ENHANCING CYBERSECURITY IN THE PRIVATE SECTOR BY MEANS OF CIVIL LIABILITY LAWSUITS—THE CONNIE FRANCIS EFFECT

Jeffrey F. Addicott *

INTRODUCTION

"*Getting cyber security right requires new thinking. But certain principles remain true in cyberspace as they are true about security in the physical world.*"[1]

—George Osborne

Change is an inevitable component of the human experience, both for individuals and the businesses that they operate within society. Sometimes changes in business standards and practices are brought about simply through the normal course of technical "evolution,"[2] but in other cases changes are brought about as the result of new laws.[3] While the Constitution most certainly envi-

* Professor of Law and Director of the Center for Terrorism Law, St. Mary's University School of Law. B.A., University of Maryland; J.D., University of Alabama School of Law; LL.M., The Judge Advocate General's Legal Center and School; LL.M. (1992) and S.J.D. (1994), University of Virginia School of Law. This article was prepared under the auspices of the Center for Terrorism Law located at St. Mary's University School of Law, San Antonio, Texas. The author wishes to acknowledge with special thanks the superb efforts of Alec T. Dudley, a second-year law student at St. Mary's University School of Law, who supported this article with outstanding research and editing.

1. Rt. Hon. George Osborne, Chancellor's Speech to GCHQ on Cyber Security (Nov. 17, 2015), https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cybersecurity.

2. The term evolution is not employed to refer to the Darwinian theory that gradual changes in the physical world are brought about by a process of natural selection and mutations. Evolution here refers to the workings of intelligence to make improvement. For a discussion of how the term evolution is misused see Jeffrey F. Addicott, *Storm Clouds on the Horizon of Darwinism: Teaching the Anthropic Principle and Intelligent Design in the Public Schools*, 63 OHIO ST. L.J. 1507, 1523 (2002) [hereinafter Addicott, *Storm Clouds*].

3. *See, e.g.*, David A. Westenberg, *Buckle Up or Pay: The Emerging Safety Belt Defense*, 20 SUFFOLK U.L. REV. 867, 868 (1986) (explaining how tort actions penalizing un-

sions that laws should emanate from the legislative branch of government, legal mandates rooted in the rich heritage of common law can come from the workings of the judicial branch. Indeed, in the modern world, jurisprudence has been a vital component in shaping—or attempting to shape—normative behavior within society by pronouncing new legal obligations, sometimes even in opposition to the majority will of the people.[4]

In the context of shaping private sector practices regarding a given business' duty owed to those injured as a result of negligence, the impact of civil action lawsuits has produced great change. While there is no question that tort litigation has brought about a sea of change in how businesses now approach maintaining "reasonable" security protections in the physical world to shield themselves from liability, this same spirit of concern and the accompanying change has not yet bled over into the cyber world. This inequity of security precautions is particularly troubling when one considers that the threat of harm to both individuals and the nation by means of cyber attacks has extreme destructive potential. Further, because much of the responsibility for ensuring safety in the cyber world rests in the hands of private business and not the government, it is imperative that the private sector be motivated to develop far greater levels of cybersecurity than currently exists.

The purpose of this article is to explore the threats posed by cybersecurity breaches, outline the steps taken by the government to address those threats in the private sector economy, and call attention to the ultimate solution, which will most certainly spur private businesses to create a more secure cyber environment for the American people—a Connie Francis-styled cyber civil action lawsuit.[5]

buckled vehicle occupants can foster increased seat belt use); *see also* Williams J. Holdorf, *The Fraud of Seat-Belt Laws*, FOUND. FOR ECON. EDUC. (Sept. 1, 2002), https://fee.org/articles/the-fraud-of-seat-belt-laws/ (describing that the vast majority of Americans opposed the enactment of seat-belt laws).

4. A recent illustration of this concept occurred with the 2015 Supreme Court decision, *Obergefell v. Hodges*, where the Court held that same-sex marriage was a fundamental right that states were required to recognize. 135 S. Ct. 2584, 2604–05 (2015). Prior to the Court's ruling, the vast majority of states had rejected calls for same-sex marriage. Even California passed Proposition 8 in 2008 establishing marriage as only between a man and a woman. *See* Tamara Audi et al., *California Votes for Prop 8*, WALL ST. J. (Nov. 5, 2008), http://www.wsj.com/articles/SB122586056759900673.

5. *See* Garzilli v. Howard Johnson's Motor Lodges, Inc., 419 F. Supp. 1210, 1211–14

I. THE CONNIE FRANCIS EFFECT

"*These kinds of suits [tort civil actions] create economic incentives for crime prevention . . . Now when you check into a hotel and you get a room key that looks like a credit card instead of your house keys, that is because of a civil lawsuit. It is cheaper for hotels to install an electronic lock system than face the liability exposure of judgments or settlements. . . .*"[6]

—Jeffrey Dion

Those of age and those who enjoy the pop music of the 1950s and 1960s easily recall the fabulous vocals of the internationally known American "singer, recording artist, and professional entertainer,"[7] Connie Francis.[8] Francis' songs had a meaningful and long-lasting effect on music and the music industry of her time. What few realize, however, is that Ms. Francis is also known for the phenomenal impact that she had in directly improving hotel security standards throughout the country. As the result of a civil action lawsuit she brought against Howard Johnson's Motor Lodges in 1976,[9] the large monetary jury award rendered for the plaintiff had a watershed impact on improving security standards not just for the Howard Johnson Motor Lodge chain, but for the entire hotel and motel industry in the United States. Without a doubt, her case directly led to vast improvements in both the quantity and quality of physical security measures—the industry was finally forced to realize their susceptibility to civil lawsuits

(E.D.N.Y. 1976) (holding that the jury's award for plaintiff, Connie Francis, was not excessive because of her projected lost income and pain and suffering after being attacked in her room at a motel).

6. *See* Brenda Craig, *Legendary Connie Francis Unsung Hero of Crime Victims Everywhere*, LAWYERSANDSETTLEMENTS.COM (Dec. 22, 2015), https://www.lawyersandsettlements.com/articles/criminal-law/interview-criminal-law-penal-offense-3-21141.html (quoting Jeffrey Dion, Deputy Executive Director of the National Center for Victims of Crime, discussing the Connie Francis suit).

7. *Garzilli*, 419 F. Supp. at 1211.

8. *See generally Biography,* CONNIE FRANCIS: THE OFFICIAL SITE, http://www.conniefrancis.com/bio4 (last visited Feb. 13, 2017) (giving the biography of singer Connie Francis and discussing her impact on the American hotel industry).

9. *See Garzilli*, 419 F. Supp. at 1211–12. At the time of the lawsuit, Connie Francis was married to her third husband, Mr. Frank Garzilli. Her legal name at the time was Mrs. Connie Francis Garzilli. *See id.*

and the accompanying need to avoid the ensuing scrutiny of a jury for similar claims of negligence.[10]

The story of how this all came to be is rooted in a horrific sexual assault at knifepoint which occurred in Ms. Francis' hotel room at a Howard Johnson Motor Lodge in 1974.[11] Coming out of a three-year retirement from live public performances, Francis began a nationwide singing tour where her first appearance was at the Westbury Music Fair in Westbury, Long Island, New York.[12] On the late evening of November 7, 1974, marking the fourth night of that engagement there, she returned to her room at the Howard Johnson Motor Lodge where she had been staying. Later that evening, a knife-wielding intruder entered her hotel room through a sliding glass door. The door gave the false appearance of being securely locked but, in actuality, was easily opened from the outside. Upon gaining entry, the unknown assailant proceeded to brutally beat and rape Ms. Francis, who believed her life was only spared because she claimed that she was a famous singer and told her attacker that a relentless investigation would result if she were murdered.[13] The subsequent lawsuit filed in 1976, *Garzilli v. Howard Johnson Motor Lodges, Inc.*, alleged the following: "Action was brought against motel owner for pain, suffering, mental anguish, humiliation and loss of earnings resulting from wife being criminally assaulted in motel and by husband for deprivation of society, companionship and services of wife."[14]

Common law tort litigation is an ancient component of Anglo-Saxon law and is concerned with the duty owed to a victim of harm due to the negligence of someone charged with protecting the victim while on their premises or under their control or protection.[15] Obviously, the actual wrongdoer is subject to civil liability. However, the culprit is often unknown or judgment proof, leaving the victim to look for redress from the owner or operator

10. *See* Chad Callaghan, *Safeguarding Hotel Guests*, HOTEL BUS. REV., http://hotelexecutive.com/business_review/2808/safeguarding-hotel-guests (last visited Feb. 13, 2017).

11. *See* Richard Harrington, *Connie Francis' Crusade*, WASH. POST (Dec. 16, 1981), https://www.washingtonpost.com/archive/lifestyle/1981/12/16/connie-francis-crusade/bbf949bc-cffa-44ae-95d0-4c1f97e7c452/.

12. *Biography*, CONNIE FRANCIS: THE OFFICIAL SITE, http://www.conniefrancis.com/bio4 (last visited Feb. 13, 2017).

13. *See id.*

14. *Garzilli*, 419 F. Supp. at 1210.

15. *See* Palsgraf v. Long Island R. Co., 162 N.E. 99, 101 (N.Y. 1928).

of the public facility responsible for their reasonable safekeeping under the law. As one commentator has rightly put it:

> Tort litigation is often trilateral in character. Interposed between the injurer and the victim is a sentinel charged with protecting the victim. The sentinel is remiss and the inadequately protected victim is harmed by a wrongdoer, one whom the sentinel should have, but did not, repel. The victim may sue both the injurer and the sentinel, but often the injurer is either unknown or insolvent.[16]

Up until the *Garzilli* case, the avenue of suing the sentinel had been a less than satisfactory proposition for most victims of crime such as Connie Francis. While tort law had long recognized "that a special relationship between two parties gives rise to an affirmative duty to act"[17] with due care in the context of that special relationship, the awarded damages for a negligent breach of that duty had been rather minimal. The types of "special relationships" recognized under the law include such things as innkeeper/guest, tavern owner/patron, common carrier/passenger, corporate officer/stockholder, prison facility/inmate, and school/student.

After an emotionally charged four-week trial, made even more notable due to the celebrity status of Connie Francis, the jury awarded the plaintiffs an unprecedented $2,650,000 in total damages after finding that the motel's failure to provide reasonable security measures was the proximate cause of the beating and rape.[18] The fact that the court acknowledged ample evidence of negligence on the part of Howard Johnson's Motor Lodges and absolutely no evidence of contributory negligence by Ms. Francis, certainly helped increase the amount of awarded damages.[19] At

16. William K. Jones, *Tort Triad: Slumbering Sentinels, Vicious Assailants, and Victims Variously Vigilant*, 30 HOFSTRA L. REV. 253 (2001). Liability in a negligence action requires that the victim prove: (1) that the defendant had a duty to the plaintiff to take reasonable care to avoid the attack or reduce its risk; (2) that defendant breached this duty; (3) that the breach was the actual and legal cause of the attack; and (4) that the breach resulted in actual harm. *See* Mark P. Buell, *Liability for Inadequate Security*, 69 FLA. B.J. 58 (1995).

17. R. Jeffrey Harris, *Whither the Witness the Federal Government's Special Duty of Protection in Criminal Proceedings After* Piechowicz v. United States, 76 CORNELL L. REV. 1285, 1292 (1991).

18. *See* Daniel B. Kennedy & R. Thomas Hupp, *Apartment Security and Litigation: Key Issues*, 11 SECURITY J. 21, 22 (1998). The jury awarded Connie Francis "$2.5 million in compensatory damages and her husband $150,000." Ms. Francis later settled with Howard Johnson's for $1.5 million. *Id*.

19. *See Garzilli*, 419 F. Supp. at 1212 n.2 ("Plaintiffs' proof with respect to defendant's negligence and proximate cause was ample and there was little, if anything, on which to

the time, the recovery in *Garzilli* was the largest judgment ever awarded where a third party was held liable for an act of sexual assault which had occurred on their premises.[20] In terms of damages, the court stated the following:

> Connie Francis' projected loss of earnings for the ensuing ten years would have been $2,585,000 and this would have made no allowance for the substantial cost-of-living increases which occurred between 1969 and 1974. In addition, of course, none of such calculations makes any allowance whatsoever for the criminal assault, the horrendous results which ensued therefrom and the pain, suffering, mental anguish and humiliation which followed.[21]

If the hotel and motel industry did not previously comprehend that they could be held liable for such vast sums of money for foreseeable criminal injuries suffered by tenants or guests on their premises, they did after *Garzilli*. *Garzilli* greatly expanded the legal obligations owed to tenants in terms of "reasonableness;" which, in turn, expanded the level of care now owed to prevent such foreseeable criminal harm.[22] In other words, by raising the bar for reasonableness, *Garzilli* set a most telling precedent for premises owners and operators regarding their "vicarious . . . liability for intentional torts committed by intruders."[23] Now viewed through the new prism of the Connie Francis case, if premises owners did not institute greater level of reasonable precautions to protect guests on their property from the foreseeable criminal acts of third parties, they could face huge monetary punishments.[24] In addition, *Garzilli* signaled that courts would now increase the duty of care owed by the hotel industry by expanding the scope of constructive notice regarding any prior criminal incidents that had occurred on the hotel/motel property, even if such crimes were different than those inflicted upon the plaintiff.[25] The

base an argument that either or both of them was contributorily negligent.").

20. Robert Alan Palmer, *The Hospitality Customer as Crime Victim: Recent Legal Research*, 13 J. HOSPITALITY & TOURISM RES. 225, 226 (1989).

21. *Garzilli*, 419 F. Supp. at 1213.

22. *See* Michael Green & William C. Powers, Jr., *Apportionment of Liability*, 10 KAN. J.L. & PUB. POL'Y 30, 38–39 (2000).

23. Alan O. Sykes, *The Boundaries of Vicarious Liability: An Economic Analysis of the Scope of Employment Rule and Related Legal Doctrines*, 101 HARV. L. REV. 563, 598 (1988).

24. *See generally* Ellen Bublick, *Upside Down? Terrorist*, *Proprietors*, *and Civil Responsibility for Crime Prevention in the Post-9/11 Tort-Reform World*, 41 LOY. L.A. L. REV. 1483, 1508–11 (2008) (discussing the expanded view of tort liability).

25. See Frederick B. Jonassen, *The Law and the Host of* The Canterbury Tales, 43 J.

court in *Garzilli* noted that four previous burglaries on the premises had essentially put Howard Johnson's Motor Lodge on constructive notice to take a higher level of what it had previously considered to be "reasonable care" for its guests. According to the court, it was not enough that new locks had been ordered but were not yet installed at the time of the rape.[26]

The *Garzilli* case continues to be cited in a multitude of legal journals throughout the United States as the seminal case discussing tort liability vis-à-vis improved hotel and motel security standards.[27] In terms of demonstrating how the law can evolve to advance new societal norms and standards, law journals invariably note how the entire legal landscape relative to victims' rights has been altered by the Connie Francis case.[28] This one case launched an avalanche of litigation against owners and operators of all sorts of business establishments, not just hotels. In the wake of *Garzilli*, scores of civil actions were filed across the nation not only by victims assaulted at hotels or motels, but also at shopping malls, movie theatres, restaurants, bars, public parks, etc.[29]

While victims in their individual capacities could now expect just compensation for their injuries based on the precedent set by *Garzilli*, the collateral impact of the Connie Francis jury award dramatically impacted the general public, as well. Increased physical premises security meant greater peace of mind for the countless number of people who lodge at such facilities. Furthermore, the sea of change in improved security measures spawned by *Garzilli* took place quickly. Similar to the reaction of beachgoers to news of a shark attack, the movement within the hotel industry to greatly increase security measures was swift and dramatic. Almost overnight, owners and operators spent significant funds to vastly improve all things related to physical security, including better locks and lighting.[30]

MARSHALL L. REV. 51, 78 (2009), for an excellent discussion on innkeeper liability.

26. *See id.*

27. *See, e.g.*, Buell, *supra* note 16, at 58; Jordan H. Leibman, *Comparative Contribution and Intentional Torts: A Remaining Roadblock to Damages Apportionment*, 30 AM. BUS. L.J. 677, 677 (1992).

28. *See, e.g.*, William K. Jones, *Tort Triad: Slumbering Sentinels*, *Vicious Assailants*, *and Victims Variously Vigilant*, 30 HOFSTRA L. REV. 253, 253 (2001).

29. *See* Buell, *supra* note 16, at 58.

30. *See* Chad Callaghan, *Lodging No Complaints*, 45 SECURITY MGMT. 72, 72 (2001);

In summary, the significant improvements in hotel and motel physical security in the United States was not the result of legislative initiative or executive mandate, but rather the workings of a single civil action litigation. In large part, the reason for what might be termed the Connie Francis effect rests in the nature of capitalism. While capitalism is undoubtedly the best economic protocol known to mankind for ensuring the maximum amount of individual and collective prosperity within a national entity,[31] it clearly operates at its best when the owners and operators of businesses in the private sector economy possess and are motivated by virtue,[32] not just profit. Sadly, those that are motivated solely for profit will only respond in positive ways when under a cost-benefit analysis based on a loss of revenue or the threat of a loss of revenue. For the "crooked" capitalist, virtuous behavior must be forced.

In much the same way that the Connie Francis lawsuit spurred a quantum leap forward in improved physical security for certain businesses, a similar scenario will soon shape the future of cybersecurity practices in the private sector. Not a day passes that news outlets do not report new cybersecurity breaches of one sort or another.[33] As more data breaches occur due to increased cyber attacks and harm results from the unauthorized release of personally identifiable information ("PII"), or more importantly, actual physical harm, civil law suits will proportionally mount to sue those targeted businesses that have failed to provide reasonable cybersecurity protections. As with *Garzilli* and its progeny, it is certainly likely that the concept of reasonableness for maintaining appropriate cybersecurity will soon far exceed current industry standards. Indeed, with every new cyber related lawsuit,

Susan H. Ivancevich & Daniel M. Ivancevich, *Mitigating Inadequate Security Claims Through Effective Security Measures*, 2 GAMING RES. & REV. J. 49, 50 (1995); Chad Callaghan, *Safeguarding Hotel Guests*, HOTEL BUS. REV., http://hotelexecutive.com/business_review/2808/safeguarding-hotel-guests (last visited Feb. 13, 2017).

31. *See generally* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS (1776) (exploring the causes of wealth creation).

32. *See* R.B. THIEME, JR., CHRISTIAN INTEGRITY 51–56 (2002) (equating the requirements of citizenship with impersonal love, integrity, and virtue); *see also*, JEFFREY F. ADDICOTT, TERRORISM LAW: MATERIALS, CASES, COMMENTS 357–67, 385 (7th ed. 2014) (discussing the nature of virtue and distinguishing the requirements of being a model citizen with the mechanics of grace salvation) [hereinafter ADDICOTT, TERRORISM LAW].

33. *See, e.g.*, Drew Fitzgerald, *Source of Cyberattack Narrowed*, WALL ST. J., Oct. 26, 2016, at A2 (speculating that the massive cyber attack in the United States on October 21, 2016 which hit Netflix, Twitter, and other websites, was the work of non-state actors).

businesses are being put on notice that greater levels of cybersecurity are expected, and juries will become less receptive to excuses. Still, as of this writing, most businesses seem content to simply hold their breath and wait. They seem unwilling to take the necessary steps to put sufficient time and money into improving their cybersecurity posture in anticipation of the future tort actions that will surely come. Again, it is as if they are awaiting the Connie Francis touchstone cyber tort lawsuit with unfathomable monetary damages before they will respond. Nevertheless, when the Connie Francis-styled cyber lawsuit comes, and it will, America will see the transformation overnight as cybersecurity upgrades cascade throughout the private sector, proving once again that economic principles are the catalyst for much needed improvement.

II. THE DEFINITIONAL FRAMEWORK OF CYBER

The fantastic workings of cyber technology have made the world of today vastly different than it was in the day of Connie Francis and her contemporaries. In a nutshell, the modern world we now enjoy is totally dependent on the workings of the cyber world. In 2014, the United States Supreme Court expressed this matter in terms of the mobile phone, but it applies to our dependence on all things cyber: "[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[34]

With billions of users, the cyber realm not only facilitates human communication—e.g., by Internet or mobile phone—it also consists of complex software packages and databases that regulate all aspects of societal infrastructure. These regulatory databases include the provision of water, electricity, banking, transportation, technology, agriculture, medical, nuclear facilities, waste management, and other services of government. While most of these services have utilized an electronic medium for some time, the major difference now is that we cannot operate any of them apart from the workings and complex actions of cyber technology. This dependency opens up new vulnerabilities that sorely challenge the limits of current cybersecurity protection.

34. Riley v. California, 134 S. Ct. 2473, 2490 (2014).

As with any technical field of endeavor, scores of new and unfamiliar terms associated with cyberspace have entered the modern lexicon. Accordingly, before one can fully discuss the need for improving cybersecurity, certain foundational terms require definition. Chief among the baseline concepts are: cyberspace, critical infrastructure, supervisory control and data acquisition ("SCADA"), and cyber attacks.

A. *Cyberspace*

The central term of discussion is labeled cyberspace. Cyberspace has many connotations and is used in a variety of contexts; synonyms include virtual space and cyber world. In the common understanding of the term, cyberspace refers to the entire function of computer-centric information technology ("IT")—hardware and software—as it is created, stored, and transmitted in the non-physical (cyber) and physical world. A 2016 Congressional Service Report refers to cyberspace as follows: "[T]he worldwide collection of connected ICT [Information and Communication Technology] components, the information that is stored in and flows through those components, and the ways that information is structured and processed."[35]

The Department of Defense Dictionary of Military and Associated Terms defines cyberspace as follows: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[36]

B. *Critical Infrastructure*

The term critical infrastructure is defined with more or less uniformity in a variety of documents and laws. Critical infrastructure refers to all the services provided that are associated with sustaining modern society, all of which have unique physical and cyber components. For instance, in the 2003 National Strategy for the

35. ERIC A. FISHER, CONG. RESEARCH SERV., R43831, CYBERSECURITY ISSUES AND CHALLENGES: IN BRIEF 1 n.2 (2016) [hereinafter FISHER, CYBERSECURITY ISSUES].

36. JOINT CHIEFS OF STAFF, JOINT PUB. 1–02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 58 (Nov. 2010) (as amended through Feb. 2016).

Physical Protection of Critical Infrastructure and Key Assets, the Department of Homeland Security ("DHS") provides a detailed list of assets of national importance—i.e., critical infrastructure. This list includes: IT; telecommunications; chemicals; transportation; emergency services; postal and shipping services; agriculture and food; public health and healthcare; drinking water/water treatment; energy; banking and finance; national monuments and icons; defense industrial base; key industry/technology sites; and large gathering sites.[37] In a 2007 publication by the DHS, the agency's list identifies five general types of critical infrastructure: (1) production industries: energy, chemical, defense industrial base; (2) service industries: banking and finance, transportation, postal and shipping; (3) sustenance and health: agriculture, food, water, public health; (4) federal and state: government, emergency services; and (5) IT and cyber: information, telecommunications.[38]

Section 5159(b)(2) of the Critical Infrastructures Protection Act ("CIPA") identifies critical infrastructures as "telecommunications, energy, financial services, water, and transportation sectors."[39] In addition, CIPA specifically recognizes the importance of critical infrastructure to society by adding that the term means all "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[40]

Reflecting America's founding roots in capitalism and the free market economy, private businesses own and operate approximately 85 percent of the nation's critical infrastructure.[41] Accordingly, the responsibility for maintaining physical and cyber security at these facilities primarily rests on private shoulders—not on the federal government. The conundrum for the government,

37. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS 35 (2003).

38. *See* HOMELAND SEC. COUNCIL, NATIONAL STRATEGY FOR HOMELAND SECURITY (2007).

39. Critical Infrastructures Protection Act (CIPA) of 2001, 42 U.S.C. § 5195c(b)(2) (2012).

40. 42 U.S.C. § 5195c(e).

41. Douglas C. Michael, *Self-Regulation for Safety and Security: Final Minutes or Finest Hour?*, 36 SETON HALL L. REV. 1075, 1128 n.268 (2006).

of course, is that it is charged with protecting the American people, not private industry.

C. *SCADA*

In the modern world, all critical infrastructures are operated by means of an electronic control system. This system regulates the thousands of interconnected computers, servers, routers, and switches associated with the myriad physical and virtual tasks inherent in operating and maintaining the functions of a given industry. In the day of Connie Francis, many of these tasks were predominately handled by people; but today, they are electronically monitored and controlled by centralized computer networks called SCADA systems, industrial control systems ("ICS"), distributed control systems ("DCS"), programmable logic control systems ("PLCS"),[42] or any functionally equivalent system. Since SCADA is the general and most common term to describe the electronic "nervous system" of these critical infrastructures, it is the term that will be used here.[43]

SCADA systems, and other equivalent systems, digitize and automate almost every imaginable task associated with a given critical infrastructure—from opening and closing valves in nuclear facilities, to operating circuit breakers on electrical power grids, to managing air traffic in the sky. In other words, SCADA systems provide the brain power to manage a critical infrastructure. Clearly, as will be discussed later, this makes the critical infrastructure extremely vulnerable to cyber attacks, which could cause massive economic and physical damage across broad sections of the country.[44]

42. *See* Robert K. Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor"*, 18 VA. J.L. & TECH. 289, 300 (2014) (defining industrial control systems); *Industrial Automation Market—Global Industry Analysis, Size, Share, Growth, Trends, and Forecast 2016-2024*, PR NEWSWIRE (Jan. 12, 2017), http://www.prnewswire.com/news-releases/industrial-automation-market---global-industry-analysis-size-share-growth-trends-and-forecast-2016---2024-300390335.html (defining SCADA, DCS, and PLCS).

43. *See* Palmer, *supra* note 42, at 302.

44. *See, e.g.*, Hillary Hellmann, Comment, *Acknowledging the Threat: Securing United States Pipeline SCADA Systems*, 36 ENERGY L.J. 157, 158, 163 (2015) (discussing how United States oil and gas pipeline SCADA systems are threatened by large-scale cyber attacks).

Since the vast majority of critical infrastructures rest in the hands of private industry, where the predominate emphasis for the owners is on maintaining system reliability and efficiency, putting large sums of money into increased cybersecurity is often of less importance to the federal government.[45] Incredibly, many SCADAs are connected to their own private corporate networks, which are in turn primarily connected directly or indirectly to the Internet. To those familiar with the process, this is a recipe for disaster. The resulting vulnerability presents an open door for an actor with the necessary skills to hack into a SCADA and, for example, disable the valves at a nuclear facility, shut down an entire electrical power grid, or redirect air traffic to harmful flight patterns.

D. *Cyber Attacks*

Not all disruptions of an information system's confidentiality, integrity, or availability ("CIA") constitute a cyber attack. The majority of SCADA disruptions are caused by unintentional human error or normal wear and tear, and are best described as cyber incidents.[46] On the other hand, the term cyber attack is most certainly the correct phrase to describe the intentional disruption of a SCADA's CIA.

All intentional attacks on a computer or its network involve actions that are meant to disrupt, destroy, or deny information. These unauthorized cyber intrusions or attacks may be performed by state actors or non-state actors seeking notoriety, monetary gain, political advantage, or even hope to engage in vandalism, terrorism, or acts of war. Thus, it is not only the matter of cyber crime, which costs billions of dollars a year to the economy, but also the fear of cyber attacks as a method of warfare.[47] In fact,

45. *See* Michael, *supra* note 41, at 1128.

46. The National Institute of Standards and Technology defines incident as: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." NAT'L INST. STANDARDS & TECH., U.S. DEPT. COM., FIPS PUB 200, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS 7 (2006). Such incidents may be intentional or unintentional. *See id.*

47. *See* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57,

planting harmful software in electronic systems to "obliterate, alter, or appropriate data has become a crucial new tactic of warfare,"[48] clearly apart from the traditional notions of fighting by land, sea, or air. But the real fear, regardless of the source of the attack, is that a cyber-strike against the nation will hit and cripple a critical infrastructure.

While most cyber breaches have involved hacks into various companies and led to the release of customer PII, the overriding concern that energizes any discussion of cybersecurity is the fear that a significant cyber attack will target one or more of the nation's critical infrastructures and cause massive physical harm. Although the cyber attack equivalent of Pearl Harbor has yet to occur against one of the nation's critical infrastructures, significant SCADA cyber attacks have already occurred and continue to occur. Two examples below are illustrative: one involves an "insider" conducting a cyber attack on a SCADA, and the other involves an "outsider" doing the same.

In *R v Boden*,[49] the Supreme Court of Queensland, Australia, upheld twenty of the twenty-six convictions against a disgruntled employee by the name of Vitek Boden. Boden hacked into the SCADA of an Australian sewage and water treatment plant and directed the pumping of 800,000 liters of sewage into the environment, causing millions of dollars in damage. He was apprehended during a routine traffic stop in Queensland where he was found in possession of a stolen computer and radio transmitter, which he had used to turn his vehicle into a mobile "command center."[50] Over the course of two months in 2000, and on forty-six separate occasions, Boden directed the SCADA to pump massive amounts of raw sewage into the local environment.

So-called insider threats are often done by disgruntled employees, like Boden, and are extremely serious. Remaining undetect-

74–77 (2010).

48. Claire O. Finkelstein & Kevin H. Govern, *Introduction: Cyber and the Changing Face of War*, at xiv (Univ. of Pa. Law Sch., Pub. Law and Legal Theory Research Paper Series, Research Paper No. 15-20, 2015), http://ssrn.com/abstract=2598671.

49. R v. Boden [2002] QCA 164 (Austl.); Marshall Abrams & Joe Weiss, *Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia*, MITRE (2008), https://www.mitre.org/sites/default/files/pdf/08_1145.pdf.

50. Barton Gellman, *Cyber-Attacks by Al Qaeda Feared*, WASH. POST (June 27, 2002), https://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006AR2006061200711_pf.html.

ed, the insider can do a variety of harm such as altering encryption and communication applications in order to copy input and output data from the control terminals to various hidden sections on the system.[51]

In *United States v. Mitra*, the United States District Court for the Western District of Wisconsin convicted an "outsider" who was able to singlehandedly breach the sophisticated cyber command and control system of a critical infrastructure, not just once, but on two separate occasions.[52] The defendant Rajib Mitra was convicted of two counts of intentional interference with computer-related systems used in interstate commerce, in violation of 18 U.S.C. § 1030(a)(5).[53] In 2003, while a student at the University of Wisconsin's graduate business school, Mitra successfully hacked into and shut down the computer-based radio system Smartnet II (made by Motorola) for police, fire, ambulance, and other emergency communications in the entire city of Madison, Wisconsin. On Halloween night of 2003, Mitra struck the State capital:

> [A] powerful signal had blanketed all of the City's communications towers and prevented the computer from receiving, on the control channel, data essential to parcel traffic among the other 19 channels. Madison was hosting between 50,000 and 100,000 visitors that day. When disturbances erupted, public safety departments were unable to coordinate their activities because the radio system was down. Although the City repeatedly switched the control channel for the Smartnet system, a step that temporarily restored service, the interfering signal changed channels too and again blocked the system's use.[54]

On November 11, 2003, Mitra changed tactics. Instead of blocking signals, he sent signals that directed the newly replaced "Smartnet base station to keep channels open, and at the end of each communication the attacker appended a sound, such as a woman's sexual moan."[55]

51. Jeffrey F. Addicott, *The Emerging Threat of Cyberterrorism*, *in* 22 UNDERSTANDING TERRORISM: ANALYSIS OF SOCIOLOGICAL AND PSYCHOLOGICAL ASPECTS 259, 262 (Suleyman Ozeren et al. eds., 2007) [hereinafter Addicott, *Emerging Threat*].

52. 405 F.3d 493, 493 (7th Cir. 2005).

53. *Id.*

54. *Id.*

55. *Id.*

Finally, perhaps the most well-reported attack on a SCADA occurred in April 2007 when coordinated cyber-attacks disrupted large portions of the banking and communication systems of the Baltic country of Estonia for almost a month.[56] The denial of service ("DoDS")[57] attack was probably the work of Russian hackers in response to the removal of a bronze statue of a World War II era Soviet soldier from a park in Estonia. When one considers that terrorist organizations such as al Qaeda and ISIS[58] have been using computers, e-mail, and encryption to support and finance their organizations for years, it is only logical to conclude that they are also fully aware that cyber attacks offer a low cost method of inflicting major damage to the West.[59]

Ironically, it was the west, not the Russians or Chinese, that actually engaged in the first significant cyber attack in the context of directly causing massive physical damage to a critical infrastructure. In June 2012, the *New York Times* reported that the United States and Israel had sent a massive virus that infected the SCADA of the Iranian nuclear reactor at Natanz.[60] The so-called Stuxnet virus caused major damage and was acknowledged by former Central Intelligence Agency Director Michael Hayden as "the first attack of a major nature in which a cyber attack was used to effect physical destruction."[61]

Although the cyber attack against Iran was significant, the United States endures the highest levels of continued and concentrated cyber attacks from not just terrorists or non-state actors,

56. *See* Scheherazade Rehman, *Estonia's Lessons in Cyberwarfare*, U.S. NEWS & WORLD REP. (Jan. 14, 2013), http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare; Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN (May 16, 2007), https://www.theguardian.com/world/2007/may/17/topstories3.russia. The Estonian cyber attack resulted in a digital infrastructure disaster as websites for government officials, government agencies, daily newspapers, and Estonia's biggest banks were overwhelmed and shut down due to the cyber onslaught of "unknown" digital information attacks. *Id*.

57. *See infra* note 66 and accompanying chart.

58. JAMES SCOTT & DREW SPANIEL, THE ANATOMY OF CYBER JIHAD: CYBERSPACE IS THE NEW GREAT EQUALIZER 5–11, 40 (2016).

59. *See* JEFFREY F. ADDICOTT, RADIAL ISLAM WHY?: CONFRONTING JIHAD AT HOME & ABROAD 12–13 (2016) [hereinafter ADDICOTT, RADICAL ISLAM].

60. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 [hereinafter Sanger, *Obama Order*].

61. DAVID E. SANGER, CONFRONT AND CONCEAL 200 (2012) [hereinafter SANGER, CONFRONT AND CONCEAL].

but a variety of actors such as China, North Korea, and Russia. In 2013, the Chairman of the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, Congressman Jim Sensenbrenner (R-WI) testified at a formal hearing that the "United States has been the subject of the most coordinated and sustained computer attacks the world has ever seen."[62] Federal Bureau of Investigations Director James Comey told Congress in early 2016 that the nation "continue[s] to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by United States victims."[63]

In a study issued by the Center for Strategic and International Studies ("CSIS"), the annual cost of cyber attacks on the world's private sector and its consumers is over $445 billion dollars, and perhaps as high as $575 billion.[64] The report went on to find that, in the United States alone, an estimated 200,000 jobs were simply not created in the civilian economy due to the billions of dollars in losses.[65]

So what are the techniques employed in a cyber attack? A June 2007 Government Accountability Office ("GAO") Report, produced a layman's chart that lists the most common techniques employed

62. *Investigating and Prosecuting 21st Century Cyber Threats: Hearing Before the Subcomm. On Crime, Terrorism, Homeland Security and Investigations of the H. Comm. On the Judiciary*, 113th Cong. 1 (2013) (statement of Rep. Sensenbrenner, Chairman, Subcomm. on Crime, Terrorism, Homeland Security, and Investigations).

63. *FBI Budget Request for Fiscal Year 2017 Before the H. Appropriations Comm, Subcomm. On Commerce, Justice, Sci., and Related Agencies* (Feb. 25, 2016) (statement by James B. Comey), https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2017.

64. Tom Risen, Study: *Hackers Cost More Than $445 Billion Annually*, U.S. NEWS & WORLD REP. (Jan 9, 2014), http://www.usnews.com/news/articles/2014/06/09/study-hackers-cost-more-than-445-billion-annually.

65. *Id*.

by hackers, each with a brief description.[66] The Report presented

66. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-705, CYBERCRIME: PUBLIC AND PRIVATE ENTITIES FACE CHALLENGES IN ADDRESSING CYBER THREATS (2007).

Type	**Description**
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial data from the sea of Internet users.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate website. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed website when the user types in a legitimate Web address. For example, one pharming technique is to redirect users—without their knowledge—to a different website from the one they intended to access. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent website when the user types in a legitimate address.
Denial-of-service Attack	An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. Denial-of-service attacks compromise the availability of the resource.
Distributed denial-of-service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Viruses	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.
Trojan horse	A computer program that conceals harmful code. It usually masquerades as a useful program that a user would wish to execute.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

four general types of cyber attacks. The first and most common cyber attack involves a service disruption or the distributed denial of service ("DDoS"), which aims to flood the target computer with data packets or connection requests, thereby making it unavailable to the user or, in the case of a website, unavailable to the website's visitors. A second, but related, type of cyber attack is designed to capture and then control certain elements of cyberspace in order to use them as actual weapons. The third category is aimed at theft of assets from, for example, financial institutions. Finally, an attack can also manifest itself by means of a conventional explosive event on a physical structure, such as a physical building that houses a SCADA.[67]

III. CYBERSECURITY

"*It's going to happen again [massive cyber-attack].*"[68]

—Martin McKeny

A. *Defining Cybersecurity*

There is no commonly accepted definition for the term cybersecurity. Different uses of the term can be found in a wide variety of federal laws, executive orders, presidential directives, and other agency directives. Taken together, cybersecurity means protecting the basic security of computerized systems from unauthorized access.

Malware	Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as useful programs or is embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

67. *See* ADDICOTT, TERRORISM LAW, *supra* note 32, at 321–23.

68. *See* Drew Fitzgerald, *National Intelligence Director Says Data Suggests 'Nonstate Actor' Was Behind Cyberattack*, WALL ST. J., Oct. 25, 2016, at A2. Mr. McKeny is a cybersecurity analyst for Akamai Technologies, Inc. *Id.*

While there are many competing definitions regarding cybersecurity, a 2005 Congressional Research Service Report entitled: *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*,[69] presents an efficacious starting point.

> A set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace. The activities can include security audits, patch management, authentication procedures, access management, and so forth. They can involve, for example, examining and evaluating the strengths and vulnerabilities of the hardware and software used in the country's political and economic electronic infrastructure. They also involve detection and reaction to security events, mitigation of impacts, and recovery of affected components. Other measures can include such things as hardware and software firewalls, physical security such as hardened facilitates, and personnel training and responsibilities.[70]

As previously stated, cybersecurity breaches originate from a variety of sources to include hostile nations, criminals, competitors, disgruntled employees,[71] terrorists, "script-kiddies,"[72] and just human error.[73] Further, breaches occur in the government and private sectors alike. For instance, in 2015 the Office of Personnel Management suffered cybersecurity attacks that resulted in the disclosure of PII of over 4.2 million current and former government employees, with another 21.5 million background inves-

69. ERIC A. FISCHER, CONG. RESEARCH SERV., RL32777, CREATING A NATIONAL FRAMEWORK FOR CYBERSECURITY: AN ANALYSIS OF ISSUES AND OPTIONS 5–6 (2005) [hereinafter FISCHER, NATIONAL FRAMEWORK], https: //www.fas.org/sgp/crs/natsec/RL32777.pdf.

70. *Id.*

71. *See, e.g.*, Damian Paletta, *Ex-NSA Contractor Stole at Least 500 Million Pages of Records and Secrets, U.S. Says*, WALL ST. J., Oct. 20, 2016, at A3 (discussing a contractor suspected of theft from the National Security Agency that contributed to the development of highly sensitive cybertools and cyberweapons used by the American government).

72. *See supra* note 51 and accompanying text; s*ee also* Rupert Cocke, *Online Banks Are Often Easy Prey For Hackers, Security Experts Say*, WALL ST. J. (June 17, 2002), http:// www.wsj.com/articles/SB1024259787474741600 (discussing the definition of a "script-kiddie").

73. *See, e.g.*, Alexander Boyko et al., *Investigating the Sayano-Shushenskaya Hydro Power Plant Disaster*, POWER MAG. (Dec. 1, 2010), http://www.powermag.com/investigating-the-sayano-shushenskaya-hydro-power-plant-disaster/. In 2009, the Sayano-Shushenskaya Russian hydroelectric power plant was shut down for maintenance. A computer technician at a separate location who was unaware of the cause for the shutdown used his computer to send an electronic signal to turn the main turbine back on. As a result of this human error, seventy-five people were killed and the facility suffered a billion dollars worth of damage. *Id.*

tigative records released.[74] In the June 2016 issue of *Time*, a story discussed how the hackers were able to penetrate the international banking system run by "a vast and powerful consortium called SWIFT, the Society for Worldwide Interbank Financial Telecommunication."[75] Hackers infiltrated Bangladesh's central banking system and sent numerous forged SWIFT messages out to other banks, requesting the electronic transfer of "roughly $1 billion to accounts in Asia."[76]

B. *Leaning Forward in the Saddle*

One of the byproducts of the September 11 terrorist attacks ("9/11") is the realization that if significant parts of the physical world could be destroyed by dedicated fanatics, *a fortiori*, our cyber world, which regulates all aspects of the critical infrastructure, might well be next. As evidenced by the ever-rising number of cyber attacks, it is certain that the level of cybersecurity protection is less than satisfactory, both in the government and the private sector. America's critical infrastructure is extremely vulnerable and ripe for a massive cyber attack. Ultimately, the real issue is not necessarily the nature or motivation of the perpetrator, it is one of cybersecurity.[77] Regardless of the entity engaged in the cyber attack, the real question is this: Does a sufficient cybersecurity framework exist that can adequately protect cyberspace and the information it contains, processes, and transmits?

Despite the seriousness of cyber attacks, the truth is many experts agree the United States does not have a sufficient cybersecurity posture to protect cyberspace, or more importantly, the

74. *Cybersecurity Resource Center*, OFFICE OF PERSONNEL MGMT., https://www.opm.gov/cybersecurity/ (last visited Feb. 13, 2017).

75. Haley Sweetland Edwards, *A New Generation of Bank Robbers Infiltrates Global Finance*, TIME, June 13, 2016, at 9.

76. *Id.*

77. *See* Statements & Releases, Office of the Press Sec'y, *FACT SHEET: White House Summit on Cybersecurity and Consumer Protection*, WHITE HOUSE (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection. Under 6 U.S.C. § 1501(5)(A) (2012 & Supp. III 2016), a "cybersecurity threat" is defined as follows:

> [A]n action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

SCADA that operates and maintains our critical infrastructure. Private industry is only partially regulated through the actions of a handful of legislative and administrative requirements; and yet, the primary responsibility for physical security and cybersecurity rests in their hands.

IV. GOVERNMENT'S RESPONSE TO SECURE CYBERSPACE

"*There are risks and costs to a program of action. But they are far less than the long-range risks and costs of comfortable inaction.*"[78]

—John F. Kennedy

In May 2009, President Obama released a Cyberspace Policy Review which contained a harsh analysis of the federal government's preparedness:

> The Federal government is not organized to address this growing problem [cyber attacks] effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way.[79]

This assessment remains accurate today in 2017. Despite the streamlining benefits associated with the recently enacted Cybersecurity Information Sharing Act ("CISA"), the overall governmental framework for dealing with cybersecurity issues is clearly more hands-off than hands-on. Accordingly, there exists a hodgepodge of over fifty federal statutes and numerous executive directives and orders, all of which reflect a rather disjointed strategy to prod the private sector forward.[80] For instance, Congress passed four cybersecurity bills in 2014 which sought to update certain areas of the law to reflect current and emerging issues related to cybersecurity.[81] The bills were the National Cybersecurity

78. *The John F. Kennedy University Story*, JOHN F. KENNEDY UNIV. (2017), http://www.jfku.edu/About-Us/The-JFK-University-Story.html.

79. *See* NAT'L SEC. COUNCIL & HOMELAND SEC. COUNCIL, CYBERSPACE POLICY REVIEW, ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE i (2009).

80. ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS (2013).

81. *See* Covington & Burlington LLP, *Congress Passes Four Cybersecurity Bills*, NAT. L. REV. (Dec. 13, 2014), http://www.natlawreview.com/article/congress-passes-four-cyber

Protection Act ("NCPA") of 2014,[82] Federal Information Security Modernization Act ("FISMA") of 2014,[83] Cybersecurity Enhancement Act ("CEA") of 2014,[84] and Cybersecurity Workforce Assessment Act ("CWAA") of 2014.[85] Of the four bills, the NCPA was the most important for the private sector. The NCPA codified provisions in the National Cybersecurity and Communications Integration Center and energized the DHS with a renewed authority to partner with the private sector.[86] The NCPA also created a federal agency data breach notification law that requires federal agencies to quickly notify individuals who are affected by a data breach, as well as certain Congressional committees.[87]

A. *Engagement Strategy*

Starting with the Clinton administration and continuing to the Trump administration, the government's approach to cybersecurity for owners and operators of private computer systems has been one of cooperative *engagement*, not mandatory government regulation, to encourage the implementation of greater levels of cybersecurity.[88] Just as the government cannot dictate the technology that private industry must develop in the marketplace, it cannot force private industry to adopt cybersecurity standards.

The government's reluctance to regulate is most certainly driven by many practical considerations. For instance, the government could never mandate a particular level of cybersecurity for the private sector for two primary reasons. First, by the time a particular government bureaucracy could agree on developing fixed standards for a given system, that effort would be rendered obsolete by new advances in the technology. Second, it is equally clear that government employees simply would not possess the technical abilities to even develop standards—the skills required to do so would draw such individuals into the far more rewarding

security-bills.

82. 6 U.S.C. §§ 148–50 (2014 & Supp. III 2015).

83. 44 U.S.C. §§ 3551–76 (2012 & Supp. II 2014).

84. 15 U.S.C § 7421 (2012 & Supp. III 2015).

85. 6 U.S.C. § 146 (2012 & Supp. III 2015).

86. *See id.* §§ 148–50.

87. *Id.*

88. *See* Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*, 15 GEO. J. INT'L AFF. 69, 69 (2014).

business world. Thus, despite the rapidly expanding reliance on cyber technology by American businesses and consumers, the government provides extremely little affirmative regulatory activity in terms of cybersecurity functions for non-government cyber systems.

The government's concept of engagement stresses the promotion of voluntary public-private alliances to better secure cyberspace. This theme of engagement predominates all of the federal laws, executive orders, and presidential directives associated with cyberspace. Although almost ten years old, a 2007 report issued by the GAO is still relevant in its observation that government and private sectors face a number of serious obstacles in promoting cybersecurity, particularly in the context of an information sharing environment between the government and the private sector.[89] The most recent cybersecurity law enacted by Congress was CISA, introduced on March 17, 2015 by Senator Richard Burr (R-NC).[90] CISA is another in a long line of efforts to encourage cooperative information-sharing initiatives between private businesses and the government. The primary purpose of CISA is "to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes."[91] The major points include: (1) sharing cybersecurity information between private entities and the federal government; (2) sharing unclassified cyber threat information with the general public; and (3) having the federal government share information regarding a cybersecurity threat that may affect said entity to prevent or mitigate damages.[92] Of particular significance, the bill explicitly states that nothing in the act forces a private entity to share information with the federal government

89. The four main categories of concern in the GAO Report focused on cyber crime, but would also be equally pertinent in regards to any type of cyber-attack: (1) accurately reporting cyber crime to law enforcement; (2) "ensuring adequate law enforcement analytical and technical capabilities[:] . . . obtaining and retaining investigators, prosecutors, and [cyber forensics] examiners" and keeping up to date with current technology and criminal techniques"; (3) "working in a borderless environment with laws of multiple jurisdictions'"; and (4) protecting information and information systems and raising awareness about criminal behavior. *Id*.

90. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (1st Sess. 2015); S. REP. NO. 114-32, at 1, 16 (2015).

91. S. 754, 114th Cong. (1st Sess. 2015).

92. *Id.*

and there are no penalties for noncompliance.[93] On the contrary, CISA shields an entity from legal liability for sharing information in accordance with CISA.[94] The bill also recognizes the right of a private entity to operate defensive measures to detect, prevent, or mitigate cybersecurity threats.[95]

In June 2016, DHS and the Department of Justice issued guidance related to CISA of 2015.[96] Complete with charts, the guidance document is meant to assist non-federal entities in how to share cyber threat indicators and other defensive measures with federal entities. The guidance document was written in response to requests from the private sector to assist in navigating the terms and definitions set out in CISA, as well as to explain more clearly the legal protections afforded.

Critics of the government's engagement strategy argue that a meaningful, cooperative, proactive, and reactive strategy between the government and private industry is piecemeal. Even the more immediate negative consequences to businesses caused by the impact of cyber crime, which drains billions of dollars from consumers and private industry each year, have not provided the necessary incentive to produce stronger and more secure computer networks. The basic reason for the lack of cooperation from privately owned companies is understandable given the perennial distrust of government coupled with the lack of desire for privately owned companies to share information about security breaches. First, private companies are concerned competitors might gain access to exclusive company data that is shared with the government through a public Freedom of Information Act (regardless of assurances in CISA) request, or by means of other sources.[97] Second, because the private sector operates in a competitive market-based economy, public revelations regarding cybersecurity

93. *Id.*

94. *Id.*

95. *Id.*

96. *See* DEP'T OF HOMELAND SEC. & DEP'T OF JUSTICE, 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 (2016).

97. *See* Jeremy J. Broggi, *Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes*, 37 HARV. J.L. & PUB. POL'Y 653, 657 (2014) (discussing how programs aid cybersecurity work); Emily Frye, *The Tragedy of the Cybercommons: Overcoming Fundamental Vulnerabilities to Critical Infrastructures in a Networked World*, 58 BUS. LAW 349, 375 (2002).

breaches could have serious negative responses from both stockholders and consumers. For instance, if a bank acknowledges a cyber breach that affects private account holders, the fear is that those customers will withdraw their funds from the bank and place them elsewhere. Under this light, in September 2016, the tech giant Yahoo was reluctant to reveal that "information had been stolen [via cyber attacks] on 500 million customer accounts."[98]

Unfortunately, it is a hard fact that very few private companies have exhibited interest in exerting the cybersecurity efforts to the degree that the government's engagement policy so strongly desires. The frustration is that, without a cooperative effort to identify breaches and the possible weak points of cybersecurity systems, the vulnerabilities to cyber attack are magnified and countermeasures remain far behind. For the time being, the government offers few driving incentives, such as the often overlooked Support Anti-Terrorism by Fostering Effective Technologies Act (the "SAFETY Act"),[99] to the private industry to work together to better secure their cyber networks.

B. *Federal Regulation and Private Business*

In contrast to the lack of regulation in the private sector, government computers are directly subject to strict cybersecurity standards set out in specific federal legislation mandating cyber protective measures, such as the requirements found in the Fed-

98. Elizabeth Weise & Mike Snider, *Yahoo's Massive, Hidden Email Search Would Be First of its Kind, If True,* USA TODAY (Oct. 4, 2016), http://www.usatoday.com/story/tech/news/2016/10/04/yahoo-searched-customer-emails-nsa-report-fbi-reuters/91548012/.

99. *See* 6 U.S.C. §§ 101, 441–44 (2012). The SAFETY Act provides a legal liability shield to designated anti-terrorism technologies thereby encouraging the adoption of innovative technologies. *Id.* § 441. Under the terms of the SAFETY Act, "sellers" of a technology that would "be effective in facilitating the defense against acts of terrorism, including technologies that prevent defeat or respond to such acts" can petition the Secretary of Homeland Security to designate such as a Qualified Anti-Terrorism Technology (QATT). *Id.* Specifically, the sellers of "any product, equipment, service, device, or technology designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism" can apply for government certification from DHS. *Id.* § 444. A cybersecurity technology that falls under the provisions of the act is certified as a QATT, which means that any liability actions regarding the use of the QATT must be brought in a federal court. *Id.* § 442. The SAFETY Act also restricts the legal claim to actual damages, removing punitive or exemplary damages from the claim. *Id.*

eral Information Security Management Act of 2002.[100] The term standards is defined by the National Standards Policy Advisory Committee as follows:

> [Standards are] a prescribed set of rules, conditions, or requirements concerning definitions of terms; classification of components; specification of materials, performance, or operations; delineation of procedures; or measurement of quantity and quality in describing materials, products, systems, services, or practices.[101]

While the government's demand for certain standards in its own computers has spilled over to the private sector, it is certainly the exception and not the rule. Exceptions to the government's hands-off approach to regulating cyberspace are scattered throughout various legislative initiatives aimed primarily at protecting PII. But apart from a few specific laws protecting PII for financial and health-related activities from disclosure, government efforts to set cybersecurity standards or make private entities responsible for protecting their own computer systems are rare. Examples of regulatory efforts include the following: the Health Insurance Portability and Accountability Act of 1996 requires certain private entities to establish cybersecurity programs that protect health-related information in their possession;[102] the Sarbanes-Oxley Act of 2002[103] and the Gramm-Leach-Bliley Act of 1999[104] require corporate executives of publicly held companies to annually certify the integrity of their financial reporting under penalty of fines or imprisonment;[105] the Children's Online Privacy

100. The Federal Information Security Act of 2002, 44 U.S.C. § 3541 (2002). This act was later updated in 2014 to become FISMA.

101. MAUREEN A. BREITENBERG, U.S. DEP'T COMMERCE, THE ABC'S OF STANDARDS-RELATED ACTIVITIES IN THE UNITED STATES 1 (1987), http://gsi.nist.gov/global/docs/NBSIR%2087-3576.pdf (citing Nat'l Standards Policy Advisory Committee, National Policy on Standards in for the United States and a Recommended Implementation Plan 6 (1978)). As suggested by its current engagement strategy, the federal government only promulgates cybersecurity standards for federal computer systems, except national security systems. The federal standards are developed by the National Institute of Standards and Technology and set out as Federal Information Processing Standards ("FIPS"). FIPS are promulgated under the simple rule-making procedures (notice and comment) of the Administrative Procedure Act. Standards regarding national security systems are developed and controlled by the Committee on National Security Systems.

102. 42 U.S.C. §§ 201, 1320d-2 (2012).

103. 15 U.S.C. § 7201 (2012).

104. 12 U.S.C. § 1811 (2012).

105. *See* Lawrence A. Gordon et. al., *Increasing Cybersecurity Investments In Private Sector Firms*, 1 J. CYBER SECURITY 3, 12 (2015); *see also* 18 U.S.C. § 1350 (2012). The Sarbanes-Oxley Act was passed in the wake of the accounting scandals at Enron and WorldCom and helped spur a significant increase in cybersecurity.

Protection Act of 1998[106] requires protection of PII regarding children; and the Securities and Exchange Commission ("SEC") imposes regulations regarding cybersecurity standards for internal financial controls.[107]

The Federal Trade Commission ("FTC") is another entity that seeks to push private industry to higher levels of cybersecurity through enforcement actions. Under section 5 of the FTC Act, the agency possesses a series of enforcement actions and consent decrees which extend cybersecurity obligations to certain private industries by holding them responsible for privacy and security promises they make to their customers.[108] Originally, the FTC facilitated cases based on the alleged failure by companies to provide adequate information security in compliance with representations they made to customers (i.e., deceptive trade practices claims). In recent years, the FTC has significantly broadened the scope of its enforcement authority by asserting that a failure to provide appropriate information security was, itself, an unfair trade practice—even in the absence of any false representations by the defendant as to the adequacy of its security.[109] For instance, in *FTC v. Wyndham Worldwide Corporation*, the federal district court found that the FTC did possess the power to assert unfair and deceptive trade practice claims against Wyndham for causing substantial consumer injury by unreasonably and unnecessarily failing to notify customers or take corrective measures to halt cyber hacks on customer's PII.[110]

A variety of federal and state E-transaction laws, such as the Electronic Signatures in Global and National Commerce Act ("E-SIGN") and the Uniform Electronic Transmissions Act ("UETA"), now require all companies to provide cybersecurity for the storage of electronic records relating to online transactions.[111] In addition, sector-specific regulations are experiencing proliferation. This in-

106. 15 U.S.C. § 6502 (2012).

107. *See* 79 Fed. Reg. 72252 (Dec. 5, 2014) (codified at 17 C.F.R. §§ 240, 242, 249 (2016)).

108. *See* 15 U.S.C. § 45 (2012).

109. 16 C.F.R. § 682.3 (2016); *see, e.g.*, Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 777–78 (W.D. Mich. 2006) (complaint alleging shoe retailer failed to provide reasonable and appropriate security for its customers PII).

110. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

111. *See* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001 (2012); UNIF. ELEC. TRANSMISSIONS ACT (UNIF. LAW COMM'N 1999) (enacted in all states, except Illinois, New York, and Washington).

cludes the Internal Revenue Service's requirement for companies to implement information cybersecurity to protect electronic tax records[112] and SEC regulations requiring cybersecurity as a condition to engage in certain E-transactions.[113] The Food and Drug Administration also has regulations requiring improved cybersecurity for certain types of records.[114]

In examining the government's attempt to enforce greater cyber standards on the private sector, it is important to note that the federal government is significantly involved in prosecuting cyber breaches when they do occur. While numerous federal statutes address cybercrimes,[115] the primary and most comprehensive statute is the Computer Fraud and Abuse Act ("CFAA") passed in 1986.[116] The CFAA has been amended many times to include various new provisions found in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "USA PATRIOT Act").[117] In short, the CFAA makes it a federal crime to gain unauthorized access to, damage, or use certain "protected" computers and computer systems illegally.[118] The term "protected" sounds limited but is actually construed quite broadly and applies to practically every computer in the world, including those computer systems used by the nation's financial institutions, by federal government entities, or in interstate and foreign commerce.[119] As one commentator succinctly put it, it is enough if the computer is "connected to the Internet."[120] The only exemptions pertain to law enforcement and intelligence agencies when performing their official duties.[121] Cu-

112. 26 C.F.R. § 1.1441-1(e)(4)(iv)(B) (2016).

113. *See* 17 C.F.R. § 240.13n-6 (2016).

114. *See* 21 C.F.R. § 20.63 (2016).

115. Some federal statutes address such things as: illegal wire fraud, 18 U.S.C. § 1343 (2012); aggravated identity theft, 18 U.S.C. § 1028A (2012); fraud in connection with identification documents, and authentication features and information, 18 U.S.C. § 1028 (2012); intentional interference with computer-related systems used in interstate commerce, 18 U.S.C. § 1030(a)(5) (2012); deceptive practices affecting commerce, 15 U.S.C. § 45(a)(1) (2012); and installing "sniffer" software to record keystroke and computer traffic, 18 U.S.C. § 2511 (2012).

116. 18 U.S.C. § 1030 (2012).

117. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

118. 18 U.S.C. § 1030(a)(2)(C).

119. 18 U.S.C. § 1030(e)(2).

120. CHARLES DOYLE, CONG. RESEARCH SERV., R 97-105, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 61 n.330 (2014).

121. 18 U.S.C. § 1030(f).

riously, military personnel are not exempted—neither from the criminal penalties of the CFAA nor from any subsequent civil action against them personally.[122]

In terms of motivating the private sector to improve cybersecurity, CFAA does provide some interesting statutory provisions. In addition to addressing acts of trafficking in passwords, espionage, fraud, and damage caused by viruses, worms, or other devices,[123] the CFAA sets out criminal penalties ranging from imprisonment for not more than a year for simple violations, to life imprisonment for intentional acts resulting in death. Furthermore, the CFAA creates a separate civil cause of action for any person who suffers loss or damage due to a violation. Victims can file suit against "any individual, firm, corporation, educational institution, governmental entity, or legal or other entity."[124] Section 1030(g) states:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves one of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.[125]

122. *See* Molly Picard, Comment, *Cyberspace: The 21st Century Battlefield Exposing Soldiers, Sailors, Airmen, and Marines to Potential Civil Liabilities*, 4 NAT'L SECURITY L.J. 125, 129 (2015).

123. *See* 18 U.S.C. § 1030(a). The seven areas of interest in 18 U.S.C. § 1030(a) include: computer trespassing, e.g., hacking, associated with a government computer, § 1030(a)(3); computer trespassing resulting in exposure to certain governmental, credit, financial, or commercial information, § 1030(a)(2); damaging either a government computer, a bank computer, or a computer that is used in interstate or foreign commerce, § 1030(a)(5); committing fraud where an integral part involves unauthorized access to a government computer, a bank computer, or a computer used in interstate or foreign commerce, § 1030(a)(4); threatening to damage a government computer, a bank computer, or a computer used in interstate or foreign commerce, § 1030(a)(7); trafficking in passwords used for a government computer, a bank computer, or a computer used in interstate or foreign commerce, § 1030(a)(6); and accessing a computer to commit espionage, § 1030(a)(1).

124. DOYLE, *supra* note 120, at 24.

125. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2012).

C. *State Efforts to Enhance Cybersecurity*

Individual states have also enacted laws associated with cybersecurity concerns. These laws address a wide range of issues, including cutting off public access to open government records, improving security measures for wireless networks, criminalizing the installation of software on another's computer which is then used in deceptive methods, requiring businesses to report loss of PII, and even requiring certain businesses to develop reasonable cybersecurity to protect PII.[126] Without question, the item of greatest interest is the requirement that certain businesses implement reasonable cybersecurity standards to protect PII.[127] Such state laws are generally known as security breach laws. In 2003, California enacted the California Database Protection Act ("CDPA"), becoming the first state in the United States to pass legislation requiring any government or private entity possessing PII to notify the owners in the event of a disclosure of PII to an unauthorized person resulting from a security breach.[128] Additionally, the CDPA placed an unprecedented statutory duty on businesses that own or authorize the use of PII to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[129] California's approach has served as a model for similar statutes in dozens of other states. As of January 2016, at least forty-seven states now require businesses to notify their customers or clients if there is a security breach involving PII.[130] These state laws generally apply to any business maintaining PII of its residents.

For instance, in 2005, the Texas legislature passed Senate Bill 122, which amended the Texas Code of Criminal Procedure and

126. *See generally* STATE OPEN GOVERNMENT LAW AND PRACTICE IN A POST-9/11 WORLD, (Jeffrey F. Addicott, Loren A. Cochran, Lucy A. Dalglish & Nathan Winegar eds., 2007) (suggesting some fear that terrorists could use open government laws to hack into government facilities, which has prompted at least forty-eight of them to add non-release provisions to their open government laws).

127. *See infra* notes 132–36 and accompanying text.

128. CAL. CIV. CODE § 1798.82 (West 2016), *amended by* 2016 Cal. Stat. 96 (A.B. 2828).

129. *Id.* § 1798.81.5(b).

130. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGIS., http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Feb. 13, 2017).

the Texas Business and Commerce Code.[131] The relevant portion of the Texas Business and Commerce Code reads:

> A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.[132]

Like the approach in California, the Texas legislature statutorily defined that businesses within the state of Texas owe a duty to their customers to implement reasonable procedures to safeguard PII. Section 521.053 of the Texas Business & Commerce Code provides:

> Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person [emphasis added].[133]

D. *Asleep at the Wheel*

Considering that ninety percent of cyber attacks target the private sector, it is evident that relying on voluntary engagement practices to protect America's critical infrastructure is inadequate. There can be absolutely no question that the threat of a significant cyber attack on the nation's critical infrastructure is a grave concern. In turn, there can be absolutely no question that, because of this potential for societal catastrophe, protecting cyberspace has passed into the realm of a societal "commons" in which the government is obligated to exert greater protection

131. S.B. 122, 79th Leg., ch. 294, § 1(a) (codified at TEX. CODE CRIM. PROC. ANN. art. 2.29 (West 2005)).

132. TEX. BUS. & COM. CODE ANN. § 48.102(a) (2006).

133. *Id.* § 48.103(c) (2006). The law defines sensitive personal data at:

> Subsection (b), an individual's first name or first initial and last name in combination with any one or more of the following items, if the names and the items *are not encrypted*:
> (A) social security number;
> (B) driver's license number or government-issued identification number; or account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Id. § 48.002(2) (2006) (emphasis added).

than it has over the past thirty years.[134] In other words, the serious threat posed by a cyber attack on our critical infrastructure—including massive human casualties, wide-scale economic damage, wide-scale disruption to public order, and significant disruption of America's national readiness for war—indicates that the government has a duty to provide meaningful protection for the common good. From this perspective, many question the efficacy of any federal approach to secure cyberspace that fails to incorporate, or adequately motivate private industry to incorporate, the highest degree of cybersecurity.

Because it is impossible to immediately determine the precise source of a cyber attack—it could be an amateur, a terrorist, a criminal, or even a hostile nation-state—the so-called "response baton" will originate with the private sector and then may be passed to law enforcement and next, perhaps, to the military. Realistically, a commons-oriented cybersecurity strategy would involve two key elements: (1) a program that requires the sharing of timely and accurate information all along the continuum, from private to government; and (2) the adoption of industry-specific cybersecurity standards and a corresponding process of certification.

Amazingly, despite lip service to the massive damage that could be caused by a significant cyber attack on the nation's critical infrastructure, the Obama administration's 2015 National Security Strategy ("NSS") not only placed "confront climate change" above the far more dangerous threat to American security posed by cyber attacks, the 2015 NSS also characterized America's primary cyber concerns as needing to "ensure access to shared spaces" such as "cyberspace" with other nations![135]

With such absurd leadership signals about cyber priorities for the nation, it is not unreasonable to question whether the government is too complacent in terms of advancing cybersecurity concerns. Neither is it unreasonable to suspect this is a film we have seen before in terms of how the government has failed to anticipate and take concrete steps to protect Americans from harm

134. *See, e.g.*, Roger Hurwitz, *Depleted Trust in the Cyber Commons*, STRATEGIC STUDIES QUAR., Fall 2012 (describing steps nations must take to ensure the survival of the internet as a "commons resource").

135. THE WHITE HOUSE, NATIONAL SECURITY STRATEGY 12 (2015).

in the physical world—most notably, from the radical Islamic terror attacks of 9/11 against the United States.[136] In the wake of 9/11, Congress authorized a bipartisan group to make findings and recommendations about what happened and why.[137] In terms of government preparedness, the 9/11 Commission produced a lengthy document that described American intelligence and law enforcement agencies' failure to anticipate and deal with the threat of the al Qaeda terror group[138] as a "failure of imagination."[139] The American government did not seriously consider the real possibility of an al Qaeda terror attack using commercial airlines as precision weapons. Consequently, the United States was caught completely by surprise, resulting in the violent deaths of 3000 humans and the loss of billions of dollars in property.[140] It is reasonable to ask if this "failure of imagination" pertaining to 9/11 will repeat itself in the cyber world due to the government's haphazard approach to cybersecurity.

136. Evan Thomas, *A New Date of Infamy*, NEWSWEEK (Sept. 13, 2001), http://www.newsweek.com/new-date-infamy-151751 (setting out a timeline of events that occurred on Sept. 11, 2001). Identification of the source(s) of a cyber-attack, including the Internet Protocol ("IP") address of the attacker, is vital to the identification of the attacker, the deployment of effective countermeasures and the development of new cyber security defense tools. An automated process of tracing the source(s) of a DDoS attack is known as "IP Traceback." Of course, IP Traceback opens up its own area of liability and privacy issues associated offensive cybersecurity actions. *Id*.

137. NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, https://www.9-11commission.gov (last modified Sept. 20 2004); *see* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 COMMISSION REPORT 1–46 (2004) (setting out a final analysis by the United States government of all the issues associated with the 9/11 attacks by al Qaeda). On September 11, 2001, nineteen members of the radical Islamic terror group named al Qaeda hijacked four United States passenger aircrafts while in flight (five terrorists each in three planes and four in the fourth that went down in Pennsylvania). The al Qaeda foot soldiers intentionally crashed two of the aircraft into the Twin Towers of the World Trade Center in New York City. A third aircraft targeted the Pentagon in northern Virginia. The fourth plane, United 93, went down in a field in Pennsylvania, most likely because of the heroic efforts of some of the passengers who stormed the al Qaeda pilots. *Id*.

138. The key declaration of war from the perspective of the radical Islamic group was made on February 22, 1998, when Osama bin Laden and the "World Islamic Front" formally issued a religious fatwa urging all Muslims to engage in physical violence against "Crusaders and Jews." PETER L. BERGEN, THE OSAMA BIN LADEN I KNOW 196 (2006).

139. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 COMMISSION REPORT 336 (2004).

140. Tom Templeton & Tom Lumley, *9/11 in Numbers*, THE GUARDIAN (Aug. 17, 2002), https://www.theguardian.com/world/2002/aug/18/usa.terrorism.

V. CYBER CIVIL LIABILITY LAWSUITS

"[I]n the data-security context, 'reasonableness is the touchstone.'"[141]

—FTC v. Wyndham Worldwide Corp.

As noted in Part IV, the government's understated theme of engagement continues to place emphasis on user privacy and cyber system integrity.[142] As a result, the matter of cybersecurity in general—particularly in terms of setting viable security standards—is left in the hands of civilian technology developers, manufacturers, and owner/operators.

If the government's engagement strategy does not adequately alter business practices, change can come from market pressures and consumer desires. At the forefront of most internet users' minds is the question of privacy.[143] As they venture online, users and consumers look for reassurance that the PII they submit will remain protected by their own computer, their Internet Service Provider ("ISP"), and the website they are visiting. Conversely, the chief concern of technology developers, manufacturers, and owner/operators is making a profit.

Still, the need to provide a service or product in a competitive marketplace can [or "lead to"] cause positive changes. For example, recognizing that users of electronic devices—from handheld mobile devices to desktop computers—demand concrete assurances that their privacy is fully protected when they are engaging in various online activities such as shopping, communicating with others, or banking, the $120 billion[144] industry has made encryp-

141. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 616 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015). The Federal Trade Commission filed unfair and deceptive practices when Wyndham failed to take appropriate steps following a cyber-attack. *Id.*

142. *See* NAT'L SEC. COUNCIL & HOMELAND SEC. COUNCIL, CYBERSPACE POLICY REVIEW, ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE i (2009).

143. *See generally* NAT'L SEC. COUNCIL & HOMELAND SEC. COUNCIL, CYBERSPACE POLICY REVIEW, ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE i (2009); David Inserra & Paul Rosenzweig, *Cybersecurity Information Sharing: One Step Toward U.S. Security*, *Prosperity*, *and Freedom in Cyberspace*, HERITAGE FOUND., (Apr. 1, 2014), http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

144. *See* JONATHAN GODFREY ET AL., ACT, STATE OF THE APP ECONOMY 4 (2016).

tion[145] a cornerstone element of business. To combat the omnipresent threat of cyber attacks, corporations around the globe have spent an estimated $75 billion in 2015 and are predicted to shell out an incredible $90 billion by 2017.[146] But is this enough?

Numerous public and private studies have offered various proposals for implementing sound security practices to ensure greater cybersecurity, particularly when it comes to critical infrastructure systems. However, a Congressional Research Service report correctly observed that none of them are "likely to be widely adopted in the absence of sufficient economic incentives for cybersecurity."[147] In other words, what is needed is a cyber version of the Connie Francis lawsuit where the affected plaintiff(s) are able to show significant physical loss, and the associated recovery is large enough to then motivate massive cybersecurity improvements across the board.

Liability issues associated with breaches of computer security rubricate cyber discussions from ISPs and other private companies, even if little is being done to rectify those concerns. As explained in Part I, civil action lawsuits for failure to protect customers from cyber attacks will soon find their way into court as tort or product liability claims.[148]

Liability under tort law requires that the defendant breached a legal duty to exercise a level of care imposed by either statute or common law. In terms of developing a reasonableness test for the level of cybersecurity owed, judges will no doubt give great consideration to the developing legal standards for information secu-

145. Brief of Amicus Curiae at 2, App Ass'n in Support of Apple Inc.'s Motion to Vacate Order Compelling Assistance, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-CM-0001-SP (C.D. Cal. Mar. 22, 2016). "[Encryption] provides the transaction security that allows companies to sell globally and provides security for much of the nation's commerce, and ensures that our most sensitive data stays private—protecting patient health information, financial data, and every American who shops online." *Id*.

146. Brief of Amicus Curiae at 9, AVG Technologies, The Computer & Commc'ns Ind. Ass'n, Data Foundry, Golden Frog, The Internet Ass'n, and the Internet Infrastructure Coal. in Support of Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, at 2, No. 5:16-CM-00010-SP (C.D. Cal. Mar. 22, 2016).

147. FISCHER, NATIONAL FRAMEWORK, *supra* note 69, at ii.

148. *See* Nigel Pearson, *A Larger Problem: Financial and Reputational Risks*, COMPUTER FRAUD & SECURITY, Apr. 2014, at 11, 13.

rity, which in this case would be discovered by reviewing industry trends in the area of cybersecurity. The legal obligation to implement adequate cybersecurity measures can be classified as either industry-specific, data-specific, or focused on public companies.[149] At a minimum, there exists at least a general obligation to provide some level of cybersecurity. Specifically, legal obligations for technology developers, manufacturers, and owner/operators regarding information security derive from multiple sources: enacted federal and state laws, regulations and government enforcement actions, and common law fiduciary duties and obligations to provide reasonable care.

What, then, is considered reasonable care in the context of cybersecurity protection? One could argue that the very fact a security breach occurs is a breach of a common law duty owed by the ISP or a commercial firm to provide reasonable security for its customers' PII. But the more likely approach is to look at industry standards.[150] In fact, various cyberspace arenas have developed a number of standards, best practices, and guidelines. While adherence to an existing industry standard is not dispositive to the determination of reasonable care owed, it is relevant. Still, as in the Connie Francis case, any given court can choose to ignore industry standards and determine that "reasonable care" demanded a higher level of duty.[151]

149. Thomas J. Smedinghoff, *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, 16 MICH. ST. J. INT'L L. 1, 10 (2007); *see also* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 433, 498–99 (2012); *supra* note 136.

150. *See* Tim Goles & Sandra G. Dykes, *Legal Perspectives on Distributed Denial of Service Attack Traceback: A Fresh Approach*, 6TH ANNUAL SECURITY CONF. 31-11 (Apr. 11–12, 2007), http://www.isy.vcu.edu/~gdhillon/Old2/secconf/secconf07/PDFs/31.pdf; *see also* Kesan & Hayes, *supra* note 149, at 433, 498–99.

151. *See* Meiring de Villiers, *Enabling Technologies of Cyber Crime: Why Lawyers Need to Understand It*, 11 PITT. J. TECH. L. & POL'Y, 1, 41 (2011). Another topic of discussion in terms of potential liability revolves around the interconnectivity of cyberspace and the idea that liability might be extended to other tortfeasors who may have contributed to the cyber-attack due to sloppy cybersecurity measures. Thus, an emerging negligence theory entitled the Encourage Free Radicals ("EFR") doctrine, extends the liability of an original tortfeasor to a second tortfeasor if it is found that the lax lever of cybersecurity measures encouraged the attacks of "free radicals." *Id*. Mark Grady, the originator of the doctrine, describes free radicals as "those individuals who are shielded from liability by anonymity, insufficient assets, lack of mental capacity, or lack of good judgment." Meiring de Villiers, *Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare*, 4 NW. J. TECH & INTELL. PROP. 13, 16 (2005). For instance, cyber criminals might fit the description of free radicals because they are judgment-proof, elusive, and protected by anonymity. The

In the interim—until a huge Connie Francis-styled cyber lawsuit takes place perhaps some movement forward can originate in the form of class action lawsuits over cyber breaches that result in the release of PII. Previously, one of the greatest legal hurdles in these class actions is the showing of injury in fact.

In 2014, two Ninth Circuit court decisions signified positive change in terms of satisfying the plaintiff's standing for an injury in fact when customer's PII was released due to a data breach by hackers. In both cases, the companies failed to take timely action to notify customers of the breach. In both cases—*In re Sony Gaming Networks & Customer Data Security Breach*[152]and *In re Adobe Systems Privacy Litigation*[153] the courts found the plaintiffs alleged a credible threat of harm based on the fact that their PII was released. In a class action suit against the retail giant Target, filed after a cyber attack resulted in the loss of 110 million customer's PII, the "[p]laintiffs contend[ed] that Target violated . . . consumer protection laws in several ways," including: "failing to maintain adequate computer systems and data security practices."[154]

CONCLUSION

"*We must defend and protect federal networks and data . . . [w]e operate these networks on behalf of the American people and they are very important and very sacred.*"[155]

—President Donald J. Trump

It was American businessmen who developed the technological advances that opened up the unfathomable marvels of cyberspace and, by so doing, spawned a modern world that is now completely dependent on cyber, particularly in the context of sustaining and

second factor necessary for applying the EFR doctrine is that the tortfeasor's encouragement of the free radical constituted negligent behavior.

152. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 954–55 (S.D. Cal. 2014).

153. *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1206–07 (N.D. Cal. 2014).

154. *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157, 1161–62 (D. Minn. 2014).

155. President Donald J. Trump, Remarks on the Meeting of Cybersecurity Experts at the White House (Jan. 31, 2017), https://www.c-span.org/video/?c4653944/rudy-giuliani-president-trump-keith-alexander.

operating our critical infrastructure. Unfortunately, if a given SCADA succumbs to a cyber attack, it could cripple a critical infrastructure and cause tremendous harm, including mass human casualties. The cyber attack might devastate electric utilities; chemical, gas, and oil refineries; public transportation; or hospital services. And there is currently no Plan B.

Since SCADA systems are designed for efficiency, not security, making them safe and secure is further frustrated by the absence of a strong federal strategy that mandates information sharing and effective cybersecurity standards. In addition, the widespread technical ignorance of security managers and the false sense of security due to the absence of a major cyber attack on America's infrastructure contribute to the vulnerability equation.

Partnering the private industry with the government to secure cyberspace is in its infancy, but given the fact that protecting the critical infrastructure as a societal "commons" is a responsibility of the government, eventually the government may be forced to implement programs to ensure the private industry shares cybersecurity information and develops proper cybersecurity measures. Unfortunately, the complacent habit of dealing only with realized threats has not imparted a sense of urgency that will ultimately be necessary to protect the cyber world and make it as safe a place as the physical world.

At the end of the day, neither private industry nor the government can defend the SCADA systems of the nation's critical infrastructure alone. Still, the larger burden will always fall upon the shoulders of private industry. Until the Connie Francis-styled cyber case occurs, the issue of tort liability and improved cybersecurity requirements will continue to bubble below the surface.[156] But like a volcano, it will one day erupt. The hope is that the impetus that propels the lawsuit, which will ignite the movement toward greater levels of cybersecurity, will be smaller in terms of sustained damage.

156. *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 311 (2005).