corp.*, 799 F.3d at 245. Wyndham also claimed that consumers could "reasonably avoid" this harm by demanding that their card issuers rescind the unauthorized charges, but the court, in ruling on the motion to dismiss, declined to make what would in effect be this ruling as a matter of law. *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 625.

193. Bambauer, *supra* note 25, at 1024 ("The combination of vulnerabilities and Internet exposure means that failures of seemingly invulnerable systems are legion.").

194. McCandless, *supra* note 40; *Verizon's Report*, *supra* note 16.

195. 15 U.S.C. § 45(n) (2012).

196. Hartzog & Solove, *supra* note 182, at 2279–80.

197. Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., FTC, to Dana Rosenfeld, Kelley Drye (Nov. 12, 2014), https://www.ftc.gov/system/files/documents/closing_letters/verizon-communications-inc./141112verizonclosingletter.pdf.

198. For example, each vulnerability in the national vulnerabilities database is evaluated using the common vulnerability scoring system ("CVSS"). The framework is composed of three indicator groups: base (the intrinsic qualities of a vulnerability), temporal (the characteristics of a vulnerability that change over time), and environmental (the characteristics of a vulnerability that are unique to a user's environment). Each vulnerability is scored on a scale from zero to ten based on the base metrics, with "ten" being most severe. The CVSS scores of the ten vulnerabilities through which the vast majority of consumer records were stolen in 2015 range between 4.3 and 7.5, with the majority being in the upper end of the interval. *See also NVD CVSS Support*, NVD, https://nvd.nist.gov/cvss.cfm (last updated Jan. 25, 2017) (providing an open framework for communicating the characteristics and impacts of IT vulnerabilities).

it licenses insecure software is another issue. Just as a company is generally required to take "reasonable" security measures, a security-software vendor could be required to license "reasonably secure" software. Pursuant to such a standard, a security-software vendor would be subject to FTC action should a substantial risk of harm result if its software is not "reasonably secure." Defining "reasonable security measures" is no simple task, however, and attempting to define "reasonably secure software" is probably *even more* difficult.

As noted throughout this Article, "[b]ugs happen."[199] But usually, security software "fails" because someone intentionally and repeatedly tries to make it fail.[200] The notion of imposing specific bounds on whether that software is somehow "flawed" in such a situation is perhaps somewhat attenuated. Surely, if a windshield has design flaws such that the windshield shatters unexpectedly when a driver drives the car down the road, the manufacturer should be responsible for the consequences. If, however, the windshield shatters only because someone has repeatedly hit the glass with a hammer, perhaps the outcome, and the responsible party, is not so clear.

Similarly, the fact that a hacker has selected a particular code to infiltrate is largely a matter of chance.[201] But once a company identifies a vulnerability, all objections related to "chance" fall away. Software with a known and material security vulnerability does not fit within any definition of "reasonably secure." A software code cannot be made completely error free, ex ante, but once a company identifies an error, it can, with some expenditure of time and money, patch or remove and replace the vulnerable software. The rules regarding liability should reflect the fact that once a company identifies a specific vulnerability, it is no longer a random target, and its software no longer falls under any definition of "reasonably secure."[202]

Returning to the fundamental question of whether a particular act is "unfair," it should be noted that the definitions of "unfair" and "deceptive" overlap.[203] There is arguably an element of "deception" when a security-software vendor, knowing of a vulnerability, does not

199. Bambauer and Day, *supra* note 169, at 1060.

200. *Id.* at 1061.

201. *E.g.*, Oriola, *supra* note 3, at 478 (describing "software penetration testing" used by hackers to probe for software vulnerabilities).

202. For example, if the vulnerabilities detection research industry uncovers and announces a vulnerability, unless and until the software vendor takes action to fix it, hackers can take advantage of that known defect. *E.g.*, Bambauer, *supra* note 25, at 1048 (discussing the markets for "zero-day" attack information); Oriola, *supra* note 3, at 482 (noting that disclosure may facilitate attacks by hackers "through the knowledge of vulnerabilities they otherwise would not have had").

203. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245 (3d Cir. 2015).

disclose it to a licensee. This is not to suggest, however, that under these circumstances the vendor has committed a "deceptive" act within the meaning of the statute.[204] But it seems fair that the vendor should disclose a known risk; therefore, the FTC and the applicable laws should recognize that if the vendor does not disclose this risk, it has acted "unfairly."

In addition, or as an alternative to the FTC, state regulators might play a role in holding security software vendors accountable for vulnerabilities. These regulators already rely on state statutes, including the "little FTC acts"[205] of the fifty states and the District of Columbia,[206] to protect consumers' data security. For example, the California Attorney General regularly investigates companies for engaging in "unfair competition" by failing to ensure data privacy or security.[207] In 2013, after Citibank failed to fix a known software vulnerability, the State of California filed a complaint against Citibank in the Superior Court of Alameda County and alleged that Citibank violated several laws, including the prohibition against "unfair" competition.[208] For the reasons proposed above in regard to federal law and the FTC, it would seem reasonable for the State to have prosecuted the vendor whose security software contained the vulnerability exploited in the breach, had that vendor known of the vulnerability and not advised Citibank.[209]

Consumers may also play a role in holding security software vendors accountable for their failure to disclose risky vulnerabilities.[210] For example, consumers can now bring state consumer-protection claims against the companies housing their data after a breach.[211] But these

204. A practice is "deceptive" if it is "likely to mislead consumers acting reasonably under the circumstances." Moncada, *supra* note 77, at 917–18. The consumers whose data is housed in company files have no direct relationship with the security software vendor which sold protective software to the company.

205. Ryan P. O'Quinn & Thomas Watterson, *Fair is Fair—Reshaping Alaska's Unfair Trade Practices and Consumer Protection Act*, 28 ALASKA L. REV. 295, 308 (2011).

206. *Id.* at 303.

207. *Privacy Enforcement Actions*, ST. CAL. DEP'T JUST., https://oag.ca.gov/privacy/privacy-enforcement-actions (last visited May 10, 2017).

208. CAL. BUS. & PROF. CODE § 17200 (West 2008).

209. Whether the definition of "unfair" in California's statute is or should be precisely the same as under the Federal Trade Commission Act ("FTC Act") is a topic outside the scope of this Article. *See generally* Alexander N. Cross, *Federalizing "Unfair Business Practice" Claims under California's Unfair Competition Law*, U. CHI. LEGAL F. 489 (2013) (noting inconsistent applications of the statutory definition in the California lower courts and arguing that an approach that adopts section 5 of the FTC Act's definition of "unfair business practices" is the best approach).

210. For the reasons discussed above, limiting liability to these circumstances seems fair and reasonable.

211. Unlike the FTC Act, state consumer protection statutes grant consumers a private right of action. O'Quinn & Watterson, *supra* note 205, at 303; *see, e.g.*, *In re* Cmty. Health Sys., Inc.,

cases face formidable obstacles. For example, courts struggle to determine what types of injury caused by data theft confer Article III standing on the consumers whose data has been stolen,[212] and many class action lawsuits falter for this reason alone.[213] Other issues regarding damages may preclude recovery, such as the "economic loss rule" in some states that limits recoverable damages to "ascertainable" or "pecuniary" loss.[214] Some state consumer-protection laws provide for a private right of action only to enforce prior regulatory orders,[215] or to prohibit class actions entirely.[216] These are only examples; the consumer protection statutes of the states and the circumstances of each data breach case are too varied to enumerate all the issues encountered by plaintiffs in these cases. But just as the law is evolving so that consumers can hold companies accountable for failing to protect their data, so, too, might that law accommodate "unfair trade practice" claims against the vendors of the software that is actually on the front line in terms of protecting the data.

CONCLUSION

Data breaches have become so common that some consumers may be suffering from "data breach fatigue."[217] And it is true that when business

Customer Sec. Data Breach Litig. (MDL 2595), No. 15-CV-222-KOB, 2016 WL 4732630, at *18–19 (Sept. 12, 2016 N.D. Ala.) (noting how named plaintiffs alleged violations of unfair trade practice laws of Florida, Nebraska, Ohio, New Mexico, Pennsylvania, Texas, and Tennessee, arising from data breach); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014) (alleging similar violations); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 985 (S.D. Cal. 2014) (bringing claims under the California Unfair Competition Law, False Advertising Act, and the Consumers Legal Remedies Act).

212. *E.g.*, Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015) (holding that customers plausibly alleged standing); *see also* Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *6 (E.D. La. May 4, 2015) (finding that the plaintiff had not adequately alleged standing and granting the motion to dismiss the case for lack of subject matter jurisdiction); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (concluding the allegations were sufficient to establish standing). Whether and to what extent future harm is a compensable element of damage for any particular cause of action asserted in a lawsuit arising from data breach is a topic beyond the scope of this Article. For a discussion regarding the validity of such harm, see generally Rachel Yoo, *An Expected Harm Approach to Compensating Consumers for Unauthorized Information Disclosures*, 19 RICH. J.L. & TECH. 1 (2012).

213. The list is a long one. For an example, see generally *Strautins v. Trustwave Holdings*, 27 F. Supp. 3d 871 (N.D. Ill. 2014).

214. *See, e.g.*, In re *Target Corp.*, 66 F. Supp. 3d at 1162 (stating that the plaintiff's injuries are cognizable under each state's consumer-protection laws).

215. *Id.* at 1163.

216. *Id.*

217. Elise Hu, *I Feel Nothing: The Home Depot Hack and Data Breach Fatigue*, NPR (Sept. 8, 2014, 2:36 PM), http://www.npr.org/sections/alltechconsidered/2014/09/03/345539074/i-feel-

data is breached, the consumers whose data is stolen usually suffer little, if any actual out-of-pocket loss from the breach.[218] But those losses do add up to billions of consumer dollars transferred to the pockets of thieves, and potentially very large costs to the breached company. Moreover, the "Internet of Things" portends more pervasive and more dangerous consequences from data breaches in the future. Even now, when a data breach may have impacted the outcome of a national presidential election,[219] consumers and consumer protection advocates should remain vigilant in the fight against the hackers.

Given the digitization of the world, and the fact that data can so easily be replicated, stored, and transmitted, preventing unauthorized access to data is probably an impossible task. But any known chink in the armor protecting that data should surely be repaired. Security vulnerabilities in software are widespread; any software can contain a security vulnerability. But when a company buys and pays for software specifically to provide data security—as opposed to operating a computer program—the vulnerability seems particularly problematic. Yet, for reasons explored in Part I, the companies purchasing that software appear unable or unwilling to hold the seller accountable. To bolster the front line of defense against consumer data theft (i.e., commercial security software and systems) federal and state regulators should consider holding the vendors of security software accountable for an "unfair trade practice" if a known vulnerability in that software is not reported to the licensees. To avoid this threatened action, vendors may well "out" the vulnerability on their own, enabling the companies using that software to close the door before the thieves arrive.

---

nothing-the-home-depot-hack-and-data-breach-fatigue ("You've certainly read the what-to-do-in-the-event-of-a-hack stories here, and elsewhere. How many times have we recommended looking at your credit card bills for any weird purchases, or had security experts remind us to change our passwords, or use two-factor authentication, or not trust the cloud with our most private images?").

218. *See generally* Riedy & Hanus, *supra* note 26 ("The theft of personal information causes minimal harm to consumers, while the business-the putative defendant-suffers far greater costs associated with a breach.").

219. Douglas Ernst, *Wikileaks Emails Reveal Podesta Urging Clinton Camp to "Dump" Emails*, WASH. TIMES (Nov. 1, 2016), http://www.washingtontimes.com/news/2016/nov/1/wikileaks-emails-reveal-john-podesta-urging-hillar/ (reporting on a "new round of WikiLeaks documents released . . . reveal[ing] a March 2015 exchange between Hillary Clinton's campaign chairman and confidant Cheryl Mills on the need to 'dump' emails").