MOBILE BANKING: THE BEST HOPE FOR CYBER SECURITY DEVELOPMENT

MATTHEW Y. CHANG*

Convenience does not come without a cost. In the realm of cyber security, for example, increases in consumer convenience have led to major breaches in security. This Note analyzes the current state of cyber security in terms of the technology and the legal environment. After establishing the hack-prone nature of internet-based technology and the inadequacy with which cyber security is dealt with in the United States, this Note recommends creation of a single governmental agency to oversee cyber security. Specifically, this agency would be responsible for managing and encouraging developments in cyber security within the financial industry, which could then be transferred to other private and governmental industries. Although the end result is better protection for consumers, in developing cyber security, it is more productive to focus laws and regulations on helping businesses protect themselves. The goal of legislation should not be to shield financial institutions from litigation but to hold them accountable while providing support.

TABLE OF CONTENTS

* J.D. Candidate 2017, University of Illinois College of Law. M.B.A. Candidate 2017, University of Illinois College of Business. B.S. Biology 2012, College of William and Mary. I would like to thank the editors, members, and staff of the *University of Illinois Law Review* for their work on this note. I would also like to thank my family and friends for their unending support through all of my personal and academic endeavors.

I. INTRODUCTION

As technology advances and gets incorporated into every facet of our lives, we pay for the convenience in various ways.[1] With the progression of transportation, from horses and buggies to trains and personal automobiles, this convenience came at the cost of increased carbon emissions, unsightly developments of railroads and highway systems, and more congested cities. People are currently looking for ways to combat the negative externalities created by technological advances in transportation, not only by investing in even newer technologies like cleaner fuel sources but also by reverting back to older methods like riding bicycles.[2]

The rise of credit and debit cards has led to a similar convenience, enabling consumers to spend money without carrying around stacks of cash. As credit card technology has advanced, there have also been negative externalities associated with it that are currently being dealt with at

1. Eleanor Lumsden, *Securing Mobile Technology & Financial Transactions in the United States*, 9 BERKELEY BUS. L.J. 139, 140 (2012). Lumsden discusses the paradox of the conflict between convenience and security in the context of mobile technology and financial transactions. Her article makes recommendations for mitigating risks posed by emerging mobile technology, but does so from the standpoint of increasing the security of the consumers. *Id.* The recommendation presented in the present note involves protecting the banking institutions. Although the end result is better protection for consumers, the focus of laws and regulations on businesses is a more productive use of resources. While consumers represent smaller pieces of unprotected data, financial institutions are the main players in mobile technology security and thus should be the focus of any changes made to security standards. *Id.* at 143. To be clear, the goal of legislation should not be to shield financial institutions from litigation but to hold them accountable.

2. *See, e.g.*, Hiroko Tabuchi, *Seeing Future in Fuel Cells, Toyota Ends Tesla Deal*, N.Y. TIMES, May 12, 2014, http://www.nytimes.com/2014/05/13/business/energy-environment/seeing-future-in-fuel-cells-toyota-ends-tesla-deal.html (discussing viable zero-emissions technologies including Toyota's hydrogen fuel cells, Tesla's electric vehicles, and the presence of gas-electric hybrid vehicles). Bill Chappell, *Cyclists Do Not Emit More Carbon than Cars, State Legislator Admits*, NAT'L PUB. RADIO (Mar. 5, 2013, 12:39 PM), http://www.npr.org/blogs/thetwo-way/2013/03/05/173523998/cyclists-do-no-emit-more-carbon-than-cars-state-legislator-admits (providing an example of a dispute regarding whether cars or bicycles emit more carbon).

the private level.[3] One such negative externality is the rise of hackers.[4] Few people know how credit cards work other than the fact that they communicate to different systems through computers and other electronic devices. As the general public has become more careless, hackers have entered the arena in swarms, likely encouraged by the drastic growth in cyber-wealth.[5] This has led to breaches in cyber security that range from petty theft of an individual's credit card to millions of people's information being stolen from company databases. Target, a fairly well-known discount retailer, is just one of many companies that has experienced a breach in its cyber security.[6] In this particular case, the breach led to credit and debit card data from forty-million accounts being stolen.[7]

This breach is just one of many instances of cyber security breaches that have occurred in recent years,[8] and the number of breaches can only be expected to grow as the technology grows stagnant and hackers catch up to the technology.[9] While technology may be able to progress, because of the extent to which the current system is in place, it is likely businesses will not be able to rely on technological advances to keep data securely out of reach of foul play. Until there is a large-scale infrastructural change, like a move from a railroad system to a national highway system, the current system will have to rely on minor changes and remain vigilant. Like watching for a shooting star, it could come at any second, and once it happens there is no going back. The only way to ensure that you see it is by not looking away. Similarly, companies will have to find a way to keep watch for the cyber attacks that will inevitably continue to happen.[10]

3. *E.g.*, Jose Pagliery, *Chip-Based Credit Cards Coming to Target*, CNN MONEY (Apr. 30, 2014, 1:46 PM), http://money.cnn.com/2014/04/30/technology/security/target-credit-card/ (discussing Target's decision to change out their current credit cards with newer models that are enabled with computer chips in the aftermath of their major breach in 2013).

4. *See generally* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503 (2013) (discussing negative externalities in regulating cyber-security and arguing that cyber-conflicts should be conceived of in administrative law terms instead of criminal or armed conflict law).

5. *See* Tom Risen, *Companies Unprepared as Hacking Increases*, U.S. NEWS (May 28, 2014, 4:33 PM), http://www.usnews.com/news/articles/2014/05/28/companies-unprepared-as-hacking-increases (reporting recent increases in hacking).

6. Gregory Wallace, *Target Credit Card Hack: What You Need to Know*, CNN MONEY (Dec. 23, 2013, 11:43 AM), http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/?iid=EL.

7. *Id.*

8. *See, e.g.*, Brian Fung, *How Many Cyberattacks Hit the United States Last Year?*, NEXTGOV (Mar. 8, 2013), http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.

9. *See* Manish Gupta & Raj Sharman, *Determinants of Data Breaches: A Categorization-Based Empirical Investigation*, 7 J. APPLIED SECURITY RES. 375, 392 (2012) (empirical study on data breaches, indicating an increasing in the rate). *See also* EDWARD G. AMOROSO, CYBER ATTACKS: PROTECTING NATIONAL INFRASTRUCTURE 133 (2011) (explaining that even long-term suppression of information regarding cyber security infrastructure for the sake of making things more difficult for hackers and third parties is not a reliable means of security "because suppressed information has a tendency to eventually become public").

10. Anne D'Innocenzio, *Data Breaches Don't Alter Habits, Poll Shows*, BOSTON GLOBE, Jan. 28, 2014, http://www.bostonglobe.com/business/2014/01/28/gfk-poll-breaches-not-changing-people-habits/

With the sudden rise of credit card use and the almost obsolete need for paper money, consumers have grown lax.[11] Though Americans report that they are afraid of becoming victims of security breaches, it seems average American shoppers are not any more inclined to be careful.[12] Though sixty-two percent of respondents to an Associated Press-GfK poll reported being very concerned when buying things on their mobile phones, only "37 percent [had] tried to use cash for purchases rather than pay with plastic in response to data thefts."[13] Smartphones have even reached the point where some mobile applications do not even require a password but ask for a "fingerprint," instructing the user to place their finger on a built-in fingerprint scanner that it then matches with a preprogrammed print.[14] Most notably, Apple has incorporated this feature, called Touch ID, into its most recent lines of smartphones.[15] Although Touch ID is secure in that it is based on advanced technologies and is not easily hacked,[16] it only further encourages people to stop thinking about security by allowing them to bypass certain security points at the touch of a finger. Regardless of the additional security added by features like Touch ID, these technologies are, intentionally or not, making the average person more reliant upon technology.

As people become more lax regarding cyber security, efforts to protect individuals becomes too daunting for any government agency to handle. Even apart from privacy issues that may arise and lead to obligations of businesses on behalf of consumers, the issues regarding cyber security only grow as people ignore certificate warnings and advances in technology and user-interfaces which make it difficult for people to care about security.

Even in the everyday activity of having a personal bank account, much of the responsibility of keeping accounts secure has been taken from the consumers and added to the load of financial institutions in the form of bank insurance.[17] The Federal Deposit Insurance Corporation

iN0HseIO2akTu1OrHegpHK/story.html (referencing an Associated-GfK poll that shows "[thirty-seven] percent [of respondents had] tried to use cash for purchases rather than pay with plastic in response to data thefts such as the one at Target . . . .").

11. *See* CSID, CONSUMER SURVEY: PASSWORD HABITS A STUDY OF PASSWORD HABITS AMONG AMERICAN CONSUMERS (2012) [hereinafter CONSUMER SURVEY], *available at* http://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf (reporting that consumers are careless about password creation).

12. *See* D'Innocenzio, *supra* note 10.

13. *Id.*

14. *See, e.g.*, *About Touch ID security on iPhone and iPad*, APPLE, http://support.apple.com/kb/HT5949 (last modified Nov. 2, 2015).

15. *Id.*

16. *Id.*; Marc Rogers, *Why I Hacked TouchID (Again) and Still Think It's Awesome*, LOOKOUT BLOG (Sept. 23, 2014), https://blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack/ (laying out instructions on how to hack the fingerprint scanner on the iPhone 5s and iPhone 6 and expressing disappointment at Apple's failure to "tighten up the security of TouchID").

17. *See Safe Internet Banking*, FEDERAL DEPOSIT INSURANCE CORPORATION, https://www.fdic.gov/bank/individual/online/safe.html (last updated July 28, 2014) (stating that if your bank is FDIC insured, you are insured to at least $250,000).

("FDIC"), an agency created by the Banking Act of 1933,[18] provides insurance for member banks' depositors up to $250,000.[19] Just by choosing a bank that is FDIC insured, consumers are put at ease and rest assured that their deposits are safe up to a certain amount. Regulations like this make it unlikely that consumers will be more careful as technology brings more conveniences. In order to protect these consumers, the government needs to focus on banking institutions and securing them. Starting there, any developments in cyber security in mobile banking can be translated to other industries in need of cyber security enhancements.

In a 2012 article, Eleanor Lumsden makes recommendations for mitigating risks posed by emerging mobile technology, but does so from the standpoint of increasing the security of the consumers.[20] In contrast, the recommendation presented in this Note involves protecting the banking institutions and creating a single agency to oversee cyber security development in that industry. This Note analyzes the current state of cyber security in terms of the technology and the legal environment. After establishing the hack-prone nature of internet-based technology and the inadequacy with which cyber security is dealt with in the United States, this Note makes recommendations that include the creation of a single agency. This agency would be responsible for managing and encouraging developments in cyber security within the financial industry, which could then be transferred to other private and governmental industries. Although the end result is better protection for consumers, in developing cyber security, it is more productive to focus laws and regulations on helping businesses protect themselves. With the increased use of cell phones to access the Internet, financial institutions are the main players in mobile technology security and should be the focus of any changes in security standards. To be clear, the goal of legislation should not be to shield financial institutions from litigation but to hold them accountable while providing support.

Part II of this Note presents background on the current state of security systems and lays out some of the laws and regulations regarding cyber security that have developed alongside advances in technology.[21] Understanding the technical background and the current legal backdrop is relevant to cyber security as a whole, but Part II specifically addresses the relevance of current legislation and regulations as they relate to the financial mobile industry. Although state laws play a large part in regulating privacy aspects of cyber security, specific differences among state laws are not discussed in this Note other than to point out that the different state laws further complicate compliance for private companies.[22]

18. Banking Act of 1933, 48 Stat. 162, 168 (1933).
19. *Safe Internet Banking*, *supra* note 17.
20. Lumsden, *supra* note 1, at 180.
21. *See infra* Part II.
22. *2015 Security Breach Legislation*, NAT'L CONF. OF ST. LEGISLATURES (Oct. 22, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx [hereinafter *Security Breach Legislation*].

Part III analyzes the potential efficacy of recommendations and changes that are being made in the mobile security industry both in terms of the law and the technology. Part IV provides a recommendation to increase cyber security of financial institutions by focusing on more business-oriented regulations and presents the need for a single agency in charge of cyber security, particularly around mobile banking. Part V concludes with a summary of why cyber security requires the attention of private and government actors and why efforts should be made to focus on financial institutions.

II. BACKGROUND

Consumers are increasingly using their phones to access the Internet.[23] Despite this increased usage and the highly anticipated product releases,[24] new phones are still based on foundational technologies that are based on radio waves and the Internet.[25] In order to deal with the legal aspects of cyber security issues, this section lays out some of the technology responsible for the increased convenience of cell phones and continues on to the current state of cyber security law.

As mobile technology became more prevalent, the government's concerns for the safety and privacy of its citizens also grew, evidenced by the creation of the Department of Homeland Security's Office of Cyber Security and Communications in 2006.[26] With the increase in mobile phone usage, particularly in mobile payments,[27] privacy became a greater concern in addition to the threat of terrorism that helped usher in the creation of the Department of Homeland Security.[28] In order to protect consumers, agencies like the Federal Trade Commission began applying existing laws like the Federal Trade Commission Act to encompass the mobile arena.[29] Because of the drastic increase in the use of mobile technology, there was not one set of regulations or laws ready to handle both the privacy and security implications that came with the increased reli-

23. *New Research: Global Surge in Smartphone Usage, UK Sees Biggest Jump with 15% Increase*, GOOGLE MOBILE ADS BLOG (Jan. 25, 2012, 8:11 AM), http://googlemobileads.blogspot.com/2012/01/new-research-global-surge-in-smartphone.html [hereinafter *New Research*].

24. *See* Katie Hafner, *Waiting for the Latest in Wizardry*, N.Y. TIMES, (June 27, 2007), http://www.nytimes.com/2007/06/27/technology/27apple.html?_r=0 (describing the anticipation and frenzy with which people waited for some phones).

25. *See* Dave Roos, *How Mobile Broadband Services Work*, HOWSTUFFWORKS.COM, http://computer.howstuffworks.com/mobile-broadband-service1.htm (last visited Jan. 21, 2016) (describing the radio technology that makes cell phones work and also allows for mobile tethering with laptops).

26. OFFICE OF CYBER SECURITY AND COMMUNICATIONS, DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/office-cybersecurity-and-communications (last updated Oct. 27, 2015).

27. Elizabeth Eraker et al., *Mobile Payments: The Challenge of Protecting Consumers and Innovation*, 10 PRIVACY & SECURITY L. REP. 212, 212 (2011) [hereinafter *Mobile Payments*].

28. *Id.*

29. Federal Trade Commission Act, 15 U.S.C. §§ 41–48 (2012); *Prepared Statement of the Fed. Trade Comm'n on Consumer Privacy and Prot. in the Mobile Marketplace Before the Comm. on Commerce, Science, and Transp.*, 112th Cong. 5 (May 19, 2011) [hereinafter *Prepared Statement*] (statement of David C. Vladeck, Director of the Bureau of Consumer Protection of the Federal Trade Commission).

ance on mobile applications.[30] As a result, cyber security law is a mixture of laws and regulations at both the state and federal levels attacking the general problem of cyber security from both privacy and security viewpoints.[31]

A. State of Current Security Systems

Though the use of technology in the financial industry has increased, the foundation of these technologies is still based on the Internet that existed decades ago.[32] Leonard Kleinrock's theory of packet switching, first published in 1961, helped make the Internet possible and is still in use today.[33]

1. The Internet and Encryption

The Internet works as a packet-switched network as opposed to a circuit-switched network used in telephone systems.[34] This means that when information is sent across the Internet, it is first broken up into pieces of information called packets that are then sent to the recipient over numerous routes, and reassembled upon receipt.[35] In order to access the Internet, a computer makes use of the Transmission Control Protocol ("TCP"), which breaks down and reassembles packets of information, and the Internet Protocol ("IP"), which tells the information how to get to its destination.[36] As these packets reach their destinations, there are security measures that can be taken to ensure there was no tampering of information en route.[37] Because information is sent over an open chan-

30. *Prepared Statement*, *supra* note 29, at 5–9 (listing the areas of commerce in which the Federal Trade Commission plays a role and further implying that certain areas of mobile security such as non-consumer protection was enforced by a different agency).

31. Jonathan S. Feld et al., *Coping with Evolving US, State Cyber Security Rules*, CORPORATE COUNSEL (May 12, 2014), http://www.corpcounsel.com/id=1202654946074/Coping-With-Evolving-US-State-Cyber security-Rules?slreturn=20140917125712.

32. Leonard Kleinrock, *Information Flow in Large Communication Nets* (May 31, 1961) (approved Ph.D. thesis proposal, Massachusetts Institute of Technology), *available at* http://www.lk.cs.ucla.edu/data/files/Kleinrock/Information%20Flow%20in%20Large%20Communication%20Nets.pdf (outlining a novel, mathematical packet switching theory that was essential to the development of Internet). For a history of the Internet from the privatization of the NSFNET, see Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89 (2001).

33. Kleinrock, *supra* note 32; PRESTON GRALLA, HOW THE INTERNET WORKS 13 (Greg Wiegand et al. eds., 1999) (describing the use of Transmission Control Protocol and Internet Protocol on the Internet).

34. GRALLA, *supra* note 33, at 13. Whereas there is a network dedicated to a single connection in a circuit switched network, in a packet-switched network, information is broken into small packets and sent over different routes because there is not a single, unbroken connection between the two parties. *Id.*

35. *Id.*

36. *Id.* at 14.

37. *Introduction to Public-Key Cryptography*, MOZILLA DEVELOPMENT NETWORK, https://developer.mozilla.org/en-US/docs/Introduction_to_Public-Key_Cryptography (last visited Jan. 22, 2016) [hereinafter *Cryptography*] (explaining different methods of encryption).

nel, like a banner with your message being flown across the sky, technological advances in this area have been focused on encrypting information before it is sent so as to prevent "eavesdropping."[38]

TCP and IP have been a part of the Internet since the 1960s and are essential to the concept of a computer network.[39] The security measures that have been put in place build on top of TCP/IP and involve methods of encryption and methods that identify tampering.[40]

One method of encryption commonly used by banks is the public-key encryption (in tandem with a symmetric key in the SSL protocol).[41] This method of encryption requires a pair of keys, a public and a private key, that enables someone to authenticate his or her identity in order to have the authority to complete particular actions.[42] Also called an asymmetric encryption, in this process, the information being sent is encrypted by the public key and can only be decrypted by the private key.[43] Similarly, information encrypted by the private key can be decrypted by the public key.[44] This method is used by banks to obtain a "signature" of the person with the public key, but it is not as useful as a means of relaying sensitive information to particular individuals because the public key is publicly distributed, meaning there is no discretion as to who has a copy.[45] Banks use public keys because they are less computationally intensive than symmetric encryption, but banks will also encrypt symmetric keys to send sensitive information.[46]

2. Cell Phones

As cell phone use has proliferated, access to development tools has greatly increased, to the point where almost anyone with a computer can create a mobile application.[47] The Android operating system allows for installation of third-party software that could sometimes jeopardize the contents of a cell phone.[48] While this is great for innovative growth, there is no check on the security measures that such third-party applications

38. *Id.* (explaining eavesdropping in a cyber security context).

39. Barry M. Leiner et al., *Brief History of the Internet*, INTERNET SOCIETY 1, 2–3, *available at* http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf.

40. *Cryptography*, *supra* note 37; *see* discussion *infra* Part II.C.1.

41. Lucian Constantin, *Security Analysis of Mobile Banking Apps Reveals Significant Weaknesses*, PCWORLD (Jan. 9, 2014, 10:12 AM), http://www.pcworld.com/article/2086320/security-analysis-of-mobile-banking-apps-reveals-significant-weaknesses.html.

42. *Cryptography*, *supra* note 37.

43. *Encryption and Decryption,* MOZILLA DEVELOPMENT NETWORK, https://developer.mozilla.org/en-US/docs/Archive/Security/Encryption_and_Decryption (last visited Nov. 11, 2015).

44. *Id.*

45. *Id.*

46. *Id.*

47. *See* Heather Clancy, *Handy Code-Free Mobile App Development Resources for Small Businesses*, ZDNET.COM, (Aug. 6, 2014, 4:58 PM), http://www.zdnet.com/article/14-diy-mobile-app-development-resources-for-small-businesses/ (discussing resources for do-it-yourself mobile application development).

48. William Enck et al., A STUDY OF ANDROID APPLICATION SECURITY, (Aug. 2011), *available at* http://www.enck.org/pubs/enck-sec11.pdf.

may or may not incorporate. Considering that "ninety-nine percent of all mobile malware in 2013 targeted Android devices,"[49] with over one billion active users of Android operating systems,[50] security of its mobile applications is a concern. Specifically, it has been noted that there is a "concern for misuse of privacy sensitive information," which directly affects any mobile application a financial institution may be touting.[51] As a select few operating systems become standard in millions of electronic devices, any security flaws will be compounded. As a result, it has been noted that operating system "designers [need] to rethink security and access control" in the devices.[52]

3. Other Mobile Payment Systems

In addition to the typical credit card or bank card transactions that occur through mobile phones, other methods of payment have emerged that some argue are more secure than common methods employed in managing mobile payments.[53] PAYware allows for credit card payments much like Square[54] but utilizes a method of encryption slightly different from the SSL encryption.[55] PAYware uses an "end-to-end" encryption that protects the customer information "at the exact instant of card swipe," ensuring the information is secure even if the phone itself has been compromised.[56] As security breaches continue to occur within well-recognized companies, some have surmised that competition for more secure mobile transactions may naturally lead private actors to continue developing better, more secure systems of payment.[57] While this could be great for the development and evolution of cyber security pertaining to mobile applications, the lack of regulation and requirement for more secure systems among companies and their mobile applications may still lead to under-secured companies and mobile applications.[58]

Other mobile payment systems incorporate different methods of encryption that are still managed through the Internet packet system.[59] These alternative methods may provide more secure methods of trans-

49. CISCO 2014 Annual Security Report 3, *available at* http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

50. Christopher Trout, *Android Still the Dominant Mobile OS with 1 Billion Active Users*, ENGADGET (June 25, 2014, 12:21 PM), http://www.engadget.com/2014/06/25/google-io-2014-by-the-numbers/.

51. Enck et al., *supra* note 48.

52. ANDROID SECURITY MODULES, http://www.androidsecuritymodules.org/ (last visited Jan. 22, 2016).

53. *Frequently Asked Questions*, Bancard Merchant Services, (last visited Feb. 8, 2015), http://www.gopayware.com/faq.php [hereinafter *Frequently Asked Questions*]; *Mobile Payments*, *supra* note 27, *at* 2095.

54. SQUARE, https://squareup.com/ (mobile credit card reader).

55. *Frequently Asked Questions*, *supra* note 53; *Mobile Payments*, *supra* note 27, at 2095.

56. *Frequently Asked Questions*, *supra* note 53.

57. *Mobile Payments*, *supra* note 27, at 4.

58. *Id.*

59. MAHIL CARR, MOBILE PAYMENT SYSTEMS AND SERVICES AN INTRODUCTION 4, *available at* http://www.mpf.org.in/pdf/Mobile%20Payment%20Systems%20and%20Services.pdf.

ferring money, but they do little to increase the security of banking mobile applications as they are used on an everyday basis.

B. State of Current Cyber Security Law

There are currently "more than 50 federal laws that govern some aspect of cybersecurity law" in the United States.[60] There is, however, no single agency responsible for cyber security, with participating agencies ranging from the Secret Service[61] (financial systems), to the Federal Trade Commission and Federal Communications Commission (consumer privacy protection),[62] the Federal Energy Regulatory Commission (energy law),[63] and even to the Food and Drug Administration (health care security).[64] Additionally, many states have enacted their own regulatory guidelines, muddling the requirements of cyber security even further from the point of view of businesses.[65]

1. Federal Laws

There have been attempts at retaliating against hackers and improving the security of existing Internet infrastructure.[66] Congress also seems to understand that the government has the duty to encourage the devel-

60. Jonathan S. Fled et al., *Coping with Evolving US, State Cybersecurity Rules*, CORP. COUNS. (May 12, 2014), http://www.corpcounsel.com/id=1202654946074/Coping-With-Evolving-US-State-Cyber%20security-Rules?slreturn=20160024215821; *e.g.*, Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996); Gramm–Leach–Bliley Act, 15 U.S.C. §§6801–6827 (1999); Federal Information Security Management Act, 15 U.S.C. §§ 3541-3549 (2002).

61. Wallace, *supra* note 6.

62. *See, e.g.*, F.T.C. v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2013 WL 1222491, at *3 (D. Ariz. Mar. 25, 2013) (discussing whether alleged security flaws are obvious, implying the existence of ambiguities in cyber security requirements of companies); *Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau*, FED. COMM. COMMISSION (Oct. 14, 2015), http://transition.fcc.gov/pshs/about-us/cybersecurity-communications-reliability-division.html.

63. *Cyber & Grid Security*, FED. ENERGY REG. COMMISSION, http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp (last updated Nov. 20, 2014) (highlighting the FERC's authority in managing energy-related cyber security).

64. Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139, 163–64 (2014) (noting the Food and Drug Administration's ("FDA") foray into cyber security regulation and its decision to start imposing cyber security requirements on medical device manufacturers).

65. *See* Lumsden, *supra* note 1, at 173. For more information on at least twenty-nine states that have introduced security breach bills in 2015, see *2015 Security Breach Legislation*, NAT'L CONF. OF ST. LEGISLATURES (Oct. 22, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx [hereinafter *Security Breach Legislation*]. *See also* Ian McKendry & Rachel Witkowski, *Battle Over Cyber Bill Reveals Fissure Between States and D.C.*, AM. BANKER (Mar. 18, 2015), http://www.americanbanker.com/news/law-regulation/battle-over-cyber-bill-reveals-fissure-between-states-and-dc-1073316-1.html (noting issues with a Cyber Bill, including complaints that "the existing regulatory regime is too fractured" and that "agencies like the FTC and the Federal Communications Commission need a clearer mandate to oversee security standards").

66. *Protecting Your Personal Data: How Law Enforcement Works with the Private Sector to Prevent Cybercrime: Field Hearing Before the Subcomm. On Cybersecurity, Infrastructure Protection, and Security Techs. of the H. Comm. on Homeland Security*, 113th Cong. 7–16 (2014) (statement of Ari Baranoff, Assistant Special Agent in Charge, Criminal Investigative Division, United States Secret Service).

opment of security-enhancing technologies, and while it may be necessary "to give law enforcement the tools it needs to do its job in the 21st century . . . [a]t the same time, we need to strike the correct balance to protect individuals' civil liberties and privacy on the Web."[67] Even so, recent hackings at a number of large retailers indicate that federal laws have not even been able to provide "uniform practices for alerting customers in the event of a breach."[68] Protecting individuals' cyber-privacy would seem to be a step. Fortunately, there are laws that attempt to do just that.[69]

One federal law that governs cyber security has a broader purpose of protecting consumer financial privacy. The Gramm-Leach-Bliley Act ("GLBA"), meant to remove barriers to the merging of financial institutions, also had an effect on cyber security by creating more restrictions and obligations regarding nonpublic personal information.[70] For example, the Gramm-Leach-Bliley Act put limits on the sharing of information for purposes such as telemarketing and "marketing through electronic mail."[71] The Act, however, also made it clear that states could provide even greater protection consumer financial privacy, making financial institutions subject to even more obligations and restrictions, which continue to vary from state to state.[72] This has led to companies being fined by states for breaches in security like "simple and unsophisticated" breaches.[73]

Another federal law that aims to protect consumer privacy does so by regulating mobile marketing, applying section five of the Federal Trade Commission Act and prohibiting "unfair or deceptive practices" in the mobile arena.[74] Although the Federal Trade Commission Act does not specifically account for consumer privacy in mobile technology, the Federal Trade Commission has recognized "that mobile technology presents unique and heightened privacy and security concerns,"[75] and have

67. *Internet Denial of Service Attacks and the Federal Response: Joint Hearing on Before the Subcomm. on Crime of the Comm. on the Judiciary and the Subcomm. on Crim. Just. Oversight*, 106th Cong. 39–41 (2000) *available at* http://commdocs.house.gov/committees/judiciary/hju67303.000/hju67303_0f.htm (prepared statement of John Conyers, Jr., Ranking Member, Representative from Michigan) [hereinafter *Denial of Service*].

68. *Obama: Companies Should Tell Customers of Data Hacks Within 30 Days*, CHI. TRIB. (Jan. 1, 2015), http://www.chicagotribune.com/news/nationworld/chi-obama-customer-data-hacks-20150111-story.html; Jack Gillum, *Obama's Cybersecurity Proposals Part of Decade-Old Programs*, WAVY.COM (Jan. 13, 2015, 5:28 PM), http://wavy.com/2015/01/13/obamas-cybersecurity-proposals-part-of-decade-old-programs/.

69. *See, e.g.*, 15 U.S.C. §§ 6801–09 (2012) (federal law functioning to protect consumer privacy).

70. *Id.*

71. 15 U.S.C. § 6802(d) (2012).

72. 15 U.S.C. § 6807(b) (2012); *Security Breach Legislation*, *supra* note 65.

73. *E.g.*, BBR Staff Writer, *Connecticut Attorney Fines Citi over Credit Card Data Breach*, BANKING BUS. REV. (Sept. 3, 2013), http://cards.banking-business-review.com/news/connecticut-attorney-fines-citi-over-credit-card-data-breach-030913.

74. 15 U.S.C. § 45(a) (2012); *Prepared Statement*, *supra* note 29, at 5.

75. *Prepared Statement*, *supra* note 29, at 10.

attempted to enforce consumer privacy by bringing suit against companies that deal with large amounts of non-public information.[76]

One such case against Twitter alleged lapses in the company's data security that allowed hackers unauthorized access to private user information.[77] Twitter was thereafter required to maintain reasonable security and obtain independent audits of its security practices.[78] Given the mobile nature of Twitter it is expected that the Federal Trade Commission would want to require more of Twitter's data security measures.[79]

Another set of laws designed in part to help regulate cyber security is the Computer Fraud and Abuse Act.[80] This set of laws was enacted to criminalize unauthorized access to computers, but has grown from its narrow interpretation to one covering almost any computer with a connection to the Internet, no longer requiring that the computer be "exclusively for the use of the Government" or financial institutions.[81]

2. Government Agencies

In addition to these federal laws, various agencies within the Department of Homeland Security have been assigned cyber security responsibilities.[82] Within the Department of Homeland Security, within the National Protection and Programs Directorate, is the Office of Cybersecurity and Communications ("CS&C"), responsible for "enhancing security, resilience, and reliability of the Nation's cyber and communications infrastructure."[83] CS&C then has five divisions, one of which is the National Cybersecurity and Communications Integration Center ("NCCIC").[84] Next, the NCCIC is comprised of four branches, including the United States Computer Emergency Readiness Team ("US-CERT").[85] A survey of the US-CERT publications available on the US-CERT website lists, among other titles, "Cyber Threats to Mobile Phones" and "Banking Securely Online."[86] These publications offer ad-

76. *Id.* at 12.

77. *Id.*

78. *Id.* at 12–13.

79. *Id.*; *New Compete study: Primary mobile users on Twitter*, TWITTER (Feb. 11, 2013, 2:28 PM), https://blog.twitter.com/2013/new-compete-study-primary-mobile-users-on-twitter.

80. 18 U.S.C. § 1030 (2012).

81. *Id.*; Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561, 1564–68 (2010) (discussing the development of the Computer Fraud and Abuse Act).

82. Promoting Private Sector Cybersecurity Information Sharing, Exec. Order No. 13,691, 80 Fed. Reg. 9,349, 9,349–50 (Feb. 13, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

83. *Office of Cybersecurity and Communications*, DEP'T OF HOMELAND SECURITY (Oct. 27, 2015), http://www.dhs.gov/office-cybersecurity-and-communications.

84. *Id.*

85. *About the National Cybersecurity and Communications Integration Center*, DEP'T OF HOMELAND SECURITY (Sept. 30, 2015), http://www.dhs.gov/national-cybersecurity-communications-integration-center.

86. PAUL RUGGIERO & JON FOOTE, U.S. COMPUTER EMERGENCY READINESS TEAM, CYBER THREATS TO MOBILE PHONES (2011), https://www.us-cert.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf; U.S. COMPUTER EMERGENCY READINESS TEAM, BANKING

vice like, "[w]hen choosing a mobile phone . . . [a]sk the service provider if the device offers file encryption."[87] In regard to online banking, the bulleted tips include "protect your computer," and "if your account is compromised, take swift action."[88] While this advice is not bad advice, it is hardly the type of information that would have much of an impact on the nation's cyber security, especially considering that the people these resources are most likely to help would have trouble navigating through the website. The scope of the various governmental agencies and departments seems too broad to positively impact cyber security and its developments.

3. Attempts at Standardization

On top of everything that Congress and various agencies have contributed, the Obama Administration has focused standardization of cyber security and has attempted to remedy this issue through a proposal called the National Strategy for Trusted Identities in Cyberspace ("NSTIC").[89] This strategy, announced in April 2011, calls for a collaboration between the Federal Government and the private sector to prevent cybercrimes and fraud by consolidating passwords and providing a way for consumers to identify themselves on the Internet.[90]

Additionally, a number of states have passed laws with varying levels of obligations.[91] Although the differences among state laws will not be covered in this Note, literature on the privacy and cyber security laws abounds.[92] For purposes of this Note, it is enough to understand that cyber security laws vary from state to state, resulting in a lack of standardization for companies that deal with cyber security, among other areas of compliance. Not to be outdone, Congress has proposed a bill to create a national breach notification standard in the hopes of federal standardization.[93]

As a complement to this bill, President Barack Obama signed an Executive Order[94] on cyber security information sharing that establishes Information Sharing and Analysis Organizations ("ISAOs"):[95] private or

SECURELY ONLINE (2008), https://www.us-cert.gov/sites/default/files/publications/Banking_Securely_Online07102006.pdf [hereinafter BANKING SECURELY ONLINE].

87. Ruggiero & Foote, *supra* note 86, at 3.

88. BANKING SECURELY ONLINE, *supra* note 86, at 1.

89. David Kravets, *Obama Calls for Secure Online-Identity System*, WIRED (Apr. 15, 2011, 4:39 PM), http://www.wired.com/2011/04/obama-online-security/; *National Strategy for Trusted Identities in Cyberspace*, WHITE HOUSE (Apr. 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf [hereinafter *National Strategy*].

90. *National Strategy*, supra note 89.

91. *See supra* note 65.

92. *Id.*

93. Mckendry & Witkowski, *supra* note 65.

94. Promoting Private Sector Cybersecurity Information Sharing, Exec. Order No. 13,691, 80 Fed. Reg. 9,349, 9,349–50 (Feb. 13, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

95. Daren M. Orzechowski, *President Obama Issues Executive Order on Cybersecurity Information Sharing*, WHITE & CASE (Mar. 6, 2015), http://www.whitecase.com/publications/article/

public entities that want to share information related to cyber security risks by collaborating with other organizations or sectors.[96] The Executive Order also designates the National Cybersecurity and Communications Integration Center as a "critical infrastructure protection program," and tasks it with collaborating and coordinating with the ISAOs to share information related to cyber security risks and to strengthen information security systems.[97] The Executive Order also provides for a "nongovernmental organization to serve as the ISAO Standards Organization ("SO"), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs."[98] The SO is to be selected through a competitive process whereby the SO "demonstrate[s] the ability to engage and work across the broad community of organizations engaged in sharing information related to cyber security risks and incidents."[99] This is both a large-scale and small-scale project; the scope of the Executive Order is large in that it attempts to create standardization across different sectors and industries,[100] but limited because it is only standardizing the sharing of information.[101] A more tailored approach could be taken.[102]

C. State of Current Affairs

This subpart explores recent events within the private and government sectors as they utilize the existing security systems under the watch of current laws and regulations. With the recent press coverage of security breaches,[103] it is clear that there is a need for government agencies and private businesses to increase security to protect consumers as well as themselves.[104] The government is clearly aware of the need for cyber security,[105] and businesses are becoming more aware of the need as well.[106]

president-obama-issues-executive-order-cybersecurity-information-sharing#.VQoipY7F80x ("The Executive Order is intended to complement the Administration's cyber threat information sharing legislative proposal released last month . . . .").

96. Exec. Order No. 13,691, 80 Fed. Reg. at 9,349.

97. *Id.* at 9350.

98. *Id.*

99. *Id.*

100. *Id.* at 9349 ("ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.").

101. *Id.*

102. *See infra* Part IV.C.

103. *See supra* notes 6–9 and accompanying discussion for examples of data breach press coverage and frequency.

104. *See e.g.*, Brian Krebs, *DDoS Attack on Bank Hid $900,000 Cyberheist*, KREBS ON SECURITY (Feb. 19, 2013, 9:03 AM), http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyber heist/ (describing a cyber attack that disabled a regional financial institution's website and transferred more than $900,000 out of corporate accounts); *see also* CISCO, *supra* note 49, at 9 http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

105. *See* Gillum, *supra* note 68 (discussing the history of cyberthreat warning centers and reporting President Obama's cyber security proposals in light of recent attacks).

106. SILICON VALLEY BANK, CYBERSECURITY SURVEY: IMPACT ON INNOVATION (2013), *available at* http://www.svb.com/pdf/cybersecurity-report/.

In one survey of businesses, a majority of respondents said they believed cyber security was a serious threat to their data, with fifty-one percent rating the threat to business interruption as serious or very serious.[107] Despite the increased awareness of potential threats, it seems the government is not shielded from cyber security snafus,[108] and financial institutions are not making visible efforts to protect themselves from cyber threats.[109]

1. Government

Even with the implementation of cyber security-measures and a number of related Executive Orders,[110] the government does not appear to be much better than private companies in navigating cyber security. When President Obama's new health care system launched in September 2013, the registration websites were flooded by uninsured Americans, resulting in crashed websites and servers in a number of states.[111] The New York website, funded in part by more than $100 million in federal grants, was less problem-ridden than the federal website.[112] The federal website had issues validating identities (i.e., failing to realize two entries with the same social security number were the same person) among other user-interface problems.[113] Even though these and other performance issues were "problems that a good website developer knows to avoid,"[114] they

107. *Id.* at 1.

108. "Snafu" originated as a military acronym for "situation normal: all fouled up," indicating that the situation was bad but in a normal state of affairs. MERRIAM-WEBSTER DICTIONARY (last visited Mar. 16, 2015), *available at* http://www.merriam-webster.com/dictionary/snafu. Its use is particularly appropriate in this context because while the government's health care website was "fouled up," the cyber security issue was not innately threatening; things were still "normal." *See infra* Part II.C.1.

109. *See, e.g.*, Wallace, *supra* note 6; Matthew Goldstein et al., *Cyberattack at JPMorgan Chase Also Hit Website of Bank's Corporate Race*, N.Y. TIMES DEALBOOK (Oct. 15, 2014, 10:01 PM), http://dealbook.nytimes.com/2014/10/15/cyberattack-at-jpmorgan-chase-also-hit-website-of-banks-corporate-race/ (providing another recent example of a cyber security breach despite high-profile occurrences in the past year).

110. *See, e.g.*, Promoting Private Sector Cyber security Information Sharing, Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (Feb. 13, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

111. Glenn Blain & Leslie Larson, *The Demand for Obamacare Overwhelmed the Servers and Crippled the System on its First Day*, NEW YORK DAILY NEWS (Oct. 1, 2013, 11:03 PM), http://www.nydailynews.com/news/politics/obamacare-overwhelmed-servers-crippled-system-day-1-article-1.1473447 ("President Obama's new health care system got off to a rocky start Tuesday as a flood of Web traffic jammed servers and crashed websites in many states, leaving countless insurance seekers out in the cold.").

112. Glenn Blain, *New York's Health Exchange One of Few Obamacare Success Stories*, DAILY NEWS (Dec. 1, 2013, 6:34 AM), http://www.nydailynews.com/news/politics/ny-health-exchange-obamacare-success-stories-article-1.1533961 ("New York developed its exchange using $370 million in federal grants, about a third of which was devoted to the information systems.").

113. Anthony Wing Kosner, *Obamacare's Website is Crashing Because Backend Was Doomed In The Requirements Stage*, FORBES (Oct. 21, 2013, 8:50 AM), http://www.forbes.com/sites/anthonykosner/2013/10/21/obamacares-website-is-crashing-because-backend-was-doomed-in-the-requirements-stage/.

114. Dan Verton, *Decoding* healthcare.gov *Security*, FEDSCOOP (Oct. 17, 2013, 1:35 PM), http://fedscoop.com/decoding-healthcare-gov-security.

were not avoided and some people who encountered these problems were simply told to try again in a week.[115]

The federal website also had major vulnerabilities potentially stemming from the "speed at which the highly complex, transaction-oriented site was developed and the last-minute nature of the security audits and certifications."[116] In order to build a system that did not have to store personal information, the federal website required constant access to seven different databases, including those used by the Social Security Administration and the Department of Homeland Security.[117] However, in providing for this security feature, the federal website exposed itself to a number of other threats by failing to include certain safeguards and validations.[118]

In a more recent incident, the State Department suffered a security breach affecting its unclassified networks,[119] and has asked Congress for $10 million for "cyber enhancements," which would cover the "replacement of obsolete operational infrastructure" as well as a re-architecting of the classified and unclassified networks that "mitigates known security vulnerabilities."[120] While such attacks are not surprising, the Department of State has received a failing score on a cyber security assessment for fiscal year 2014 (and 2013 and 2012) based on the eleven cyber security program areas.[121]

In a report compiled by the Office of Management and Budget, the Department of State received a zero percent in fiscal year 2014 for "strong authentication" implementation, indicating the State Department needs to improve its methods of verifying personal identities.[122] Indeed, the State Department does not yet require anyone to use the two-step Personal Identity Verification that was made mandatory by a Presidential Directive in 2004[123] and plans on achieving full compliance by January 2018.[124] The State Department also does not encrypt its emails or

115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. Aliya Sternstein, *State Says it Needs to Rebuild Classified Computer Networks After Hack*, NEXTGOV (Mar. 10, 2015), http://www.nextgov.com/cybersecurity/2015/03/state-rebuild-classified-computer-networks-after-hack/107157/.
120. SECRETARY OF STATE, DEPARTMENT OF STATE CONGRESSIONAL BUDGET JUSTIFICATION APPENDIX 1: FISCAL YEAR 2016 69 (2015), *available at* http://www.state.gov/documents/organization/236393.pdf [hereinafter BUDGET APPENDIX].
121. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, ANNUAL REP. TO CONGRESS: FEDERAL INFORMATION SECURITY MANAGEMENT ACT 86 (2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf [hereinafter ANNUAL REPORT]. The assessment is carried out by each agency's Inspectors General and is reported to the Office of Management and Budget where it is compiled and sent to Congress in an effort to improve cyber security within the Federal system. *Id.* at 6, 26.
122. ANNUAL REPORT, *supra* note 121, at 6, 20.
123. *Id.* at 62, 91; Homeland Security Presidential Directive/HSPD-12—Policy for a Common Identification Standard for Federal Employees and Contractors, 2 PUB. PAPERS 1765 (Aug. 27, 2004), *available at* http://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2-doc-pg1765.pdf.
124. BUDGET APPENDIX, *supra* note 120, at 61.

scan for malware in remote access connections.[125] Fortunately, other agencies have been receiving better cyber security assessment scores, and some have even improved since 2012.[126]

In light of these reports, it is easy to understand how Hillary Clinton, former Secretary of State, could have solely used a personal email account throughout her four years in the State Department.[127] Even in her position of power, Mrs. Clinton overlooked potential cyber security issues, which is becoming the mindset of the average American person.[128]

2. Banks and Individuals

Individuals are likely the ones most affected by security lapses in mobile banking applications, but are also least likely to change their habits.[129] Whether that is due to low potential loss and indifference from having low checking account balances or a misplaced trust in the banking industry, these habits do not seem to be moving towards safer and more secure practices and are even penetrating the general security practices of high-level government officials.[130]

A security analysis of mobile banking apps for iOS devices (Apple's iPhone operating system) from sixty financial institutions has determined that many of these apps are vulnerable to attacks and did not take necessary security measures in dealing with sensitive information.[131] Problems with these applications included unsecured server communications and data storage, vulnerabilities in the code, failure to authenticate certificates, and running on phones despite the phones being jailbroken.[132]

Although the tested banking applications typically used SSL encryption, ninety percent of the tested applications were found to be initiating non-encrypted connections, forty percent did not validate the authenticity of certificates from the server, and half of them were accessible through a web interface that made the phones more vulnerable to JavaScript injections seeking to steal login information.[133] With millions of people using mobile banking applications, these applications that exude

125. ANNUAL REPORT, *supra* note 121, at 54–55.

126. *Id.* at 28 (indicating an assessment score of 42%).

127. *See* Michael S. Schmidt, *Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules*, N.Y. TIMES (Mar. 2, 2015), http://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html.

128. *Id.*

129. D'Innocenzio, *supra* note 10; *see also Consumer Survey*, *supra* note 11 (finding that "consumers are careless about password creation" and "believe they are safe," further exposing many businesses to data or security breaches).

130. *See* D'Innocenzio, *supra* note 10*; see also* Schmidt, *supra* note 127.

131. Constantin, *supra* note 41.

132. *Id.* Electronic devices often have software that prevents the user from using certain unauthorized software. Jailbreaking is the process of hacking a device to get past that layer of software, giving you more control over the device. Because the iPhone is limited to software downloaded from the Apple App Store, the term "jailbreaking" was coined "in reference to breaking the iPhone out of Apple's App Store 'jail.'" Mike Keller, *Geek 101: What is Jailbreaking?*, PCWORLD, http://www.pcworld.com/article/249091/geek_101_what_is_jailbreaking_.html.

133. Constantin, *supra* note 41.

convenience while hiding cyber security vulnerabilities are a major concern.[134]

Financial institutions, however, are not the only source of cyber security issues in the mobile arena. According to a survey of consumer password habits from 2012, sixty-one percent of consumers reuse passwords among multiple websites and forty-four percent of consumers change their password only once a year or less.[135] Possibly reassuring is the fact that only twenty-one percent of consumers have had an online account compromised.[136] Perhaps more indicative of problems to come: eighty-nine percent of consumers felt secure with their current password management and use habits.[137]

III. ANALYSIS

The government has taken steps towards securing the nation's critical infrastructure, but it is clear that there is still more progress to be made.[138] Various proponents of cyber security have suggested changes and remedies regarding cyber security as a whole, but many of these ideas ask too much of the government. Given the colossal task of improving cyber security, it should start with cyber security in financial institutions and mobile banking. Part III will analyze currently enacted federal laws and the potential efficacy of other recommendations for improving cyber security and their impact on security in the mobile banking industry. It will then analyze the need for cyber security developments specifically in the financial industry.

A. Government Remedies

Current cyber security laws are too focused on protecting consumers, and although there is a need for standardization, there has not been a consensus on how to go about creating a federal standard.[139] The structure put in place by the government for controlling cyber security is not completely ineffectual, but it is redundant, unorganized, and does not ensure the best future for cyber security in the United States.[140] From fed-

134. Robin Sidel, *Banks Make Smartphone Connection*, WALL STREET JOURNAL (Feb. 12, 2013, 12:01 AM), http://www.wsj.com/articles/SB10001424127887323511804578298192585478794 ("J.P. Morgan Chase & Co., which started offering mobile banking in 2009, said that it has some 13 million customers who use its mobile services.").

135. CONSUMER SURVEY, *supra* note 11. Particularly troubling is the fact that 18 to 24-year-olds are more likely to reuse passwords than any other age group, at seventy-six percent. *Id.*

136. *Id.*

137. *Id.*

138. *See supra* Part II.C.

139. *See* Mckendry & Witkowski, *supra* note 65 ("Among the many complexities standing in the way of data security legislation, now add to the mix disagreements between state and federal authorities over who is better equipped to oversee security standards.").

140. Gillum, *supra* note 68 ("Some of the warning centers, such as the ones protecting banks and computer companies, are highly regarded. But others have been marked by uneven cooperation among members and confusion about roles during a cyberattack.").

eral laws to regulations and even state laws, there is room for improvement if not standardization. This subpart analyzes federal laws, current government actions, and recent suggestions.

1. Federal Laws

Laws like the Gramm-Leach-Bliley Act are too broad. The Gramm-Leach-Bliley Act falls under the purview of the Federal Trade Commission,[141] but as expected in cyber security regulation, compliance of this Act in certain cases can also be enforced by other agencies or departments like the United States Department of the Treasury.[142] The GLBA allows states to openly dictate what privacy laws companies must follow,[143] resulting in too much variance across the country. This also allows for laws and precedents that do not help alleviate the cyber security problem or even incentivize financial institutions to improve their cyber security. In the case of Citibank in Connecticut, a security breach occurred through a vulnerability that had gone undetected for two years and affected roughly 360,000 customers.[144] Citibank paid a $55,000 fine and was subjected to a third-party security audit.[145] Despite state laws, Citibank's credit card account system was left open to even "simple and unsophisticated" attacks.[146] Connecticut's laws are not effectively protecting consumers' financial privacy nor are they moving institutions to implement more intensive security measures.

Also, laws like the Computer Fraud and Abuse Act that criminalize certain cyber security-related actions, are in need of further changes. As the interpretation of these kinds of laws continues to expand their scope, the rights of normal citizens and the legality of their actions become increasingly vague.[147] Taking, for example, the case of Aaron Swartz, you have a young computer programmer and entrepreneur who gained access to M.I.T.'s network as an authorized guest and proceeded to download thousands of academic articles.[148] As this was neither "hacking" nor "breaking in," the Computer Fraud and Abuse Act should not have applied, yet multiple allegations were brought against Swartz under the Computer Fraud and Abuse Act, alleging that Swartz obtained "information whose value exceeded $5,000," and resulting in an indictment for

141. 15 U.S.C. § 6822(a) (2012).

142. 15 U.S.C. § 6822(b) (2012).

143. 15 U.S.C. § 6807 (2012).

144. Sean Sposito, *Connecticut Attorney General Fines Citibank for Data Breach*, AMERICAN BANKER (Sept. 3, 2013, 8:42 PM), http://www.americanbanker.com/issues/178_170/connecticut-attorney-general-fines-citibank-for-data-breach-1061765-1.html.

145. BBR Staff Writer, *supra* note 73.

146. *Id.*

147. Kerr, *supra* note 81 (discussing the vagueness of the Act).

148. Tim Wu, *Fixing the Worst Law in Technology*¸ THE NEW YORKER (Mar. 18, 2013), http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology; Indictment at 11-12, United States v. Swartz, No. 1:11-cr-10260 (D. Mass. July 14, 2011), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/217117/united-states-of-america-v-aaron-swartz.pdf [hereinafter Indictment].

up to thirty-five years in prison.[149] Before the multiple allegations were cleared up, Aaron Swartz committed suicide.[150] Although Swartz's death may or may not stem from allegations brought under the Computer Fraud and Abuse Act, it is clear that the Act as it is being implemented now does little for the progress of cyber security and even less for the protection of consumer privacy.

In attempting to control cyber security and to protect consumer privacy by criminalizing certain actions, the government has enacted a law that is overinclusive and criminalizes many actions of ordinary people.[151] Rather than deterring the hackers and actual persons of interest in the cyber arena, the Computer Fraud and Abuse Act expands its purview to bringing charges against anyone who uses a computer.[152] This progression of the law, although born of a sensible nature,[153] does little to aid in the protection of cyber security, both that of the nation and of private financial institutions.[154] Also distinguishing itself from federal laws enacted to protect consumer privacy, the Computer Fraud and Abuse Act does little to aid companies in protecting consumer data.[155]

Some members of Congress and academics have pushed for amendments to the Computer Fraud and Abuse Act, commonly known as "Aaron's law," but this Act has seen amendments before.[156] Furthermore, proposed amendments following Swartz's suicide only proposed a change in some of the language, providing an exception for "terms of service" violations.[157] Federal laws should not be focused on catching criminals, and amendments to these laws should not result in mere exceptions for select groups of people.[158] As members of Congress have pointed out in the past, "[t]argeting cybercrime with up-to-date criminal laws and tougher law enforcement is only part of the solution."[159] Laws like the Computer Crime Enforcement Act have been enacted, attempt-

149. Wu, *supra* note 148; Indictment, *supra* note 148, at 11–12.

150. Michael Martinez, *Internet Prodigy, Activist Aaron Swartz Commits Suicide*, CNN (Mar. 7, 2013, 11:41 AM), http://www.cnn.com/2013/01/12/us/new-york-reddit-founder-suicide/.

151. Kerr, *supra* note 81, at 1562. ("The CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access will render it unconstitutional. Such interpretations would either provide insufficient notice of what is prohibited or fail to provide guidelines for law enforcement in violation of the constitutional requirement of Due Process of the law.").

152. *Id.* at 1587.

153. *Id.* at 1561 ("In 1984, Congress enacted a narrow statute designed to criminalize unauthorized access to computers.").

154. *See generally id.* (mentioning that the changes being made to the Computer Fraud and Abuse Act are of little use and that the Act should be void for vagueness).

155. *See generally id.* (mentioning that the changes being made to the Computer Fraud and Abuse Act are of little use and that the Act should be void for vagueness).

156. Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013); Kerr, *supra* note 81, at 1563–71 (providing overview of past amendments to the Act).

157. Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013); Mark Murfin, Note, *Aaron's Law: Bringing Sensibility to the Computer Fraud and Abuse Act*, 38 S. ILL. U. L.J. 469, 480 (2014).

158. *Id.* at 481.

159. *Denial of Service*, *supra* note 67 (prepared statement of Patrick J. Leahy, U.S. Senator from Vermont).

ing to find other parts of the solution.[160] Unfortunately, some parts of the solution remain to be found.[161] These laws instead should find those like Swartz who have a passion for computer programming, and incentivize the development of more secure systems.

2. Government and Private Firm Cooperation

People seem to agree that the government has a duty to work with the private sector to improve cyber security, but it has not proven to be a simple task.[162] Even the strategy set forth by the Obama administration is not without flaws.[163] While consolidating passwords and creating a single form of identification on the Internet may be helpful and useful to consumers, it could also be catastrophic; from the viewpoint of an individual consumer, this is a great idea only until something goes wrong. This has been compared by some to losing your entire wallet instead of just your driver's license or your credit card.[164] While this strategy aims to reduce the fear of identity theft, it only compounds the problems if something does go wrong.[165]

The government has also acknowledged that this project will not be a quick solution and has laid out five- and ten-year benchmarks.[166] Since its inception, this strategy has moved many private firms to implement methods like multi-factor authentication to begin improving cyber security by preventing unsophisticated attacks.[167] While this strategy acknowledges the problems that are becoming apparent within cyber security,[168] in the end, it attempts to solve cyber security problems by gathering all the valuables and placing them in a locked jar. The only problem arises when someone runs off with the entire jar. This solution focuses too much on making consumers feel safe instead of focusing on increasing security measures. The disarray of websites and passwords may actually help increase security for consumers. Despite all its flaws, this strategy is

160. Computer Crime Enforcement Act, 42 U.S.C. §§ 3711–3713 (2012) (providing grants for states to improve education, training, enforcement, and prosecution of computer crimes).

161. *See, e.g.*, *infra* Part IV.A.

162. *See Denial of Service*, *supra* note 67 (prepared statement of Patrick J. Leahy, U.S. Senator from Vermont) ("The government has a responsibility to work with those in the private sector to assess those vulnerabilities and defend them."); Grant Gross, *New Study Calls for Cybersecurity Overhaul in U.S.*, PCWORLD (last visited Jan. 28, 2016), http://www.pcworld.com/article/183658/article.html ("The U.S. government and private businesses need to overhaul the way they look at cyber security, with the government offering businesses new incentives to fix security problems, the Internet Security Alliance said."); *see also* Promoting Private Sector Cybersecurity Information Sharing, Exec. Order No. 13,691, 80 Fed. Reg. 9,349, 9,349 (Feb. 13, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf. (designating a specific government agency to collaborate with the private sector).

163. Kravets, *supra* note 89; *see National Strategy*, *supra* note 89.

164. Kravets, *supra* note 89.

165. *Id.*; *National Strategy*, *supra* note 89.

166. Kravets, *supra* note 89; *National Strategy*, *supra* note 89.

167. Jeremy Grant, *It's Not Just About Security; Identity is the Great Enabler*, NAT'L STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE NOTES (OCT. 23, 2014), https://nstic.blogs.govdelivery.com/2014/10/23/its-not-just-about-security-identity-is-the-great-enabler/.

168. *National Strategy*, *supra* note 89.

a step towards standardizing and increasing the security measures that are required of financial institutions.

In perhaps another step forward, Congress has attempted to address cyber security by proposing a national breach notification standard that would require private entities to notify affected individuals and third parties of the breach.[169] While this attempt to move towards a federal standard is sensible, it has a smaller effect than it appears, especially in regard to mobile banking and financial institutions. Although section 3 of the proposed bill requires breach notification, financial institutions subject to the GLBA are automatically deemed to be in compliance with some parts of the proposed legislation.[170] Further muddling the attempt at standardization, section 5 delegates enforcement of sections 2 and 3 to the Federal Trade Commission as violations of the Federal Trade Commission Act.[171]

Two problems arise from bills crafted in this manner. First, the proposed legislation would preempt stronger breach notification laws in several states while achieving only a pseudo standardization,[172] and second, the legislation would not provide any greater security to financial institutions or users of mobile banking applications than already exists. Although the thought of a federal standard is not a bad one, the standards are set too low, leaving some advocates frustrated with the lack of significant cyber security laws being enacted.[173]

Having so many government agencies promulgating rules on cyber security also leads to varying punishments that could sometimes seem drastic.[174] For example, Title 15 of the United States Code allows for a fee or imprisonment of up to ten years for certain violations of federal privacy law.[175] Congress has proposed other laws, one that prohibits certain practices relating to spyware and has penalties of up to $3 million[176]

169. Data Security, and Breach Notification Act, S. 177, 114th Cong. § 3 (2015).

170. *Id.*

171. 15 U.S.C. § 57(a)(1)(B) (2012).

172. Grant Gross, *Proposed data breach notification bill criticized as too weak*, PCWORLD (Mar. 18, 2015, 11:45 AM), http://www.pcworld.com/article/2898932/proposed-data-breach-notification-bill-criticized-as-too-weak.html ("Proposed legislation that would require U.S. businesses to notify affected customers after data breaches is too weak because it would preempt stronger breach notification laws in several states and it wouldn't cover several classes of data, including geolocation and health information, critics told lawmakers.").

173. Mckendry & Witkowski, *supra* note 65 ("We do, however, have serious concerns that the standards set by this bill are too low . . . ."); James Arden Barnett Jr., *Cyber Security: Fixing Policy with New Principles and Organization*, 2014 WL 2315048 at *1, (2014) ("Almost one hundred bills relating to cyber security have been introduced over the last five years, but no significant legislation has been enacted into law. In frustration over the failure by Congress to exercise its power, the Obama administration launched Executive Order 13636 in February 2013 . . . .").

174. 15 U.S.C. § 6823 (2012) (explaining the criminal penalty of a fine or imprisonment for up to ten years).

175. *Id.*

176. H.R. 29, 109th Cong. §§ 2–4 (2005), *available at* https://www.govtrack.us/congress/bills/109/hr29/text.

and another that allows five years of imprisonment for concealment of any security breach resulting in $1,000 of harm.[177]

What this means for mobile applications is unclear. It still gives financial institutions a large amount of discretion in their security measures. Especially given the loose nature of the Android operating system, efforts like the National Strategy for Trusted Identities in Cyberspace will have varied effects on mobile banking as vigilant institutions implement new strategies and rise to the call of the national strategy, and cost-cutting institutions rely on consumers' savvy and leave their security systems vulnerable to a breach.

3. New "Cyber Security" Agency

Some have advocated the creation of a new government agency to take on the task of centralizing cyber security in the United States.[178] This has the potential to improve cyber security, but there are also some very distinct disadvantages to such a plan. Having an agency dedicated to cyber security—if feasible—could be beneficial, but with the relative speed of technology compared to government action, waiting on an agency would likely mean foregoing any developments in cyber security.[179] Nevertheless, an analysis of the advantages and disadvantages of a cyber security agency sheds light on what should and could be done.

a. Advantages

A single agency in charge of cyber security could provide some benefits to institutions at risk of security breaches. This would create a centralized place where companies could go to understand their requirements regarding cyber security.[180] The agency could also act as a think tank, performing research to enhance cyber security in our nation and advocating security changes and updates, in addition to setting minimum requirements of cyber security.[181] This would not entail creating a single standard of encryption or a specific method of securing sensitive data, which would only serve to metaphorically put all our eggs in one basket.[182] Instead, it would mean companies no longer have to deal with nav-

177. Data Security, and Breach Notification Act, S. 177, 114th Cong. (2015).

178. *See* Lumsden, *supra* note 1.

179. *See* Barnett, *supra* note 173, at *1 ("Almost one hundred bills relating to cyber security have been introduced over the last five years, but no significant legislation has been enacted into law.").

180. *Id.* The Obama administration has done something similar with the launch of the National Institute of Standards and Technology. *Id.* While this division is responsible for some aspects of cyber security, it is a far cry from being in charge of cyber security completely.

181. *Id.* at *4. This is not a task that has been taken on by the NCCIC, NIST or NSTIC, likely due to the enormous scope of the endeavor. *National Cybersecurity and Communications Integration Center*, Department of Homeland Security, http://www.dhs.gov/national-cybersecurity-communications-integration-center (listing responsibilities involving coordination, recovery, and mitigation as opposed to actual development).

182. Tamar Haspel, *Monocrops: They're a Problem, but Farmers Aren't the Ones Who Can Solve It*, THE WASHINGTON POST (May 9, 2014), https://www.washingtonpost.com/lifestyle/food/monocrops-theyre-a-problem-but-farmers-arent-the-ones-who-can-solve-it/2014/05/09/8bfc186e-d6f8-11e3-8a78-

igating regulations from multiple agencies.[183] Assigning this function to a single agency could also preclude some companies from drawing out lawsuits in which the lack of security was clearly underdeveloped.[184] This would affect not only the way companies implement cyber security measures but also the other agencies that currently use resources to deal with companies and their security breaches.[185] This would lighten the load by taking these duties from other agencies and centralizing them in an agency specialized to perform that very function.[186]

A separate agency could also serve as the hub for the collection, analysis, and distribution of cyber threats.[187] Presidents Bill Clinton and George W. Bush have already set the precedent for such centers of information, but the instability and the lack of a proper "home" for this function further advocates for the creation of an agency dedicated to cyber security.[188] The responsibility for cyber threat warning centers was juggled about as bases of operations ceased to exist and the Executive branch went through changes.[189] In the midst of all the shuffling, some positive changes were made that expanded the scope of the warning centers "to cover 16 critical industries," "including *banking*, transportation, *communications*, and energy."[190]

Various industries involved in the cyber security of mobile banking applications are already recognized as areas that need special attention like cyber threat warning centers;[191] an agency dedicated to cyber security would certainly aid in securing mobile banking.

b. Disadvantages

On the other hand, any focus on mobile banking would be lost due to the enormous responsibility given to this hypothetical agency.[192] Despite the possible advantages of creating a new agency to head the movement for improved cyber security, the disadvantages are numerous.

8fe50322a72c_story.html (pointing out that having all your eggs in one basket leaves you vulnerable to a devastating loss).

183. *See supra* Part II.B.2.

184. *See*, *e.g.*, BBR Staff Writer, Connecticut Attorney Fines Citi over Credit Card Data Breach, BANKING BUS. REV. (Sept. 3, 2013), http://cards.banking-business-review.com/news/connecticut-attorney-fines-citi-over-credit-card-data-breach-030913.

185. *See supra* Part II.B.

186. Naturally, the result of allocating all responsibilities to one entity would mean all the other entities would be free of those responsibilities.

187. Gillum, *supra* note 68. (discussing the history and purpose of cyberthreat warning centers).

188. *Id.*

189. *Id.* ("In 2003, President George W. Bush moved responsibility for the warning centers from the FBI's now-defunct National Infrastructure Protection Center to the Homeland Security Department. The warning centers have since been expanded to cover 16 critical industries, and others—such as one covering retail stores—have launched separately.").

190. *Id.* (emphasis added).

191. *Id.*

192. *National Cybersecurity and Communications Integration Center*, DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/national-cybersecurity-communications-integration-center (displaying an organizational chart and breaking down responsibilities, implying these functions cannot all be served by one entity).

Such an agency would lead to bureaucracy, which would further prevent standardization.[193] One thing bureaucracies have in common is a tendency to grow.[194] Thus far, the bureaucratic system has yet to come up with a solution for cyber security, but the solution from a government standpoint is to add more employees, more job titles, and more intermediate, specialized jobs.[195] Looking at the state of similar introductions of new agencies, or even the implementation of the Affordable Care Act,[196] there are a number of problems, some of which were anticipated but others that arose after the start of implementation.[197] If another agency is created to try and centralize cyber security, it is more than likely that unforeseen issues will manifest. Moreover, some of these issues will likely be those often associated with bureaucracies, including reduced innovation, lack of communication as it progresses up the agency ladder, and slower decision making.[198]

A new government agency would also not have the expertise to deal with an issue as complex as our nation's cyber security.[199] In staffing an agency of this nature, finding enough qualified employees would be one problem, but a bigger issue would be drawing the most qualified prospective employees away from the private sector and convincing them to work in the public sector.[200] Drawing from the financial industry, in which "the income gap between financial industry employees and their regulatory counterparts makes it likely that the expertise of regulators will be far less than that of their industry counterparts," any agency created to take on all cyber security-related responsibilities would be noticeably handicapped from the start.[201]

193. *Id.* Standardization cannot be achieved if responsibilities are so widely distributed as the organizational chart depicts. *Id.*

194. *Secretarial Work*, THE ECONOMIST, June 26, 2010, http://www.economist.com/node/16436337 ("Bureaucracies grow faster than they can be pruned.").

195. *See Reforming the Bureaucracy*, USHISTORY.ORG, http://www.ushistory.org/gov/8d.asp (last visited Feb.1, 2016) ("Bureaucracies move slowly. One hand doesn't always know what the other is doing . . . . There are so many agencies organized in such confusing ways.").

196. The Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119–1025 (2010) (codified throughout 26 and 42 U.S.C.). *See supra* Part II.C.1.

197. *E.g.*, Sarah Kliff, *Think Your State Has Obamacare Problems? They're Nothing Compared to Guam*, THE WASHINGTON POST WONKBLOG (Dec. 19, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/12/19/think-your-state-has-obamacare-problems-theyre-nothing-compared-to-guam/.

198. HOWARD P. GREENWALD, ORGANIZATIONS: MANAGEMENT WITHOUT CONTROL 364 (2008).

199. *See* Robert Hinck, *For Hire: Cybersecurity Specialist*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (last visited Feb. 1, 2016), http://csis.org/blog/hire-cybersecurity-specialist ("Only 120 cyber security experts go into government after graduation, but the government is looking to increase that number to a thousand . . . One thing that everyone does agree on is the need for more individuals with a cyber security background.").

200. *Cf.* Steven L. Schwarcz, Regulating Financial Change: A Functional Approach 23–24 (Mar. 2, 2015) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2469467 (reaching similar conclusions about the workforce in the financial industry).

201. *Id.*

It has also been suggested that creating a standardized network creates a natural target.[202] For example, in the financial market network, which was created pursuant to a Congressional mandate, "security has been consistently compromised," and much of the necessary security has been of the reactive variety: waiting for an attack and then developing a fix.[203] Creating a single network of information ensures that hackers know who to target.[204] This along with the notion that the "nature of software development implies that even the best software will be flawed" seems to indicate that a central command for cyber security development may invite some unexpected problems.[205]

There is also an overlap between cyber security and consumer financial privacy that cannot be ignored.[206] With one agency in charge of cyber security and other agencies in charge of privacy, the overlap would result in a messy division of responsibilities. Certain cyber security measures that are already codified would also have to be combed through and altered to ensure the new cyber security agency had the intended authority.

B. Technology

Some have advocated a complete overhaul of the Internet in order to curb hacking.[207] Because current technological advances like HTTP-S are built to work on top of older technologies like TCP/IP, hackers are catching up;[208] it seems only a completely different Internet structure would be able to slow them down.[209]

An advantage of this system would be increased security since having a completely new infrastructure would also mean a completely clean

202. Supriya Sarnikar & D. Bruce Johnsen, *Cyber Security in the National Market System*, 6 RUTGERS BUS. L.J. 1, 17 (2009).

203. *Id.* at 4, 17–18.

204. *See id.* at 17–18.

205. *Id.* at 18.

206. *See supra* Part II.B.1.

207. *See, e.g.*, Parmy Olson, *The Largest Cyber Attack in History Has Been Hitting Hong Kong Sites*, FORBES (Nov. 20, 2014, 10:40 AM), http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/ (noting that there could be no technical solution to the denial-of-service cyber attacks unless the Internet were to be re-architected).

208. *See* AMOROSO, *supra* note 9 (explaining that even long-term suppression of information regarding cyber security infrastructure for the sake of making things more difficult for hackers and third parties is not a reliable means of security "because suppressed information has a tendency to eventually become public"). *But cf.* Jessica Twentyman, *Hackers Kept at Bay by Lack of a Standard Platform*, FINANCIAL TIMES, Feb. 16, 2010, http://www.ft.com/cms/s/182621ca-176a-11df-87f6-00144feab49a,Authorised=false.html?siteedition=uk&_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F182621ca-176a-11df-87f6-00144feab49a.html%3Fsiteedition%3Duk&_i_referer=&classification=conditional_standard&iab=barrier-app("At the same time, he adds, relatively few hackers have the in-depth skills and understanding necessary to create viruses capable of targeting a specific mobile platform."). At least four years have passed since the time this was said, and the skills and understanding of hackers is likely to have increased as mobile platforms have grown more stable.

209. *See* Steve Gold, *Hacking the Internet–Bringing Down Infrastructure*, 8 ENG'G AND TECH. MAG. (Sept. 17, 2013), http://eandt.theiet.org/magazine/2013/09/hacking-the-internet.cfm (explaining that the Internet is not as robust as people think and that the Department of Homeland Security never got around to "raising the security of the Internet's own architecture").

slate. Another advantage would be the increased control since these would likely be run as intranets, possibly requiring identity authentication for initial access.[210]

Unfortunately, the factors that make the Internet so prone to security breaches are also what make the Internet so useful.[211] The massive reach of the Internet and the open access to the worldwide web allow for the accumulation of knowledge that currently exists.[212] The fact that everyone is on the same Internet also provides a level of convenience that would not be possible through a new Internet system.[213] At the extreme end, this would require designing a new infrastructure without using the packet system, which would necessitate assembling a team of engineers to design a structure.[214] This would also be costly and risk having negative results and unknown consequences.[215] Given the rising number of people using cell phones to access the Internet[216] and the millions of people using mobile banking applications, the technology cannot be "upgraded," but the cell phones and mobile application developers cannot be left to their own devices.[217]

Other changes in mobile payment technology, like PAYware, add layers of encryption and hardware on top of the existing security measures, but still fall short of protecting information once a company stores it.[218] As mobile banking becomes more prevalent and Internet-based technology keeps building on itself,[219] the financial industry opens itself up further to cyber security issues.

210. *See* Neil Kokemuller, *The Advantages of Implementing a Corporate Intranet*, HOUSTON CHRONICLE (last visited Feb. 1, 2016), http://work.chron.com/advantages-implementing-corporate-intranet-3285.html (describing the benefits of an intranet within a company).

211. *Denial of Service*, *supra* note 67, at 39–40 (prepared statement of John Conyers, Jr., Ranking Member, Representative from Michigan), *available at* http://commdocs.house.gov/committees/judiciary/hju67303.000/hju67303_0f.htm ("We must acknowledge that the same interconnections that make the Internet so robust also make it vulnerable to attack. The same openness and ease with which people can share information also makes it easier to invade people's privacy.").

212. *Id.*

213. DAVID ALDERSON & KEVIN SOO HOO, CENTER FOR INTERNATIONAL SECURITY AND COOPERATION, STANFORD UNIVERSITY, THE ROLE OF ECONOMIC INCENTIVES IN SECURING CYBERSPACE 7 (Nov. 2004), *available at* http://fsi.stanford.edu/sites/default/files/alderson-soo_hoo-CISAC-rpt_1.pdf.

214. In the aftermath of a security breach, the State Department asked Congress for "$10 million to support 'the necessary rearchitecting' of [its] . . . networks." Sternstein, supra note 119. This level of rearchitecting will still build on top of the existing TCP/IP system, but any large-scale architecting of a replacement internet would likely require even greater funds.

215. *Id.*

216. *New Research*, *supra* note 23.

217. Sidel, *supra* note 134.

218. *See supra* Part II.A.3.

219. *See supra* Part II.A.1.

C. Cyber Security and Financial Systems

The nature of the financial industry invites trouble, and cyber security is similarly prone to its own set of problems.[220] The financial industry—essentially a large pile of money—is a prime target for hackers looking to gain access to financial accounts, especially as the hacking becomes more complex, and infiltrated banks remain oblivious to cyber attacks.[221] Similarly, computer-based technology has always been an ad hoc type of advancement. If a shirt or fashion accessory were only "almost finished," it would probably not be desired by very many people.[222] The opposite seems to be the case with computer-based technology.[223] It is often the newer, "beta" version of software that is most appealing, and operating systems are released with full knowledge—on the part of developers and users—that there will be bugs, patches, and updates.[224] This sole feature of technology makes it seemingly impossible to regulate cyber security; it is so naturally prone to having issues that they are expected even in the absence of outside intervention.[225] It is doubly concerning when this technology is merged with another industry that seems to have similar problems: the financial industry.[226]

Arguments have been made for which industries' cyber security should receive the most attention,[227] but in light of increased cell phone usage and mobile banking,[228] the appeal to hackers of breaking into financial institutions, and the proactive efforts of banking institutions,[229] government efforts should be spent on developing cyber security related to financial institutions.

220. *See* Tom Huddleston, Jr., *In Wake of Banking Hacks, Senate Will Focus on Finance Industry Security*, FORTUNE (Dec. 5, 2014, 3:57 PM), http://fortune.com/2014/12/05/senate-hearing-cyber-attacks-finance/ ("The U.S. government concerned about cybersecurity in the financial sector, which it sees as a prime target for hackers looking to gain access to countless customers' financial accounts and information.").

221. *See* Mae Anderson, *Hackers Steal Up to $1 Billion From Banks, Security Co. Says*, YAHOO! TECH (Feb. 15, 2015), https://www.yahoo.com/tech/s/hackers-steal-1-billion-banks-184427738--finance.html?nf=1; Huddleston, *supra* note 220.

222. *But cf.* countless number of "unfinished" (read fake) handbags purchased.

223. *See* Consumer Electronics Show, *Experience Innovation at CES*, Consumer Technology Association, http://www.cesweb.org/Why-CES/Experience-the-International-CES (explaining why CES is worth attending and implying the appeal of newer, possibly unfinished technology).

224. *See* Russell Kay, *System Development Life Cycle*, COMPUTERWORLD (May 14, 2002, 7:00 AM), http://www.computerworld.com/article/2576450/app-development/system-development-life-cycle.html (explaining the software life cycle that takes in account bugs, fixes, and other programming issues).

225. *See id.* (implying that bugs are to be expected).

226. *See* Brett Scott, *Open Source Hacking*, STIR BLOG, http://stirtoaction.com/open-source-hacking/ (last visited Feb. 2, 2016) (stating that hacking financial systems could cause financial crashes and affect the world economy). Similarities are also drawn between technology systems and financial systems. *Id.*

227. *See, e.g.*, Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats*, 19 B.U. J. SCI. & TECH. L. 319, 319 (2013).

228. *New Research*, *supra* note 23.

229. Jordan Robertson & Michael Riley, *JPMorgan Goes to War*, BLOOMBERG BUSINESS (Feb. 19, 2015, 6:00 AM), http://www.bloomberg.com/news/articles/2015-02-19/jpmorgan-hires-cyberwarriors-to-repel-data-thieves-foreign-powers (reporting JPMorgan Chase's aggressive tactics in investigating its security breaches).

Millions of people currently utilizing mobile banking applications are not likely to stop, and that number will more than likely grow.[230] That, in conjunction with the lack of diligence put into designing mobile applications,[231] raises major concerns and makes banking institutions a prime target for government help. Instead of figuring out the "most critical" industry, cyber security developments should focus on the financial industry.

IV. RECOMMENDATION

It seems that companies are sufficiently aware of the need to increase cyber security.[232] Whether it is to protect themselves or to protect consumer privacy, it makes little difference. There needs to be a more focused approach, however, to improving cyber security. Cyber security regulation has merely been the sideshow to the main attraction of consumer privacy. Only until recently with the massive proliferation of cybercommunications and cybercrimes has the government truly attempted to address the problems in cyber security.[233] This Part recommends narrower, business-oriented regulation and suggests that a single agency dealing with just the financial industry would be an optimal start to the government lending a hand to the private sector with regard to developments in cyber security.

A. Business-Oriented Regulation

One problem with the current regulation of financial institutions is that it comes about largely as a result of laws focused on protecting consumer privacy. There are also few concrete requirements for cyber security specifically in the area of mobile applications.[234] Laws should be written in a way that does not function primarily to protect consumers as this results in harsh results for private companies while achieving little.[235] They should instead aim to protect the financial institutions themselves.[236]

In order to protect financial institutions, regulations should be designed to encourage innovation, incentivizing development of technology.[237] Instead of regulating for the sake of consumers whilst scaring companies from making any changes or bringing any changes to light,[238] new

230. Sidel, *supra* note 134.

231. *See supra* Part II.C.2.

232. *Mobile Payments*, *supra* note 27.

233. *See* Barnett, *supra* note 173, at *1 (arguing that the government has recently proposed more than a hundred cyber security laws while enacting very few of them).

234. *See supra* Part II.B.

235. *See supra* Part III.A.1.

236. *See id.*

237. Barnett, *supra* note 173, at *5.

238. *Cf.* Schwarcz, *supra* note 200, at 18 (analogizing risk management in the financial industry to active cyber security players, there will be a lack of an incentive for companies to actively monitor their systems and develop their own processes).

laws should bolster security by first encouraging self-monitoring within these companies and then self-improvement.[239] These improvements may be better education programs for higher up executives with access to more sensitive information.[240] Improvements to regulations could also extend to changes to the cyber security infrastructure and updating software through collaboration and coordination.[241]

Because so much of business today is conducted electronically, any protection or advancement in cyber security can then also be extended and applied to other businesses that are or have been targets of hackers and have something to lose from a security breach. This would also flow back into protecting the national cyber infrastructure. Naturally, as cyber security improves as a whole, consumers will have even less to worry about in terms of the safety of their electronic transactions.

B. Focused Regulation

Given the current disarray and lack of standardization, Congress should work on focusing regulation as to prevent unnecessary hardship on areas like cell phone security.

One way regulation can be focused is not by reacting to problems by tweaking existing laws—as seen in the case of Aaron Schwartz[242]—but by acting preemptively, seeking out problems in cyber security before they arise, and ensuring that the infrastructure and technology continues to develop. Remaining stagnant only makes it easier for hackers to take advantage of existing security systems.[243] Much like Professor Schwarcz seeks an alternative to the ad hoc, past-focused means of regulating the financial system,[244] the government should regulate the areas related to the cyber security of mobile applications instead of the banking institutions.[245] This can be done by determining what factors surrounding the cyber security of specific areas like banking mobile applications are causing the most cyber security issues and regulating from there.[246]

Now that cell phones have risen to full prominence, having replaced alarm clocks, walkmen, and candles,[247] focused regulation could fall upon

239. Barnett, *supra* note 173, at *5 (drawing comparisons between cyber security and the 9-1-1 system that came about with the help of government regulation but was later incorporated into the industry).

240. *See supra* Part II.C.1.

241. Promoting Private Sector Cybersecurity Information Sharing, Exec. Order No. 13,691, 80 Fed. Reg. 9,349, 9,349 (Feb. 13, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

242. *E.g.*, Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).

243. *Prepared statement*, supra note 29.

244. *See generally* Schwarcz, *supra* note 200, at 8–10 (seeking out factors that impede financial markets that could be regulated to reduce certain problems in that context).

245. *See supra* III.C.

246. Schwarcz, *supra* note 200, at 8–9.

247. Jill Reilly & John Hutchinson, *Pope on a Bus! Francis Shows He's Still a Man of the People as He Hops on Board Minibus to Church on His First Day on the Job*, DAILYMAIL.COM (Mar. 15, 2013, 5:53 PM), http://www.dailymail.co.uk/news/article-2293785/Pope-bus-Francis-shows-hes-man-people-

communications companies.[248] Although cell phone carriers are subject to some government regulations,[249] they are also given protection from things like class-wide arbitrations.[250] Regulating such services would allow a multi-faceted approach[251] to improving the cyber security involved in banking applications. Starting there, this could be transitioned into improving cyber security in other, arguably less urgent industries, all of which would contribute to the security of the nation and its largely cyberspace based infrastructure.[252]

C. Single Agency

Although there are a number of disadvantages to having a single agency be responsible for cyber security, mobile banking could still benefit from having a single agency in charge of cyber security. A new agency would still provide a starting point for a more organized method of ensuring companies prioritize cyber security as much as they would prioritize locking the doors to their offices. The aforementioned recommendations for regulations pose large obstacles for Congress,[253] but this can be made more manageable by creating a single agency to create standardization across just one industry: the financial industry. By reducing the scope to just one industry, an industry that is actively seeking change, the government can more effectively support the private sector.[254] The recommended agency then, is not truly an agency, but a governmentally organized cooperative operation. The steps that President Obama has taken to assign NCCIC to a greater role in pursuing a federal standard are a good start, and it can potentially be grown to encompass the recommendation laid out here.[255] The messy organization of the cyber security organizations within the Department of Homeland Security are spread across too many functions and industries,[256] but harnessing that manpow-

hops-board-minibus-church-day-job.html (comparing the crowds welcoming the arrival of the new pope in 2005 and 2013, going from candles to a sea of LCD screens).

248. Andrew Johnson, *Plan to Make the iPhone a Payment Tool May Accelerate*, AMERICAN BANKER (Nov. 3, 2010), *available at* http://www.americanbanker.com/issues/175_212/iphone-payment-tool-plan-1028195-1.html (Having hooks into the carriers is going to be important for any kind of future mobile interoperable payments system."). Although this is not in the context of the government having hooks in the carriers, it makes sense to assume that the carriers, and control of them, would play an important role in the future of mobile payments systems.

249. *See, e.g.*, Unlocking Consumer Choice and Wireless Competition Act, 17 U.S.C. § 1201 (2012) (allowing consumers to "unlock" phones to work on different wireless networks).

250. AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740, 1753 (2011) (abrogating California's rule that found waivers of class arbitration in consumer contracts unconscionable).

251. Multi-faceted, meaning regulation is not directed only at the spot where the problem is first noticed: in the laps of big companies.

252. *Denial of Service*, *supra* note 67, at 40 ("Many of our critical infrastructures and our government depend upon the reliability and security of complex computer systems. We need to make sure that these essential systems are protected from all forms of attack.").

253. *See* Barnett, *supra* note 173, at *1; *supra* Part II.B.

254. *See* Robertson & Riley, *supra* note 229, (reporting JPMorgan Chase's aggressive tactics in investigating its security breaches).

255. *See supra* Part II.B.2.

256. *See supra* Part II.B.2.

er and combining it with financial institutions that are willing to invest in their security at this time is likely the best way to initiate progress in our nation's cyber security.[257]

Even if a completely new agency cannot be created, assigning the role of overseeing the regulation of cyber security and developments in financial industry security to a specific agency or entity would be beneficial to both banks and users of mobile banking applications. Though this would still increase costs and resources needed, having one agency take on such a role would start to create a more centralized cyber security structure, at least within that industry.[258]

The creation of a new agency would oversee cyber security and prevent unfair practices on behalf of consumers,[259] but would also be in charge of further developing data security for the protection of company data and consumer privacy; a much more manageable endeavor if limited to a single, money-driven industry.

Some areas of technology are being implemented too rapidly for the government to throw a safety net out to catch all of the problems, but working *with* private companies, much like President Obama attempted with Executive Order 13,691, will help.[260] A more specific undertaking must occur in which the most critical and time-sensitive industries are overseen.

At the very least, whether it is a government organization like the NCCIC or a private entity like an SO,[261] someone should be put in charge of cyber security regarding banking mobile applications. These applications are being used with increasing frequency, and there must be a handle on the situation before hackers can fully exploit the opportunity. Because consumers have so little they can do to protect themselves once they are using a mobile banking application and security of phones can be compromised in a number of ways, there is a need for that specific area of cyber security to be controlled, at least in the United States, by some well-intending, innovative group of people.[262] The sooner this can be established, the more easily the industry will be able to react to any major problems that emerge in the coming years. Any progress that is

257. *See supra* Part III.

258. This would imply centralized regulation, as opposed to centralized technology.

259. 15 U.S.C. § 45(a) (2012).

260. Promoting Private Sector Cybersecurity Information Sharing, Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (Feb. 13, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

261. *See supra* Part II.B.2.

262. Although the Internet and many critical infrastructures are privatized, the government played a major part in the Internet's birth and success, and can be helpful now as well. *See* Kesan & Shah, *supra* note 32.

made in this industry will also benefit other critical industries[263] and trickle down to raise the bar of cyber security one notch at a time.[264]

As globalization makes the world a smaller place, mobile banking across countries is inevitable. Assigning this role immediately is the almost only way to preemptively fight back the hackers and maintain the security of consumers, our companies, and our nation.

Despite the fact that the problems in cyber security are multiplying and have reached a point where security breaches within large companies and among software developers have become common knowledge and unworthy of the front-page, it continues to be neglected, with literature piling up on the topic of cyber security policy.[265] Like a puppy that is never trained, the unregulated cyber security systems will keep peeing in the house and causing problems you would not expect until it finally runs out into the road and gets some real attention.[266]

There are problems that come to light in more than one context.[267] One of these is the number of well-qualified security professionals.[268] Although this is not a problem easily solved in the short-term, it is one of the multiple problems that should be acted upon sooner rather than later. It is also reasonably simple enough for the government to be able to facilitate.[269] Considering various grant programs have been established in the name of cyber security, such programs should be moderately easy to create and will have a positive hand in helping to control the state of our nation's cyber security.[270]

Through the implementation of these recommendations, building on top of the cyber security agencies that already exist,[271] the government can help push cyber security development forward by working specifically with mobile banking and cyber security in the financial industry.

263. This is assumed because security across industries is Internet-based, which likely means similar measures will be technically feasible across industries.

264. *See* Barnett, *supra* note 173 (calling for the government to help private entities raise the cyber security "bar").

265. *Id.*

266. This has been likened to a cyber security equivalent of Pearl Harbor. Leon E. Panetta, Secretary of Defense, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, (Oct. 11, 2012), *available at* http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136 ("The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.").

267. *See* Sarnikar & Johnsen, *supra* note 202.

268. *Id.*

269. Press Release, Office of the Vice President, The White House, Vice President Biden Announces $25 Million in Funding for Cybersecurity Education at HBCUs (Jan. 15, 2015) [hereinafter *Press Release*], *available at* http://www.whitehouse.gov/the-press-office/2015/01/15/vice-president-biden-announces-25-million-funding-cybersecurity-educatio.

270. *Id.*; Gillum, *supra* note 68 (discussing changes that Obama has proposed regarding cyber-threats and related areas).

271. *See supra* Part II.B.2.

V. CONCLUSION

As the Internet has grown in its fury, so have the problems that come along with it.[272] With everyone so dependent on technology, much of which revolves around the Internet, it is inevitable that people will continue to embrace technology in search of convenience. In the name of convenience, people will have full access to their bank accounts on their phones.[273] Technology will also continue to encourage lackadaisical use,[274] granting access to sensitive information at the touch of a finger,[275] allowing the installation and use of unsecure software, and bypassing all manners of disclosures, terms, and security notifications with a single click.

The idea of cyber security is not a new idea; the government has been aware of the need for such measures in the United States for decades.[276] As private companies and financial institutions rely more on the Internet cyber infrastructure, and widely publicized security breaches increase in frequency, it is clearer that something must be done to protect these companies that deal with such sensitive information.[277] In addition to the protection of these companies, their cyber infrastructure, and data, consumers need their privacy protected from hackers as well as ill-prepared companies.[278]

It is practically impossible to get rid of the Internet or to replicate it in a newer, safer version.[279] As such, there is a real need for the development of newer encryption technologies.[280] Existing technologies provide a certain level of security, but by its nature, are likely to become outdated.[281] The government should take it upon itself to help push the development of cyber security forward, as this development is essential not only to the security of financial institutions and consumer privacy, but to the entire infrastructure upon which the United States government, as a member of the modern era, depends.[282]

Within the financial industry, the government should incentivize the development of cyber security and find solutions to foreseen problems, taking a step forward from reactive methods of cyber security.[283] By getting involved first with the financial industry, the government can help in the development of cyber security so that it can be applied to other critical infrastructures.

272. *See supra* Part I (discussing externalities and the tradeoffs between convenience and security).
273. *See supra* Part I.
274. *See supra* Part II.
275. *See supra* Part I.
276. *Denial of Service*, *supra* note 67.
277. *See supra* Part III.
278. *See supra* Part II.B.
279. *See supra* Part III.B.
280. *See supra* Part III.B.
281. *See supra* Part II.
282. *See supra* Part IV.
283. *See supra* Part III.C.

The creation of a separate entity could provide a means of focusing cyber security regulation, dealing at once with the cyber security regulation and regulation on behalf of consumer privacy, and the financial industry is the place to start. As the Internet continues to amass, it is inevitable that a nation pivotal in its success require an entire entity to prevent disaster in our nation's cyberspace.[284]

284. *Cf.* Kesan & Shah, *supra* note 32.