Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 11
Issue 1 *SYMPOSIUM: The Role of Technology in Compliance in Financial Services: An Indispensable Tool as well as a Threat?*

Article 7

12-1-2016

Like a Bad Neighbor, Hackers Are There: The Need for Data Security Legislation and Cyber Insurance in Light of Increasing FTC Enforcement Actions

Jennifer Gordon

NOTES

LIKE A BAD NEIGHBOR, HACKERS ARE THERE: THE NEED FOR DATA SECURITY LEGISLATION AND CYBER INSURANCE IN LIGHT OF INCREASING FTC ENFORCEMENT ACTIONS

ABSTRACT

Privacy has come to the forefront of the technology world as third party hackers are constantly attacking companies for their customers' data. With increasing instances of compromised customer information, the Federal Trade Commission (FTC) has been bringing suit against companies for inadequate data security procedures. The FTC's newfound authority to bring suit regarding cybersecurity breaches, based on the Third Circuit's decision in FTC v. Wyndham Worldwide Corp., is a result of inaction—Congress has been unable to pass sufficient cybersecurity legislation, causing the FTC to step in and fill the void in regulation. In the absence of congressional action, this self-proclaimed authority is improper. This Note proposes that Congress enact a law giving the FTC actual authority to regulate data breaches. Thereafter, the FTC should use its rulemaking authority to establish procedural data security guidelines for companies to follow; this Note offers procedural guidelines for the FTC to enforce. It is necessary for companies to know how to protect themselves against FTC enforcement actions. As cyber risk is burgeoning, as self-regulation has proven insufficient, and as the FTC is continuously bringing suit against companies for inadequate data security, it is further necessary for companies to obtain stand-alone cyber insurance to protect themselves in the modern marketplace.

INTRODUCTION

As hackers are constantly attacking companies for their customers' data and their corporate intelligence, privacy has come to the forefront of the technology world.[1] The Federal Trade Commission (FTC) has been increasingly bringing suit against companies that it deems to have inadequate data security procedures.[2] Although the FTC currently reigns over more territory than any other agency that deals with privacy,[3] it is now necessary

1. *See* Stephen H. Jett, *Corporate Boards Beware: The FTC is Watching*, PRIVACY & DATA SECURITY INSIGHT (Sept. 28, 2015), http://www.privacyanddatasecurityinsight.com/2015/09/corporate-boards-beware-the-ftc-is-watching/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PrivacyAndDataSecurityInsight+%28Privacy+and+Data+Security+Insight%29.

2. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law Of Privacy*, 114 COLUM. L. REV. 583, 588 (2014).

3. *Id.*

for Congress to take control and enact legislation to direct the way in which companies set their cybersecurity practices by giving regulatory authority to the FTC; the FTC's regulation of cybersecurity in the absence of legislation is improper. Given the increase in the FTC's regulation, it is essential for the FTC to provide guidance to companies on how to protect themselves, and their customers, from a data breach.[4] As cyber risk[5] is burgeoning, and as self-regulation has proven insufficient, it is necessary that companies obtain cyber insurance and that courts uniformly recognize such insurance as sufficient.

The year 2014 demonstrated to the world the immense and inherent cyber risk that companies face with cases including *In re Target Corporation Customer Data Security Breach Litigation, Financial Institution Cases*, *FTC v. Wyndham Worldwide Corp.*,[6] and many more. Companies are currently facing not only private civil actions in response to security breaches,[7] but also potential "governmental and regulatory investigations, fines, and penalties,"[8] primarily led by the FTC. As cyber risks are causing first party losses, as well as third party losses,[9] the expenses due to these lawsuits have grown exponentially. In its 2014 study on the costs of data breaches, the Ponemon Institute found that the average breach in the United States costs an

4. "The term 'data breach' refers to 'unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information.'" Gregory J. Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 190 n.16 (2015).

5. Cyber risk "generally includes any loss exposure associated with the use of electronic equipment, computers, information technology, and virtual reality." Gregory D. Podolak, *Cyber Risk Coverage Litigation Heats Up as Exposure and the Insurance Market Evolve*, AM. B. ASS'N INS. COVERAGE LITIG. (June 13, 2014), http://apps.americanbar.org/litigation/committees/insurance/articles/marchapril2014-cyber-risk-litigation.html.

6. *See* Thad A. Davis, Michael Li-Ming Wong & Nicola M. Paterson, *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 640 (2015); *see generally In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014); *see generally* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

7. *See* JUDITH H. GERMANO & ZACHARY K. GOLDMAN, CTR. ON LAW AND SEC., N.Y. UNIV. SCH. OF LAW, AFTER THE BREACH: CYBERSECURITY LIABILITY RISK 1 (2014).

8. Roberta D. Anderson, *Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz,* 49 TORT TRIAL & INS. PRAC. L.J. 529, 539 (2014).

9. *See* Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges,* 33 QUINNIPIAC L. REV. 369, 374 (2015) (explaining that first party losses are those suffered directly by the affected company and third party claims are brought by others against the compromised company); *see* Thomas H. Bentz, Jr., *Protecting Against Cyber Risk – A Primer on Cyber Insurance*, HOLLAND & KNIGHT (Jan. 15, 2015), https://www.hklaw.com/PrivacyBlog/Protecting-Against-Cyber-Risk-A-Primer-on-Cyber-Insurance-01-15-2015/ (explaining that first party losses include: forensic investigation coverage, data loss and restoration coverage, network business interruption coverage, cyber extortion coverage, and theft coverage. Third party losses include notification costs, litigation expenses, defense of regulatory proceeding costs, crisis management costs, online defamation, and copyright and trademark infringement costs).

organization around $5.58 million.[10] Companies need to insure themselves against these losses[11] in order to remain competitive.

As of now, litigation surrounds the fragmented and disconnected framework of state and federal laws governing cybersecurity obligations.[12] Even with recent case law affirming the FTC's open-ended authority to regulate corporate privacy and data security under the Federal Trade Commission Act (FTCA),[13] the law surrounding cybersecurity and cyber breaches is far from settled. Furthermore, it is still unclear how the FTC will regulate data security and other data practices without new, guiding congressional legislation.[14] There is an increasing need for more guidance from Congress and a need for significant legislation on this topic. Cybersecurity needs concrete laws[15] and regulations similar to the data security legislation in the financial and health industries.

Part I of this Note provides an overview of the current state of cyber crime and discusses the increasing threat of cyber attacks by hackers. Part II discusses the FTC and its current regulations and heightened authority over security breaches; therein this Note argues that, as of now, in the absence of legislation, the FTC has too broad of a power in managing these cases, even in the aftermath of *Wyndham*. Part III assesses the concept of cyber insurance and delves into the need for companies to obtain stand-alone cyber insurance coverage. Part IV of this Note argues for the clear need for congressional legislation and, in-turn, FTC regulatory guidelines for companies to follow. Part IV recommends procedural security guidelines for the FTC to enact and thereafter enforce.

I. THE CURRENT STATE OF CYBER CRIME

The quantity, sophistication, and severity of cyber attacks grow worse every day.[16] It has become clear that there is no such thing as an

---

10. *See* Allison Grande, *Regulators Are Fueling Cyberinsurance Demand, Report Says,* LAW360 (Oct. 21, 2015, 7:58 PM), http://www.law360.com/articles/717044/regulators-are-fueling-cyberinsurance-demand-report-says.

11. "In the case of individuals, a data breach involves stolen 'personally identifiable information'. . . . For corporations, it can involve various forms of sensitive or confidential information such as client records, bid data, trade secrets, financial records, and litigation information." Podolak, *supra* note 5.

12. *See* GERMANO & GOLDMAN, *supra* note 7, at 2.

13. *See generally* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (the court held that the FTC has jurisdiction in connection with cybersecuity matters and also has the power to regulate corporate privacy and data-security procedures pursuant to the FTCA). *See generally* Federal Trade Commission Act, 15 U.S.C. §45(a) (2012).

14. *See* Evans, *supra* note 4, at 189.

15. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1050 (2014); *see infra* Part IV.

16. *See* Kevin LaCroix, *Guest Post: Cyber Security, Cyber Governance, and Cyber Insurance: What Every Public Company Director Needs to Know,* THE D&O DIARY (June 4, 2014), http://www.dandodiary.com/2014/06/articles/cyber-liability/guest-post-cyber-security-cyber-governance-and-cyber-insurance-what-every-public-company-director-needs-to-know/.

"unbreachable" firewall or an impenetrable security system; no technology is immune from hacking.[17] As "[a]t least ninety-seven percent of Fortune 500 companies have been hacked,"[18] it is clear that cyber threats are a reality faced by all in our modern world. Further, the National Security Agency's director stated that "[t]he ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history."[19] According to Forrester's annual research, at least 60% of brands were predicted to discover a breach of sensitive data in 2015, with the actual number being as high as 80% or more.[20]

Today the cyber crime "market" is full of highly organized groups, often connected with traditional crime groups, and is rapidly growing and continuously innovating.[21] This market is "full of increasingly sophisticated organizations, people, products, and methods for communicating and conducting business transactions."[22] Where cyber criminals originally hacked merely for small, personal gain or bragging rights, the cyber atmosphere has changed in recent years as hackers are looking for much greater gain.[23] Furthermore, modern software is too complex for defects to be completely eliminated and hackers can infiltrate virtually any system;[24] no matter what protections a company places on its software, no software will ever be completely secure. As this threat upsurges, market pressures have been "pushing businesses towards better cybersecurity in order to remain competitive."[25] In view of how significant the damage and potential liability resulting from a data breach can be, companies cannot afford to be without cybersecurity insurance.[26]

Even with the increase in cyber crime and the industry's acknowledgement of the need for greater cybersecurity, lawmakers have yet to pass any significant data security enforcement legislation, which has led

17. Anderson, *supra* note 8, at 532.

18. Noah G. Susskind, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 578 (2015).

19. Anderson, *supra* note 8, at 531–32 (alteration in original) (quoting DOUGLAS MAUGHAN, BILL NEWHOUSE & TOMAS VAGOUN, THE NEXT WAVE BUILDING A NATIONAL PROGRAM FOR CYBERSECURITY SCIENCE (2012), https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-19-4.pdf).

20. CYBERSECURITY VENTURES, CYBERSECURITY MARKET REPORT 26–27 (2015) [hereinafter CYBERSECURITY MARKET REPORT], http://cybersecurityventures.com/cybersecurity-market-report/.

21. *See* Lillian Ablon & Martin Libicki, *Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data*, 82 DEF. COUNS. J. 143, 144–45 (2015).

22. *Id.* at 144.

23. *See id.*

24. *See* Bambauer, *supra* note 15, at 1020.

25. Susskind, *supra* note 18, at 594.

26. *See* Daniel Garrie & Michael Mann, *Cyber-Security insurance: Navigating the Landscape of a Growing Field*, 31 J. MARSHALL J. INFO. TECHNOLOGY & PRIVACY L. 379, 379 (2014).

the FTC to intervene and fill the void.[27] The FTC's data security regulation originally centered predominantly around cases of deceitful promises, but today it has developed into something much greater—the FTC is suing companies for vague promises of security, promises that hackers can easily force these companies to break.[28]

II. THE FTC AND CYBER CRIME

A. THE FTC'S GROWING REGULATORY AUTHORITY UNDER THE FTCA

While the FTC was established to ensure fair competition in commerce, the agency's powers expanded greatly with the enactment of the FTCA. The FTCA's goal was "to prohibit 'unfair or deceptive acts or practices' in addition to 'unfair methods of competition'—thereby charging the FTC with protecting consumers directly . . . . "[29] The FTCA gives the FTC an amorphous privilege to broadly prohibit companies from engaging in deceptive or unfair business practices.[30] Unlike FTC claims for "deceptive"[31] practices, where companies have broken their promises, "[b]eginning in 2005, the FTC began bringing actions under the [FTCA's] unfairness prong for companies that failed to use reasonable security practices to safeguard customers' personal information."[32] It was not until 2015 that a court held that the FTC's authority extended to regulating data security as unfair practice.[33] Now, the FTC has taken the lead—it plays a central government role in data security enforcement.[34] The primary source of its enforcement power is Section 5 of the FTCA, which prohibits "unfair or deceptive acts or

---

27. *See* Zosha Millman, *After Big Win at Third Circuit in Wyndham Suit, FTC Will Continue to Regulate Data Breaches,* LXBN (Aug. 25, 2015), http://www.lxbn.com/2015/08/25/ftc-wins-big-wyndham-third-circuit/.

28. *See* Solove & Hartzog, *supra* note 2, at 636.

29. Solove & Hartzog, *supra* note 2, at 598; *see* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015) (explaining that this occurred in reaction to "several early cases [which] limited 'unfair methods of competition' to practices harming competitors and not consumers . . . Congress [then] inserted an additional prohibition in §45(a) against 'unfair or deceptive acts or practices in or affecting commerce.'").

30. *See* Evans, *supra* note 4, at 201.

31. Alden Abbott, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, HERITAGE FOUND. (Sept. 10, 2014), http://www.heritage.org/research/reports/2014/09/the-federal-trade-commissions-role-in-online-security-data-protector-or-dictator. The deception only occurs when "business conduct causes tangible harm to consumers who acted reasonably and were misled." *Id.* However, this Note only concerns the "unfairness" prong.

32. Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation,* 9 HARV. L. & POL'Y REV. 355, 358 (2015).

33. *FTC Held to Have Authority to Regulate Cybersecurity Practices Under Section 5 of the FTC Act*, CHADBOURNE (Sept. 24, 2015), http://www.chadbourne.com/sites/default/files/publications/150924_ftcheldauthorityregulatecybersecurity_clientalert_0.pdf [hereinafter *FTC Held to Have Authority*]; *see generally* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

34. *See* Davis, Li-Ming Wong & Paterson, *supra* note 6, at 632.

practices in or affecting commerce."[35] The FTC views this statute "as a 'broad consumer protection mandate' that Congress intended to allow the Commission to respond to the 'unanticipated, unremunerated threats' consumers face in the marketplace."[36]

To prove unfairness under Section 5, the FTC must prove the following elements: "(1) an act or practice caused or is likely to cause substantial injury to consumers; (2) the injury was not reasonably avoidable by consumers; and (3) the injury was not outweighed by countervailing benefits to consumers or competition."[37] In 2014, The FTC Commissioner stated that "[t]his [unfairness] standard calls for an economic analysis of the allegedly unfair business practice. The economic analysis it invites is an appropriately flexible one—incorporating not only the harms to aggrieved consumers but also any benefits to consumers or to competition more generally."[38] These elements, particularly the first,[39] are easily met and further, the reviewing court must accord substantial deference to the FTC's interpretation of the FTCA.[40] "The FTC has issued over 170 privacy-related complaints against companies,"[41] and thus far, over the past decade, the FTC has pursued over fifty enforcement actions under its deception and unfairness authorities against companies that it considered to have "inadequate" data security practices.[42]

B. FTC V. WYNDHAM WORLDWIDE CORPORATION

The 2015 Third Circuit *Wyndham* case is instrumental, as a court held for the first time that the FTC's "longstanding authority to regulate 'unfair methods of competition in or affecting commerce' under [Section] 5 of the [FTCA], extends to regulation of cybersecurity practices that are harmful to consumers . . . ."[43] In addition, the court held that the defendant Wyndham

35. Evans, *supra* note 4, at 201.
36. *Id.*
37. *Id.*
38. Abbott, *supra* note 31 (alteration in original) (citing Joshua D. Wright, Comm'r, Fed. Trade Comm'n, Remarks to TechFreedom and the International Center for Law and Economics, The Economics of Digital Consumer Protection: One Commissioner's View (July 31, 2014), http://www.ftc.gov/system/files/documents/public_statements/573061/010731techfreedom.pdf).
39. Very recently, the FTC further broadened the definition of "substantial injury." In the FTC's Opinion and Final Order, *In the Matter of LabMD, Inc*., relating to charges of unfair trade practices based upon alleged data security violations, the FTC asserted the authority to take data security enforcement action against companies under the FTCA for their security practices regardless of whether the data security violations have caused actual financial or physical harm to particular consumers. In addition, the commissioners found that the FTCA "allowed for 'preemptive action,' meaning that no showing of actual harm [is] necessary." David Heck, *No Harm? No Matter. FTC Broadens Data Security Liability,* NAT'L L. REV. (Aug. 3, 2016), http://www.natlawreview.com/article/no-harm-no-matter-ftc-broadens-data-security-liability.
40. *See* Solove & Hartzog, *supra* note 2, at 613.
41. *Id.* at 610.
42. Abbott, *supra* note 31.
43. *FTC Held to Have Authority*, *supra* note 33.

had fair notice that its cybersecurity practices fell short of the requirements of the FTCA's "unfairness prong."[44]

The FTC filed suit against Wyndham after hackers on three occasions accessed Wyndham's network and its property-management systems. These data breaches resulted in the exposure of private financial data[45] from over 600,000 accounts[46] and more than $10 million in fraud loss.[47] Following these breaches, the FTC began to investigate Wyndham's data security practices, and shortly thereafter brought legal action against Wyndham.[48] Wyndham declined to enter into a consent order and the FTC proceeded with its first unsettled lawsuit,[49] alleging that Wyndham's cybersecurity procedures, which had failed to protect customers' personal and financial data, violated the FTCA's prohibition on "unfair" acts or practices.[50] Wyndham had failed to implement reasonable data security by:

> (1) allowing Wyndham-branded hotels to store payment card information in readable text; (2) allowing the use of easily guessable passwords; (3) failing to use firewalls and other readily available security measures; (4) allowing franchisees and others to connect to the network without appropriate precautions; (5) failing to adequately restrict access to its network and servers; (6) failing to utilize reasonable measures to detect and prevent unauthorized access; and (7) failing to follow proper incident response procedures.[51]

Instead of settling, Wyndham challenged the FTC's authority to bring action against it under Section 5.[52]

Wyndham claimed that the FTC lacked the authority to charge the failure to maintain adequate data privacy as an unfair trade practice because Congress did not give the FTC authority to assert charges of unfair trade

---

44. *See* John P. Hutchins, *Like Neiman Marcus, Wyndham is Not All It's Cracked Up to Be,* LAW360 (Oct. 1, 2015, 10:27 AM), http://www.law360.com/articles/708180?utm_source=rss&utm_medium=rss&utm_campaign=articles_search.

45. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242 (3d Cir. 2015).

46. Greg Everts, *Franchisors Take Note: FTC's Authority to Regulate Corporate Data Security May Affect You*, FRANCHISE L. INSIDER (Sept. 14, 2015), http://franchiseinsider.quarles.com/2015/09/franchisors-take-note-ftcs-authority-to-regulate-corporate-data-security-may-affect-you/.

47. 5 DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW § 28.04 35 (Matthew Bender Rev. Ed. 2015).

48. *See* Davis, Li-Ming Wong & Paterson, *supra* note 6, at 641.

49. *See* Hutchins, *supra* note 44; *see* Evans, *supra* note 4, at 202 (explaining that consent orders are FTC orders "in which companies agree to institute more robust data security procedures and make long-term commitments to third party security assessments."); *see also* Solove & Hartzog, *supra* note 2, at 613–14 (explaining that the FTC has discretion in determining the "access and scope" of the consent order procedure and that a typical FTC consent order contains "financial penalties, bans on certain activities, and requirements for corrective action. It also commonly contains reporting, audit, and compliance requirements for up to twenty years.").

50. *See* Everts, *supra* note 46.

51. *Id.*

52. *See FTC Held to Have Authority*, *supra* note 33.

practices regarding data security.[53] Wyndham additionally claimed that, even with such authority, the FTC's enforcement of its unfairness claim before formal promulgation of unfairness regulation violated fair notice principles.[54] Wyndham filed a motion to dismiss, yet the court ruled in favor of the FTC, holding: "(1) that the [FTCA's] prohibition on 'unfair' acts and practices is broad enough to grant the FTC authority over business data-security practices, and (2) Wyndham, based on the plain language of the Act and FTC statements, did in fact receive 'fair notice.'"[55] However, the Third Circuit merely ruled that the FTC has the power to regulate these data security practices under the FTCA. The case will go back to the trial court, where the parties will litigate the issue of whether Wyndham's data security practices were actually "unfair" under the FTCA.[56]

Wyndham demonstrates that the FTC is one of the primary regulators of cybersecurity and data-breach responses in the United States; the FTC sues companies even when third party hackers cause the cybersecurity breaches.[57] In the wake of *Wyndham*, it is very likely that the FTC will now use its power much more aggressively and will increasingly overreach in its authority. With the increase in investigations and, in turn, the increase in costs that companies will face if and when the FTC brings suit against them, companies' boards need to make changes to defend themselves against such actions.[58]

C. INAPPROPRIATE FTC AUTHORITY IN THE ABSENCE OF CONGRESSIONAL ACTION

The FTC's authority over cybersecurity breaches is a result of inaction—Congress has been unable to pass significant cybersecurity legislation, causing the FTC to step in and fill the void in regulation.[59] This self-proclaimed authority, in the absence of congressional action, is unfounded and should be challenged. Although consumer protection is necessary, when weighing the costs and benefits of the FTC's enforcement, as of now, the FTC is doing more harm than good. If, however, courts continue to affirm the FTC's authority to regulate cybersecurity, as argued in Part IV *infra*, Congress should enact a law giving the FTC authority to regulate these data

53. *See* Bender, *supra* note 47, at 36.1.

54. *See id.* at 36.2.

55. Everts, *supra* note 46.

56. *See* Hutchins, *supra* note 44.

57. *See FTC Held to Have Authority*, *supra* note 33.

58. *See* Timothy Cornell, *Wyndham: A Case Study in Cybersecurity: How the Cost of a Relatively Small Breach Can Rival that of a Major Hack Attack,* METROPOLITAN CORP. COUNS., Apr. 2015 at 15.

59. *See* Steven Caponi, *To Business' Chagrin, Cybersecurity is FTC's Turf Now,* LAW360 (June 10, 2014, 1:06 PM), http://www.law360.com/articles/545258/to-business-chagrin-cybersecurity-is-ftc-s-turf-now.

breaches. Thereafter, the FTC should use its rulemaking authority[60] to establish procedural guidelines for companies to follow. "When law specifies cybersecurity measures, security improves."[61]

Several issues undermine the FTC's authority to regulate cybersecurity. First, Congress has never explicitly granted the FTC authority to "initiate enforcement actions challenging cyber preparedness."[62] In contrast, "in prior Congressional proceedings, the FTC has repeatedly conceded that it had no authority to regulate data-security, as evidenced by the fact that the FTC had previously asked Congress to pass new legislation giving the FTC authority to regulate data-security."[63] Further, Section 5 of the FTCA is silent on data security; this section does not mention data security in any way, nor applicable security standards for computer software systems.[64] Section 5 also does not provide clarity on the legally required data security safeguards, and this is no clearer after the decision in *Wyndham*.[65] Furthermore, the FTC derives its authority from "a 100-year old consumer protection statute that broadly prohibits companies from engaging in *deceptive or unfair business practices*."[66] "When invoking its unfairness authority under Section 5, the question the Commission considers is . . . 'what was expected' of the company."[67] But, what is expected of the company? The FTC merely states that the standard expectation is adequate data security.[68] But, again, what is adequate data security?

Due to the uncertainty surrounding cybersecurity law, it is unfair for the FTC to sue companies for not knowing what constitutes "fair" and "adequate" security measures. How can businesses ensure compliance without published requirements from the FTC?[69] The only guidance that companies have is the FTC's January 31, 2014 press release and the FTC's

60. Congress gave the FTC such rulemaking and enforcement authority under COPPA in 1998. *See* Solove & Hartzog, *supra* note 2, at 602. "In 1999, under GLBA, Congress gave the FTC, among other agencies, the authority to 'establish appropriate standards for financial institutions subject to their jurisdiction' in order to 'insure the security and confidentiality of customer records and information' and 'protect against unauthorized access.'" *Id.* at 602–03.

61. Bambauer, *supra* note 15, at 1048.

62. Caponi, *supra* note 59.

63. Paul R. Gupta, Thomas Lahiff & Aravind Swaminathan, *Living in a Post-Breach World: What Regulators, the Courts, the Executive Branch, and Congress are Doing about Cybersecurity*, FINTECH L. REPORT, Jan.–Feb. 2014, at 1.

64. *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, And Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 700 (2013).

65. *See id.*

66. Brookman, *supra* note 32, at 358.

67. 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, 920 (2015).

68. *See id.*

69. Caponi, *supra* note 59.

Guide for Business.[70] Within the press release, the FTC maintained that its enforcement of cybersecurity protections is based on a reasonableness standard.[71] The FTC standard requires that "[a] company's data security measures . . . be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[72] This standard "fails to address a practical reality—implicitly recognized by the agency . . . that the ever evolving nature of technology creates a moving target for agency enforcement *as well as* entity compliance."[73] In addition, this standard "remains largely undefined by courts."[74] It is simply unfair for the FTC to sue companies for the actions of third parties under such a broad standard, in the absence of any congressional guidance.

If the FTC wishes to continue its regulation, it should convince Congress to pass a law giving the FTC authority to establish clear regulatory guidelines. Thus far, the FTC's guidance brochure merely states five broad "key principles" for companies to apply in safeguarding personal information. These key principles are:

> (1) Take stock. Know what personal information you have in your files and on your computers; (2) Scale down. Keep only what you need for your business; (3) Lock it. Protect the information that you keep; (4) Pitch it. Properly dispose of what you no longer need; and (5) Plan ahead. Create a plan to respond to security incidents.[75]

These vague guidelines are grossly insufficient. These standards are inconclusive, as the *Wyndham* court suggests that it would merely *consider* these factors relevant to a legal determination of reasonableness.[76] The FTC needs to adopt clearer guidelines, and in doing so, the FTC needs to provide case specific cost-benefit analyses, demonstrating why it should be able to sue companies, which it has yet to do.[77] The FTC should not have authority to sue companies when it gives no cost-benefit analysis and further fails to prove any benefits that such suits will have for consumers.

---

70. *See generally* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015) [hereinafter START WITH SECURITY], https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

71. *See* Stegmaier & Bartnick, *supra* note 64, at 695.

72. *FTC Held to Have Authority*, *supra* note 33.

73. Stegmaier & Bartnick, *supra* note 64, at 695.

74. James D. Gassenheimer & Lara O'Donnell, *Heightened Expectations: Mitigating the Threat of Cybersecurity Litigation in an Ambiguous Regulatory Environment,* DRI FOR DEF., Feb. 2015, at 50.

75. FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION A GUIDE FOR BUSINESS 1 (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

76. *See* Gassenheimer & O'Donnell, *supra* note 74, at 53.

77. *See* Abbott, *supra* note 31.

In addition, the FTC's enforcement actions embody tactics that force settlements. The FTC singles out vulnerable companies after they suffer a very large and public data breach; it then investigates the breach and strong-arms the company to stipulate to a consent order.[78] Under such consent orders, "companies agree to institute more robust data security procedures and make long-term commitments to third party security assessment."[79] This is a problem, as consent orders do essentially nothing; companies cannot protect themselves using self-regulation. It should be repeated that virtually every system, no matter the cybersecurity practices implemented, can be breached. Therefore, it is a waste of the FTC's time and resources to bring suit and further require the company to implement procedures that are not proven to prevent breaches, or to even shield it from FTC suit. The purpose of these consent orders is to prohibit future wrongful activities.[80] However, the FTC has yet to prove that these supposedly inadequate security procedures, like those at issue in *Wyndham*, are even wrongful.[81] The FTC's inability to prove wrongful procedures demonstrates why the FTC should not have this authority.[82]

D. COUNTERARGUMENTS

Conceivably, the FTC has informal data security authority sufficient to regulate cyber breaches.[83] Commentators argue that because Congress has not imposed strict limits on the FTC's authority, the FTC therefore has implied authority to regulate cybersecurity.[84] Further, because the Supreme Court has established that courts "must defer to an agency's construction of the statute under which it operates, especially if Congress has failed to act or speak out regarding the specific legal issue,"[85] commentators argue that the FTC is simply construing the statute since Congress has failed to act or speak out on this legal issue. However, as shown below, these counterarguments are misplaced.

Commentators contend that the FTC's privacy jurisprudence has developed "along classic common law developmental patterns."[86] The FTC has stated that the unfairness doctrine is the "result of an 'evolutionary process' that refines the standard over time through cases, rules, and

78. *See* Hutchins, *supra* note 44.
79. Evans, *supra* note 4, at 202.
80. *See* Moncada, *supra* note 67, at 913–14.
81. *See* Hutchins, *supra* note 44.
82. *See generally The FTC's Proposed Wyndham Settlement and its Implications for the Regulatory Landscape,* KING & SPALDING (Dec. 11, 2015), http://www.kslaw.com/imageserver/KSPublic/library/publication/ca121115c.pdf.
83. *See* Moncada, *supra* note 67, at 925–26.
84. *See id.* at 926.
85. *Id.* at 928–29.
86. Solove & Hartzog, *supra* note 2, at 627.

Commission statements."[87] In so arguing, commentators believe that this type of development is the "natural and logical outgrowth of multiple applications of a particular general standard" and that "through a multitude of cases, a detailed list of problematic security practices has emerged."[88]

Similarly, the FTC takes the position that its public statements and its past enforcement actions provide the industry with "notice of different features of data-security that must be evaluated in order to maintain a reasonable data-security program."[89] If this is so, this Note posits that those statements and past enforcement actions are not sufficiently detailed to truly put companies on notice. Furthermore, why has the FTC not simply published this so-called list of guidelines to follow from past cases, as conclusive? Commentators answer that "[t]here is no one-size fits all data-security model that can work for all business types and data-collection models."[90] Further, they argue that the FTC's "incorporation of qualitative judgments into language that lacks specific qualitative standards or even any qualitative standard is also a natural byproduct of the common law process."[91] These arguments neglect to assess the fact that although the FTC has mandated a vague baseline standard, this standard is not well established. In just nine cases, only one of which has been published, has the FTC relied "exclusively upon its 'unfairness' authority to establish de facto cybersecurity standards."[92]

Further, this analysis fails to adequately address the questions of whether the FTC is appropriately applying its Section 5 authority in finding unfairness, and whether it is imposing undue burdens on businesses by failing to provide any guidance beyond that found in these nine cases.[93] It seems unjust for the FTC to expect companies to follow such broad and inconclusive standards from only nine cases that exclusively target "unfairness."[94] Further, although commentators have made different lists of what they believe the FTC's guidelines to be when determining unreasonable security measures,[95] who is to say that when the FTC sues the next company that follows all of those "guidelines," that it will not sue the company for lacking a different, previously unmentioned security measure?

Commentators argue that the FTC's Best Practices Guidelines and the "Start with Security" guide[96] inform companies on how to implement

87. *Id.* at 638–39.
88. *Id.* at 649–50.
89. Caponi, *supra* note 59.
90. Moncada, *supra* note 67, at 939.
91. Solove & Hartzog, *supra* note 2, at 569.
92. Bruce J. Heiman, Soyong Cho & Andrew L. Caplan, *The FTC Has Already Set Cybersecurity Standards*, LAW360 (Mar. 5, 2015, 2:07 PM), http://www.law360.com/articles/626447/the-ftc-has-already-set-cybersecurity-standards.
93. *See* Abbott, *supra* note 31, at 4 n.19.
94. *See* Heiman, Cho & Caplan, *supra* note 92.
95. *See id.*
96. *See* START WITH SECURITY, *supra* note 70.

reasonable security measures and that, accordingly, the FTC has developed a form of "soft law."[97] Again, as mentioned above, these are inconclusive recommendations that do not have the force and effect of law; further, the FTC has not explicitly stated that "the recommendations listed in the publication are the focus of its data-security investigations under Section 5."[98]

Finally, in response to the argument that the FTC must exercise its optional rulemaking authority, some have argued that this would be too burdensome and time consuming; they believe "it would render the Commission's authority useless because [it] would be too slow to respond to pressing issues at hand, such as frequent data breaches."[99] However, an effective case-by-case analysis can coexist with a set of guidelines for companies to follow. Further, it is not unreasonable to request the FTC to produce a set of specific guidelines for companies to follow to prevent suit—especially since it has proven effective in other areas, such as the health and financial spheres. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule,[100] which is "one of the most specific data security laws,"[101] lists safeguards that must be in place to ensure appropriate protection of electronic health information. Similarly, Congress has imposed requirements on firms in the financial sector, banks, and other financial institutions, to meet the security requirements of the Gramm–Leach–Bliley Act (GLBA)[102] Safeguards Rule.[103] The above argument is further hindered by the fact that "the FTC has used rulemaking to implement other data-security-related laws" in the past.[104] Since the FTC has used this authority effectively before, there is no reason that the FTC cannot do so again.

III. CYBER INSURANCE

The cyber insurance industry, which did not exist fifteen years ago, was created in response to regulation.[105] "As regulators are becoming more

97. Moncada, *supra* note 67, at 932.

98. Stegmaier & Bartnick, *supra* note 64, at 701.

99. Moncada, *supra* note 67, at 927–28. To illustrate the burden of rule-making, the Commission must (1) publish a notice that states with particularity the proposed rule; (2) allow interested persons to submit their "written data, view, and arguments;" and (3) hold an informal hearing to allow interested persons to "cross-examine each other." *Id.*

100. *See generally* The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1937 (codified as amended at 42 U.S.C. § 1320 (2012)).

101. *See* Solove & Hartzog, *supra* note 2, at 655.

102. *See* Bambauer, *supra* note 15, at 1048–49 (however, GLBA is a standard, not a rule); *See generally* Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended at 15 U.S.C. §§ 6801–09 (2012)).

103. *See generally* Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.1–5 (2016).

104. Stegmaier & Bartnick, *supra* note 64, at 707.

105. *See* Allison Grande, *Privacy 'Bill Of Rights' To Boost Demand For Breach Coverage,* LAW360 (Oct. 23, 2015, 5:58 PM), https://www.mayerbrown.com/files/News/13679f14-45c2-41ad

aggressive in investigating data breaches and levying fines on affected companies, this coverage has become increasingly important" in mitigating financial liability.[106] Today, the cybersecurity insurance market is the fastest growing segment of the insurance industry, due to the rise of cyber threats.[107] The cyber insurance market has more than doubled, growing from $1 billion to $2.5 billion in the past two years.[108] Still, the market has a long way to go; it is estimated that only "one in three companies has insurance specifically to protect against [data breach] losses."[109] However, in the era of immense, high profile data breaches, companies are beginning to realize that they must take proactive positions against the risk of loss—they must insure against the inevitable.[110]

Due to the great potential liability resulting from a single data breach, companies cannot afford to be without cybersecurity insurance.[111] Since companies believe that cyber attacks are so unpredictable, they reason that cyber insurance is too expensive.[112] However, as market and FTC pressures increase, businesses are pushed towards better cybersecurity to remain competitive. Moreover, "[a]s this new form of insurance continues to emerge and develop, it is important for companies to understand the current state of the market and the nature of the protection that they need in order to prudently obtain coverage for cyber-security breaches."[113] It is imperative that companies obtain cyber risk insurance when developing their risk management programs.[114] The most informed way to purchase cyber insurance is to understand the risks to which the company is exposed.[115]

The most recent data breaches involving Target Corporation and Home Depot cost these companies millions of dollars in financial damages.[116] These recent breaches have shown how enormous the liability from a single breach

---

-b5e0-f21f88f9d695/Presentation/NewsAttachment/d9cef92a-8587-410f-9ca3-e4ac0a5d83a4/PrivacyBillOfRightsToBoostDemandForBreachCoverage.pdf.

106. Grande, *supra* note 10 (quoting Rob Jones, Global Head of Fin. Lines Specialty Claims, Am, Int'l Grp. Inc.).

107. *See* Garrie & Mann, *supra* note 26, at 379.

108. CYBERSECURITY MARKET REPORT, *supra* note 20, at 8.

109. Michael N. DiCanio, *Preparing for the Inevitable: Insurance for Data Breaches,* N.Y. L.J. (May 19, 2015), https://www.lowenstein.com/files/Publication/c8b97609-204a-4735-ae92-dd3c4c292fb0/Presentation/PublicationAttachment/8ee423b0-aa5e-474d-9cb9-49a78ad1ec0c/Preparing%20for%20the%20Inevitable_Insurance%20for%20Data%20Breaches.pdf.

110. *See id.*

111. Garrie & Mann, *supra* note 26, at 379.

112. *See id.* at 384.

113. *Id.* at 379.

114. *See* Howard B. Epstein & Theodore A. Keyes, *Cyber-Risk Insurance Update*, N.Y. L.J. (July 27, 2015), http://www.newyorklawjournal.com/id=1202733060552/CyberRisk-Insurance-Update?slreturn=20160815192503.

115. *See* Diane D. Reynolds, *How an Incident Response Plan Can Reduce Your Cyber Insurance Costs,* PRIVACY & DATA SECURITY INSIGHT (Oct. 20, 2015), http://www.privacyanddatasecurityinsight.com/2015/10/how-an-incident-response-plan-can-reduce-your-cyber-insurance-costs/.

116. *See* DiCanio, *supra* note 109.

can be.[117] In light of these breaches, it is imperative for companies to not only obtain insurance, but to understand the insurance policies that they have purchased. National and international reports suggest that, even faced with these examples, a significant number of corporations of all sizes may lack insurance that would sufficiently cover them in the event of a data breach.[118] Compliance officers must ensure that their companies are adequately protected by their insurance policies.

A. INSURANCE POLICIES

First, it is fundamental for companies to understand their insurance policy's cybersecurity coverage.[119] Most companies have various forms of traditional insurance policies that may cover cyber risks, such as commercial general liability (CGL); only a few companies currently carry specialty insurance policies that are specifically designed to afford coverage for cyber risks.[120] However, insurance companies are capitalizing on the increase in data breaches by adding data breach exclusions to these types of CGL policies and creating new specialized cyber insurance policies designed to specifically insure against losses from hackers and other cyber threats.[121] These cyber insurance policies are becoming more widely available[122] as CGL insurers are aggressively denying cyber risk coverage.[123]

Companies looking for coverage for cyber losses have generally looked to their CGL policy, and these efforts have been met with mixed success in the courts.[124] The Insurance Services Office (ISO) has modified the standard form CGL policy to address coverage for electronic-related publications into the following three parts: "(1) Coverage A: Bodily Injury and Property Damage Liability; (2) Coverage B: Personal and Advertising Injury Liability; and (3) Coverage C: Medical Payments."[125] However, the cases in which courts construed CGL policies for data breach claims might now be moot, as the ISO "recently revised the standard CGL form to exclude data breaches from coverage."[126] Although courts have yet to test the newest exclusions, it

117. For example, Target revealed that the data breach it suffered in 2013 had cost around $252 million and it received around $100 million from its insurance company. Home Depot lost $43 million from its data breach and received $15 million from its insurers. *See* Davis, Li-Ming Wong & Paterson, *supra* note 6, at 646.

118. *See id.*

119. *See* Garrie & Mann, *supra* note 26, at 383.

120. *See* Anderson, *supra* note 8, at 542.

121. *See* Jim Vorhis & Joan Cotkin, *How Courts Have Decided Coverage Issues in Cyber Insurance Cases,* L.A. LAW, Sept. 2015 at 37.

122. *See* Dan Zureich & William Graebe, *Cybersecurity: The Continuing Evolution of Insurance and Ethics,* 82 DEF. COUNS. J. 192, 195 (2015).

123. *See* Podolak, *supra* note 9, at 382.

124. Zureich & Graebe, *supra* note 122, at 195.

125. Podolak, *supra* note 9, at 380.

126. *See* Zureich & Graebe, *supra* note 122, at 195. In 2001, the ISO revised the definition of "property damage" to omit coverage for "electronic data." *See* Podolak, *supra* note 5. In 2004, the

is inferable that these exclusions will create significant gaps in coverage for cyber claims.[127] Due to these gaps in CGL policies, companies must look to obtaining stand-alone cyber insurance policies.

B. ATTEMPTS TO RECOVER LOSSES UNDER CGL POLICIES

Although claims involving "property damage" and "bodily injury" arise often, today's insurance litigation focuses primarily on coverage surrounding the issue of "publication," which triggers the "personal and advertising" coverage.[128] "Personal and advertising injury" is defined by the ISO to include a list of enumerated offenses, including the offense of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[129] As most cyber-attacks on companies involve compromised information, the principal issue is whether such compromised information was a "publication" by the company.[130]

A recent highlighted case that deals with this issue is *Zurich American Insurance Co. v. Sony Corp. of America*.[131] The legal dispute in *Zurich* arose between Sony and its insurers; this case highlights the challenges that companies face in their attempt to persuade "insurance companies to cover losses arising from cyber risks under CGL policies."[132] In *Zurich*, Sony sought CGL "personal injury" coverage following a hack of its PlayStation Network that resulted in stolen personal information of one hundred million users.[133] Zurich, the insurance company, "contend[ed] that the relevant policy language 'oral or written publication in any manner of the material that violates a person's right of privacy' requires the publication be made by the insured." The court agreed with this argument.[134]

The Supreme Court of New York, Appellate Division, held that Zurich and another insurance company "did not have a duty to defend because the alleged publication was not 'conducted or perpetrated by the policyholder'—

ISO added an exclusion for damages "arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." *See id.* In 2013, the ISO added an optional endorsement that modified the "personal and advertising injury" definition to eliminate coverage for "oral or written publication, in any manner, of material that violates a person's right of privacy" which was a key basis of coverage for data breach claims. *See id.* Finally, in 2014, the ISO eliminated coverage for damages arising out of "any access to or disclosure of any person's or organization's confidential or personal information . . . or [t]he loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." *See id.*

127. *See* Zureich & Graebe, *supra* note 122, at 196.

128. Podolak, *supra* note 9, at 383.

129. Anderson, *supra* note 8, at 544.

130. *See* Podolak, *supra* note 9, at 383.

131. *See generally* Zurich Am. Ins. Co. v. Sony Corp. of Am. 6 N.Y.S.3d 915 (N.Y. App. Div. 1st Dep't 2015).

132. Anderson, *supra* note 8, at 543.

133. *See* Podolak, *supra* note 9, at 390.

134. *See id.*

a requirement not found in the language of the insurance policies."[135] The judge stated that "'insurance policies' coverage for the oral or written publication of materials that violate a person's right to privacy could not be triggered through the actions of third parties, in this case, the hackers . . . ."[136] In other words, because hackers stole the information, there was no publication by Sony, and thus no coverage.[137] In contrast to the holding in *Zurich,* courts should hold that information compromised by third party hackers does constitute a "publication," and afford coverage for such breaches,[138] as the U.S. District Court for the Eastern District of Virginia has held.[139]

The *Zurich* courts decision seems at odds with the FTC's reasoning for bringing its suits against companies that have inadequate cybersecurity. First, the relevant language in the CGL policy makes no mention of who must make the publication. The underlying class action suit against Sony alleged that Sony's security measures permitted the hackers to gain access to the network, meaning that Sony was responsible, as the FTC would argue, for the publication; this should at least have triggered the duty to defend.[140] Further, if the court holds that this was not a publication by Sony, but rather a publication by a third party, then how can the FTC sue and essentially blame companies for these third party hacks? The FTC is suing companies for publications by third parties, but they are not publications for insurers to protect. Companies are taking a hit from multiple sides with no help, prompting the need for stand-alone cyber risk insurance policies.

C. STAND-ALONE CYBER RISK INSURANCE

Recently, insurers have been marketing newer insurance products specifically tailored to covering cyber risks—this coverage has been called "the new frontier of the 21st century market."[141] This market was created in response to many insurers removing cyber coverage from CGL and other

135. Bibeka Shrestha, *Sony Fights Ruling That Nixed Data Breach Coverage*, LAW360 (Apr. 11, 2014, 2:53 PM), http://www.law360.com/articles/527570/sony-fights-ruling-that-nixed-data-breach-coverage.

136. *Id.*

137. *See* Podolak, *supra* note 9, at 390.

138. *See* DiCanio, *supra* note 109.

139. *See id.* The U.S. District Court for the Eastern District of Virginia held in *Travelers Indemnity v. Portal Healthcare Solutions,* that "making medical records accessible triggered the policy coverage, even though no third-party was alleged to have viewed the information, because, according to the court, '[p]ublication occurs when information is 'placed before the public' not when a member of the public reads the information placed before it.'" *Id.*

140. *See* Podolak, *supra* note 9, at 390.

141. Anderson, *supra* note 8, at 591–92 (quoting Harry Cylinder, *Evaluating Cyber Insurance*, CPCU EJOURNAL, Dec. 2008, at 1).

traditional policies;[142] in light of this change and court decisions such as *Zurich*, stand-alone cyber risk policies can cover the insurance coverage gap, giving companies an opportunity to mitigate the loss associated with a data breach.[143]

This cyber insurance market is referred to as the "Wild West" of insurance, as new policies are created on a regular basis and as old policies are constantly updated and revised.[144] However, what is clear is that the market intends for stand-alone cyber insurance policies and general CGL policies to work together.[145] Today, in most standard CGL policies, property damages coverage for electronic data[146] losses is limited to losses "that result from physical injury to tangible property, with tangible property being defined so as not to include electronic data."[147] On the other hand, stand-alone cyber policies tend to exclude coverage for property damage claims.[148] In light of inconsistent court decisions regarding CGL policy coverage, it is essential to companies' protection to receive advice on how to proceed in obtaining full coverage, using both types of policies.

Due to the increased publicity surrounding cybersecurity breaches and the insurance market for these breaches, the market is competitive—forcing cyber insurance plans to be greatly negotiable.[149] When companies are deciding which cyber insurance plan to purchase, they will want to obtain a cyber insurance policy that will:

> (1) defend and indemnify against claims alleging a data privacy incident or a breach of network security; and (2) pay the costs to investigate forensically a data privacy or cybersecurity incident, pay for an attorney . . . , [pay to] cover the costs to send out letters notifying individuals about the incident . . . , [and] pay the costs of credit or fraud monitoring products offered to affected individuals.[150]

In addition, companies should take advantage of policies that adhere to third party liabilities, as well as first party cyber loss. Third party cyber liability policies usually cover the insured company against liability arising from

---

142. *See generally* Jeff Sistrunk, *Sony Hack Shows Need for Cyber Coverage On Many Fronts*, LAW360 (Jan. 9, 2015, 2:04 PM), http://www.law360.com/articles/609561/sony-hack-shows-need-for-cyber-coverage-on-many-fronts.

143. *See* Epstein & Keyes, *supra* note 114.

144. *See* SCOTT GODES, UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW: LEADING LAWYERS ON ANALYZING RECENT TRENDS, CASE LAWS, AND LEGAL STRATEGIES AFFECTING THE INTERNET LANDSCAPE 45, 46 (2015).

145. *See* Podolak, *supra* note 9, at 403–04.

146. *See* Anderson, *supra* note 8, at 571–72 (electronic data is defined as "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CDROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.").

147. Podolak, *supra* note 9, at 403.

148. *See id.* at 403–04.

149. *See* Anderson, *supra* note 8, at 594.

150. GODES, *supra* note 144, at 46–47.

hacks and other third party data breaches. The types of events that give rise to this coverage include a failure to secure data, theft of property, network security failure, and/or acts, errors, or omissions of employees or third party vendors.[151]

On the other hand, companies will want to be cognizant of cyber risk policies that include important exclusions. Although "in many cases these exclusions are intended to limit coverage to the specialty area of cyber risk and to avoid overlapping with general liability, D&O or other insurance policies,"[152] because of the increased need for these policies, companies need to make sure that the policies are not excluding necessary coverage. Specifically, companies need to beware of cyber insurance policies that "expressly require that a loss be directly caused by, or solely and directly caused by, an insured cause," because this would again exclude liability for third party hacks,[153] similar to the *Zurich* case.

It is important to recognize that cyber risk insurers are aware of the fact that companies are purchasing this insurance in response to alleged governmental regulation and statutory violations.[154] This is exemplified by the *National Union Fire Insurance Company of Pittsburgh v. Coinstar, Inc.*[155] decision, where the court denied insurance coverage.[156] As *Coinstar* demonstrates, insurance companies are increasingly using governmental regulation and statutory violations to deny coverage for cyber breaches;[157] companies must beware of this exclusion.

As with every decision regarding insurance, companies must look to the costs of these insurance policies. The unpredictable probability and costs of data breaches make cybersecurity insurance very expensive.[158] For example, in 2013, cybersecurity insurance premiums totaled $1.3 billion.[159] Moreover, because of the high costs of this type of insurance, companies are put in the position of choosing whether to spend money on cybersecurity insurance or to invest in technology that they believe will improve their cybersecurity.[160] It is argued that because companies are beginning to invest in this type of

151. *See* Anderson, *supra* note 8, at 595.
152. Epstein & Keyes, *supra* note 114.
153. Podolak, *supra* note 9, at 405.
154. *See id.*
155. *See generally* Nat'l Union Fire Ins. Co. of Pittsburgh v. Coinstar, Inc., 39 F. Supp. 3d 1149 (W.D. Wash. 2014).
156. *See* Thomas B. Caswell, *2014 May Be Cyber Insurance's Most Popular Year Yet*, LAW360 (Mar. 21, 2014, 12:36 AM), http://www.law360.com/articles/520146/2014-may-be-cyberinsurance-s-most-popular-year-yet (explaining that on February 28, 2014, the U.S. District Court for Seattle ruled in *National Union Fire Insurance Company of Pittsburgh v. Coinstar Inc.,* that "the common liability policy exclusion for a 'violation of statute in connection with sending, transmitting or communicating any material or information' served to preclude any coverage for the hacking of PII from Coinstar's video rental kiosks.").
157. *See* Podolak, *supra* note 9, at 405.
158. *See* Garrie & Mann, *supra* note 26, at 384.
159. *Id.*
160. *See id.* at 385.

insurance, that if these policies "indemnify state actions, administrative fines, property damage, business interruption, and consumer lawsuits arising from a breach," companies will not have an incentive to devote sufficient resources to their own security measures in an attempt to prevent such breaches.[161] This argument is flawed—because the main purpose of cyber risk insurance policies is to allow the insured to transfer the risk of a breach or compromise of its network, "[i]t comes as no surprise . . . that insurers concentrate on the implementation and maintenance of appropriate security and IT protocols as the foundation of the coverage."[162] Insurance companies will even deny coverage to companies that do not have the cybersecurity measures in place that they deem sufficient.[163]

Further, the Department of Homeland Security has stated that "a robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection."[164] In addition, according to the Ponemon Institute, "preparing for a breach can greatly reduce the cost of a breach."[165] Insurers will reward the companies that choose to take precautionary steps, including "implement[ing] defensive measures such as an incident response plan and designat[ing] a team to execute that plan."[166] As such, it is likely that if a company spends a great deal on its cybersecurity infrastructure, cyber insurance agencies will offer insurance at a lower premium.[167]

As interpretations of cyber insurance policies are still in their infancy, it is crucial that companies understand their insurance policies and their risk in this developing area of law.[168] To do so, companies need courts to affirm solid and dependable insurance risk transfer strategies; "and now that the area of insurance for privacy and cyber security risks is expanding, there is likely to be an explosion of litigation regarding the meaning of insurance policies that cover these new and burgeoning risks."[169] It is essential that companies can follow settled law regarding cyber insurance, as the objective of such

161. *Id.*
162. Podolak, *supra* note 9, at 406.
163. *See* GODES, *supra* note 144, at 47–48 (explaining that in *Columbia Casualty Company vs. Cottage Health System,* a CNA insurance company sued Cottage Health, the insured, for failing to maintain minimum security practices; they argued that such failure allowed CNA to avoid covering the claim).
164. Davis, Li-Ming Wong & Paterson, *supra* note 6, at 647 (quoting the Department of Homeland Security).
165. Reynolds, *supra* note 115.
166. *Id.*
167. *See* Garrie & Mann, *supra* note 26, at 385.
168. *See* GODES, *supra* note 144, at 57.
169. *Id.*

insurance is to give companies an additional layer of financial security in times of heightened government regulation.[170]

IV. THE NEED FOR CYBERSECURITY LEGISLATION AND GUIDELINES

A. FOLLOWING THE LEAD OF HIPAA AND GLBA

"It is no longer a matter of *if* a breach is going to happen, but rather *when*."[171] As argued in Part II *supra*, prevention will never be enough and therefore, the FTC should not have the authority to sue companies for not implementing cybersecurity practices that neither the FTC, nor Congress, have ever set out. Instead, Congress should pass legislation for the corporate business sphere, similar to HIPAA in the health sphere and GLBA in the financial sphere. Similar to HIPAA and GLBA, the newly established legislation should give power to the FTC to institute guidelines for companies to follow when implementing security procedures; if done, these companies will know how to sufficiently protect themselves pursuant to the FTC's standards.

To begin, "[t]he financial sector is more secure than other industries and operates under specific cybersecurity mandates embedded in law. This correlation is no coincidence."[172] In 1999, President Clinton signed GLBA into law.[173] Subtitle A of GLBA Title V requires the FTC and other federal agencies to "establish appropriate standards for the financial institutions . . . relating to administrative, technical, and physical safeguards" for certain information.[174] The FTC issued the Safeguards Rule,[175] which "requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure."[176] The FTC believes that this rule strikes an appropriate balance between allowing flexibility to financial institutions and establishing standards of safeguarding consumer information.[177] If the FTC struck a balance there, it should do the same in the corporate business sphere as well. Further, there is evidence that GLBA's dilute mandate

---

170. *See id.*

171. Patricia Bailin & Arielle Brown, *Preparing for A Data Breach: Data Security Regulations and Best Practices*, 32 WESTLAW J. COMPUTER & INTERNET 1, 1 (2015).

172. Bambauer, *supra* note 15, at 1050.

173. *See* Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.1–5 (2016).

174. 15 U.S.C. § 6801(b) (2012) (explaining that the objectives of these standards are to: "(1) [e]nsure the security and confidentiality of customer records and information; (2) protect against any anticipated threats [to the security of] such records; and (3) protect against unauthorized access to or use of such records or information [that could cause harm to the customer].").

175. *See generally* 16 C.F.R. § 314.

176. *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying [hereinafter *Complying with the Safeguards Rule*].

177. *See* 16 C.F.R. § 314.

increases cybersecurity for financial institutions; "[i]n a study by WhiteHat Security, banking websites had the fewest average serious security vulnerabilities of any industry. . . ."[178] If the FTC's main goal is to prevent cyber attacks, the best way to do that is to follow the financial industry's lead.

HIPAA Title II, similar to GLBA, requires the Department of Health and Human Services (HHS) to draft rules to increase the efficiency of the health care system by creating standards and guidelines for the use and dissemination of health care information, in order to protect the privacy and security of such information.[179] The Security Rule[180] was adopted in 2003[181] to implement the provisions of HIPAA. HIPAA's Security Rule is known to be "one of the most specific data security laws,"[182] and the new cybersecurity regulation guidelines for the corporate business sphere should mimic its structure.

Congress needs to pass legislation that gives the FTC authority to adopt a rule or regulation such as the Safeguards Rule and the Security Rule mentioned above. In doing so, "[a] regulatory strategy must be developed to strike a healthy balance between consumer-privacy interests and companies' interests in innovation and profit. Data-security enforcement standards cannot be so rigid as to stifle business growth or give hackers time to exploit the rules."[183] The following guidelines are recommendations for the first proposed rule in hopes to solicit comments to improve the guidelines to strike this balance.[184] This set of guidelines is not a one-size-fits all list; instead, it is meant to give companies guidance on how to structure their own security programs to avoid suit by the FTC in the event of a breach.[185]

178. Bambauer, *supra* note 15, at 1049.

179. *See Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html (last visited Nov. 22, 2015) [hereinafter *Summary of HIPAA*].

180. *See* CTR. FOR MEDICARE & MEDICAID SERVS., SECURITY STANDARDS: ADMINISTRATIVE SAFEGUARDS 27–28 (2007) [hereinafter SECURITY STANDARDS], https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf (providing that the Security Rule has three safeguard guidelines sections: (1) Administrative Safeguards in §164.308; (2) Physical Safeguards in §164.301; and (3) Technical Safeguards in §164.312).

181. *See generally Summary of HIPAA*, *supra* note 179.

182. Solove & Hartzog, *supra* note 2, at 655 (explaining that "the HIPAA Security Rule requires organizations to access the control risk by implementing security programs, testing the company's data security, ensuring that outside data vendors secure data, training employees in data security, and implementing authentication and access control procedures." In addition, this security rule "requires technical safeguards, such as identification access controls and encryption, and physical safeguards, such as secure data disposal and physical access safeguards.").

183. Moncada, *supra* note 67, at 941.

184. *See* Department of Health and Human Services, 68 Fed. Reg. 8334 (Feb. 20, 2003).

185. *See* Davis, Li-Ming Wong & Paterson, *supra* note 6, at 650.

B. RECOMMENDATION OF GUIDELINES TO IMPLEMENT[186]

Companies are required to deter, detect, and defend against security breaches.[187] To start, companies must form a compliance team to understand and relay to their employees the correct way to comply with the new guidelines. Next, companies must hire a security team of cybersecurity-certified experts to work with the compliance team in implementing the safeguard guidelines below. This security team shall "develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards that are appropriate to [the company's] size and complexity, the nature and scope of [the company's] activities, and the sensitivity of any customer information at issue."[188] If a corporate entity fails to follow the guidelines listed below, and a data breach follows, the entity will be on notice that the FTC has the authority to bring action for such violations.

First, there must be an employee management and training division, where the company will be required to designate a privacy team responsible for developing and implementing its privacy policies and procedures.[189] Therein, the company shall designate one Security Official for the overall responsibility of the development and implementation of security procedures.[190] This security team shall: (1) conduct a background check on each employee who will have access to customer information;[191] (2) train its engineers in secure coding;[192] and (3) train the company's employees on its privacy policies and procedures, including basic steps to maintain the security, confidentiality, and integrity of customer information.[193] In doing so, the company shall implement a security awareness and training program for all of the employees to complete.[194]

Next, each company must have information systems to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information,[195] and assess the sufficiency of any safeguards in place to control those risks. To do this, each company shall "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected . . . information held by the [company]."[196]

---

186. The following proposed guidelines were created by using and combining the published findings from the FTC's holdings in data-breach cases and the guidelines in GLBA and HIPAA.

187. *See generally Complying with the Safeguards Rule*, *supra* note 176.

188. Standards for Safeguarding Customer Information, 16 C.F.R. § 314.3(a) (2016).

189. *See* 15 U.S.C. §§ 6801(b), 6805(b)(2) (2012).

190. *See* SECURITY STANDARDS, *supra* note 180, at 8.

191. *Complying with the Safeguards Rule*, *supra* note 176.

192. *See* START WITH SECURITY, *supra* note 70.

193. *Complying with the Safeguards Rule*, *supra* note 176.

194. *See* SECURITY STANDARDS, *supra* note 180, at 14.

195. *See* 15 U.S.C. §§ 6801(b), 6805(b)(2) (2012).

196. SECURITY STANDARDS, *supra* note 180, at 4.

Therein, each company shall only collect information from consumers that the employees, based on their security training, believe is necessary.[197] When the necessary information is collected, the company must dispose of it when the legitimate business need for it has subsided.[198] In addition, the company shall restrict employee access to a "need to know" basis and tailor administrative controls specifically to each employee's job needs.[199]

Each security team must develop technical safeguards to protect its information by implementing technical policies and procedures for its electronic information system.[200] In doing so, the company shall develop a unique authentication process. In addition to the use of passwords, companies should implement more secure authentication methods such as tokens or biometrics in which the employee must, for example, use his or her fingerprint and then type in his or her unique identification password.[201] This system should automatically log the user out after a thirty-minute period of inactivity. Further, companies shall implement a mechanism to encrypt electronic information to secure confidential material during storage and transmission; in doing so, the team shall make sure that the cryptography is secure throughout its lifecycle, not just during the initial transmission.[202] To do this, the data security team shall use a "tried-and-true industry tested and accepted method[]" to ensure the upmost trusted protection.[203]

Next, the company must "[i]mplement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."[204] The security team shall test the system for vulnerabilities at least once a week and must have intrusion detection and prevention software to monitor the network for suspicious hacking activity. In addition, there must be sufficient measures in place that have been tested to detect unauthorized access to its network.[205] Further, the team shall set security alerts and have an effective process in place to receive, address, and respond to security vulnerability reports and alerts.[206] The team shall evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring; they must update and test procedures regularly to address vulnerabilities that have the potential to arise.[207] The company must continuously improve its system to keep up with the fast-changing pace of

197. *See* START WITH SECURITY, *supra* note 70, at 2.
198. *See id.*
199. *Id.* at 3.
200. *See* Department of Health and Human Services, 68 Fed. Reg. 8334, 8356 (Feb. 20, 2003).
201. *See* Gupta, Lahiff & Swaminathan, *supra* note 63, at 7; *see also* Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164.312 (2016).
202. *See* START WITH SECURITY, *supra* note 70, at 6.
203. *See id.*; *see also* 45 C.F.R. § 164.312.
204. Department of Health and Human Services, 68 Fed. Reg. at 8377.
205. *See* START WITH SECURITY, *supra* note 70, at 8.
206. *See* 15 U.S.C. §§ 6801(b), 6805(b)(2) (2012).
207. *See id.*

cybersecurity attacks, strategies, and regulator activity.[208] Each employee must sign a statement of adherence to the security policies and procedures and, if violated, the employee will be subject to[209] a set of disciplinary procedures set out by the company.[210]

Further, each corporate entity must select service providers that can maintain appropriate safeguards; the company must make sure its contract requires service providers to maintain safeguards, and the company must oversee service providers' handling of customer information.[211] The security team shall continue to monitor to ensure that the service provider is meeting the company's requirements.[212] The company shall request that detailed records be kept on parties with access to the corporation's data stores and shall ensure that third parties entrusted with this access have data security policies of comparable strength to the corporation.[213]

In the event that a breach occurs, the company must have an established incident response plan including a response team, developed procedures for working with law enforcement, a customer notification and assistance process,[214] and a contingency plan that includes a disaster recovery plan.[215] The company must mitigate any harmful effect it learns was caused by use or disclosure of protected information. In doing so, it must: (1) take immediate action to secure any information that has been compromised; (2) preserve and review files or programs that may reveal how the breach occurred; and (3) if feasible, bring in security professionals to help assess the breach.[216]

Lastly, each company must develop a Written Information Security Plan (WISP) outlining their security practices so that, if a breach does occur, the company can readily hand the WISP over to the FTC and the company's insurance provider to promptly address the issue of whether the company took reasonable security precautions.[217] The WISP shall document the information collected and stored by the company, along with the protocols, based on the guidelines, for handling each record.[218]

The FTC cannot regulate the aforementioned list of guidelines without receiving the power to do so from Congress. Only then will the FTC have the authority to regulate any company whose database stores consumer data.

---

208. *See* Davis, Li-Ming Wong & Paterson, *supra* note 6, at 652–53.
209. *See* SECURITY STANDARDS, *supra* note 180, at 6.
210. *See* Davis, Li-Ming Wong & Paterson, *supra* note 6, at 649.
211. *See Complying with the Safeguards Rule*, *supra* note 176, at 2.
212. *Id.*
213. *See* Davis, Li-Ming Wong & Paterson, *supra* note 6, at 652.
214. *See* Bailin & Brown, *supra* note 171, at 3.
215. *See* Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164.308(a)(7)(i) (2016).
216. *Complying with the Safeguards Rule*, *supra* note 176, at 5; *see also* SECURITY STANDARDS, *supra* note 180, at 17.
217. *See* Bailin & Brown, *supra* note 171, at 2.
218. *See id.* at 4.

Companies will be required to meet the guidelines eventually set out as formal rules by creating a security team to implement the guideline procedures. Companies that meet these guidelines will ensure protection against FTC suit, as well as coverage from their insurance company.

CONCLUSION

In this era of increasingly sophisticated cyber crime, where "[e]very 79 seconds, personal data [is] stolen,"[219] the corporate business sphere is in desperate need of data security implementation guidelines. Companies are suffering significantly due to the FTC's data security enforcement litigation. As of now, in the absence of any Congressional action, the FTC is an inappropriate body to handle these types of breaches, and because it continues to do so, it is imperative that companies protect themselves with the aforementioned cyber insurance policies. The legislation enacted by Congress, and thereafter the data security rules and guidelines promulgated by government agencies in the financial and health spheres, have been successful; it is therefore at this point necessary for the corporate business sphere to follow their lead and look to this Note's proposed solution. Companies must be put on notice to not only protect consumers from the risk of information loss, but to protect the companies themselves from FTC action.

Jennifer Gordon[*]

219. Abbott, *supra* note 31.

* B.A., Binghamton University, 2014; J.D. Candidate, Brooklyn Law School, 2017. I would like to thank my family and friends, particularly my parents, Anne LaGorga Gordon and Mark Gordon, for their constant love, support, and guidance. I would also like to thank everyone at the Brooklyn Journal of Corporate, Financial & Commercial Law, in particular, Jordan Meddy and Alissa Cardillo, for their time and effort in helping prepare this Note for publication.