Securing Mobile Technology & Financial Transactions in the United States

Eleanor Lumsden*

One of the paradoxes of modern life is the conflict between convenience and security. Advances in technology simultaneously usher in progress and pain. The development of mobile and smartphone technology will have a significant positive impact on financial transactions and the average consumer's access to financial services. Nevertheless, there are several reasons to secure mobile technology and financial transactions in the United States. First, cell phones increase the risk to personal security and most U.S. wireless carriers are using outdated encryption technology. Second, many cell phone users are more concerned with convenience—caring more about the availability and functionality of smartphone applications—than with potential security threats. This will change as more consumers use their phones for financial transactions. Third, evidence from other developed countries, including Canada and several nations in Europe, has shown that it is possible to provide additional security protections for consumers.

Americans rely on their smartphones to transmit financial data about themselves, their work places and families. While some privacy laws have been interpreted to cover the unique threats posed by mobile technology, most do not, and security and privacy issues in regards to mobile banking have been largely unheralded.

This Article identifies existing privacy laws and security regulations that have been applied to mobile technologies by federal and state governments, by courts, and by various regulatory agencies. The Article then analyzes the shortcomings of the current regulatory framework in the United States. After examining several policy recommendations, as well as current standards in the telecommunications industry, the Article concludes with several suggestions for mitigating the risks posed by emerging mobile technology. Without entirely upending the current system, U.S. laws can be expanded and streamlined to address future challenges.

* Associate Professor of Law, Golden Gate University School of Law, J.D., NYU School of Law, A.B., Princeton University. This project would not have been completed without the research and scholarship assistance provided by GGU School of Law. I am indebted to Ramey Barnett, Kate Lauer, and Priya Sanger for their helpful comments and suggestions. I would also like to thank my research assistants, Natasha Mazina and Pamela Talledo for their help in researching this project.

I. INTRODUCTION

"The cell phone is not only bridging the digital divide but it is changing the way people who have never had bank accounts or credit cards deal with money."[1]

One of the paradoxes of modern life is the conflict between convenience and security. The development of mobile and "smart" phone technology is a sign of progress, and will have a significant positive impact on the average consumer's access to financial services. The global community will nevertheless need to address challenges— issues of privacy and security that similarly arose at the introduction of the personal home computer and the Internet— before many Americans will trust mobile banking platforms for financial transactions.

1. NICHOLAS P. SULLIVAN, YOU CAN HEAR ME NOW: HOW MICROLOANS AND CELL PHONES ARE CONNECTING THE WORLD'S POOR TO THE GLOBAL ECONOMY 125 (2007).

Securing Mobile Technology & Financial Transactions in the United States

Before the development of the smartphone, or cell phones with access to data services and the ability to connect to the Internet, the average consumer used cellular telephones primarily as a means of making phone calls and sending text messages to communicate with others. Now, technological advances are reshaping the world. Smartphones are small and portable and have replaced landlines in more than 3 out of 10 (31.6%) American households.[2] "The percentage of households that are wireless-only has been steadily increasing," and in certain demographic groups, "a majority live in households with only wireless telephones."[3] Consumers are increasingly relying on these phones to transmit sensitive financial data through seemingly secure channels, but in the process may also unwittingly expose personal information about themselves, their work places,[4] and families.

Yet smartphones are essentially mini-computers and unfortunately share the computer's weaknesses.[5] Although software developers have found ways of addressing the security threats posed to electronic data stored on computers, they have not eliminated them. Smartphones, similarly embedded with extremely sensitive personal and financial data, are also vulnerable but many cell phone users appear more concerned with convenience—caring more about the availability and functionality of smartphone applications—than with potential security issues posed by the use of the phone itself. Nonetheless, there are several reasons why it is important to secure mobile technology and financial transactions in the United States.

First, many consumers store just as much if not more personal information about themselves on their cell phones than on personal computers,[6] not realizing how making certain choices, such as remotely accessing financial services on unsecured wireless channels, adversely impacts the confidentiality and secu-

2. Stephen J. Blumberg and Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January-June 2011*, Division of Health Interview Statistics, Dec. 21, 2011 at 1.

3. *Id*. at *2-3*. "Nearly 6 in 10 adults aged 25–29 (58.1%) lived in households with only wireless telephones. Nearly three in four adults living only with unrelated adult roommates (71.3%) were in households with only wireless telephones. Half of all adults renting their home (52.5%) had only wireless telephones." *Id.*

4. One can, for example, "expose sensitive work information to systems your company's IT department has no control over" by a simple act "like forwarding your corporate e-mail to your Gmail account." *Katia Moskvitch*, Mobiles and Tablets: A New Threat to the Business World?, *BBC NEWS (June 30, 2011), http://www.bbc.co.uk/news/business-13962653.*

5. Elizabeth Wasserman, *Mobile Payments: Who Will Regulate?*, POLITICO (April 4, 2011, 4:44 AM), http://www.politico.com/news/stories/0411/53112.html ("Since smartphones are miniature computers, strong cryptography and authentication protocol can be built into their systems—but it is up to device manufacturers and service providers to ensure these protections are in place for NFC [near field communication] transactions.").

6. *See e.g.*, Giselle Tsirulnik, *How Consumers Will Use Their Mobile Devices During the Holidays*, Mobile Commerce Daily, Nov. 28, 2011, http://www.mobilecommercedaily.com/ 2011/11/28/how-consumers-will-use-their-mobile-devices-during-the-holidays ("Approximately 52 percent of smartphone users will use their device to research products, redeem coupons and use apps to assist in their holiday gift purchase.").

rity of their private information. Apart from an interest in keeping personal information secure, privacy interests are implicated based on an ordinary consumer's desire simply to keep certain information private. Despite the risks, few consumers even consider, much less purchase, software to protect their smartphones. Certain companies, anticipating the growing need for such protection, now provide services that allow consumers to remotely lock or erase data on stolen or lost cell phones.[7] These companies also have applications that can help owners locate lost or stolen phones, and alert users about "malicious applications and ones that encrypt conversations to thwart eavesdropping."[8] Whether these services will be utilized more widely in the future is an open question.

Second, many in the wireless industry acknowledge that cell phones increase the risk to personal security because most carriers are using outdated encryption technology which is vulnerable to attack.[9] The technology that is most commonly employed in the United States is less secure than the technology used in other developed countries, including Canada and many nations in Europe.[10] Changes have not been implemented because updating the existing encryption systems would be time consuming, expensive, and probably cost prohibitive for cell phone manufacturers.[11]

Third, evidence from other countries demonstrates that it is possible to provide additional security protections for consumers by enacting legislation that limits the long-term storage of cell phone records (which often contain name, address, and other highly sensitive information) by private companies. In the United States for example, cell phone records can be kept indefinitely by cell phone companies; not so in Europe where companies can only store consumer data for limited periods of time.[12] Limiting the length of storage will lessen the vulnerability of these records.

Outside of the mobile payment and telecommunications industries, and de-

7. Lookout, Inc., a mobile security company based in San Francisco, California developed an application called Lookout Mobile Security that not only monitors applications installed on phones to see if they are leaking confidential information, but also provides the ability to "report your mobile as stolen, lock it, and, if necessary, erase the data that it contains remotely." ROBERT VAMOSI, WHEN GADGETS BETRAY US: THE DARK SIDE OF OUR INFATUATION WITH NEW TECHNOLOGIES 190 (2011); *see also* Moskvitch, *supra* note 4.

8. Moskvitch, *supra* note 4.

9. Vamosi, *supra* note 7 at 52-53.

10. *Id.*; *see also* Donald A. Cohn, Jonathan P. Armstrong & Bruce J. Heiman, Who Steals My Name: The US and EU Response to Data Security Breach, *ACC Docket, 24, no. 6 June 2006 24, 29 (*"Currently about 33 different European jurisdictions (including the 25 within the EU) have some form of privacy or data protection law in place.").

11. Vamosi, *supra* note 7, at 52-53.

12. *Id.* at 183-84. Europe has strict privacy policies regarding commercial data collection and certain "use-limitation" laws which prevent companies from selling or using customer's personal account information. Also, anyone collecting such information can only retain the information for a period of up to two years. *Id.*

spite efforts by consumer protection advocates, the growing trend of mobile banking and the unique privacy and security threats posed by the attendant technology have been largely unheralded by legal scholars.

This Article identifies the federal privacy laws and online security regulations that have been applied to mobile technologies by courts and federal and state agencies. Although many laws aimed at consumer privacy and security currently exist, this Article takes the position that these laws are nevertheless insufficient, and analyzes the shortcomings of our current regulatory framework. This Article also examines several policy recommendations made by consumer protection experts, as well as best practices and current standards, before concluding with several additional suggestions aimed at mitigating the security risks posed by emerging mobile technology in the United States.

II. IS PRIVACY A FUNDAMENTAL HUMAN RIGHT? THE DEVELOPMENT OF PRIVACY RULES AND U.S. CONSUMER PROTECTION

"Internet-based communication technologies strain the existing legal system because courts have often refused to recognize a 'reasonable expectation of privacy' in Internet electronic communications, reasoning that, as the Internet is public in nature, communications therein should receive a disfavored privacy protection status."[13]

The foundations of our modern privacy laws were established in 1890 in *The Right to Privacy*, a now seminal law review article by Samuel Warren and Louis Brandeis.[14] Brandeis and Warren argued, well before the conventional wisdom of the time, that the advent of new communications meant that society would need to provide more, not less, protection to safeguard individual privacy rights.

The first major case on the subject, Pavesich v. New England Life Insurance Co.,[15] expanded upon the Warren/Brandeis thesis and carved out a new tort for the invasion of privacy. The U.S. Supreme Court eventually followed suit with the landmark Griswold v. Connecticut decision in 1965,[16] and Loving v. Virginia in 1967.[17] Currently, the right to privacy is explicitly recognized in the state constitutions of ten states.[18]

13. Frederick M. Joyce & Andrew E. Bigart, *Liability for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VA. L. REV. 1502 (2007) (citing Daniel B. Garrie, Matthew J. Armstrong & Donald P. Harris, *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected*, 29 SEATTLE U. L. REV., 97, 122-23 (2005)).

14. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

15. Pavesich v. New England Life Insurance Co., 50 S.E. 68 (Super. Ct. Ga. 1905).

16. Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (acknowledging the right of privacy of married couples to use contraceptives).

17. Loving v. Virginia, 388 U.S. 1 (1967) (the right to marry is included in the right to privacy).

18. The ten states include: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Mon-

The availability of the Internet and new media (including Facebook, YouTube and blogs) is challenging conventional privacy doctrine. The impact of these new media vehicles will necessitate a change in our laws to fill in the widening gaps in traditional jurisprudence. In fact, some scholars believe that current U.S. privacy laws are insufficient to protect today's average consumer from the new threats posed by burgeoning communications technologies,[19] and will be unable to meet the rising challenges to personal privacy posed by the Internet and new media.

At common law, the tort of "invasion of privacy" has developed particular meanings over time,[20] and has also been supplemented by statute.[21] Still, in the U.S. at least, there does not appear to be complete agreement that privacy is a fundamental human right. California is one of ten states that recognizes a right to privacy in its constitution.[22] There are also many federal laws that protect privacy, and the U.S. Constitution explicitly carves out the boundaries of certain governmental intrusions. However, the confusing patchwork of interconnecting rules presents a challenge for even adept lawyers, government regulators, and telecommunications providers, much less the ordinary layperson, to decipher. While this might be said to be a problem of all laws, it is essential to clarify the rules in this area because there is little incentive for the various actors, including banks, telecommunications providers, and cell phone manufacturers, to work together to resolve these issues. Having differing standards and practices is ultimately harmful, and not helpful to consumers.

Despite the statutory hedging that appears to rule the day, heady and significant change is afoot in the United States. Unfortunately, data breaches and the leakage of personal information pose threats to individual autonomy, states' rights and national security, and implicate the financial system as a whole. This fact has been acknowledged by individual state legislatures, by the President, and by Congress.

In 2009, President Barack Obama created the White House Office for

tana, South Carolina and Washington. See National Conference of State Legislatures, Privacy Protections in State Constitutions, http://www.ncsl.org/issues-research/telecom/privacy-protections-in-state-constitutions.aspx.

19. Joyce & Bigart, *supra* note 13, at 1484 ("The federal framework of laws intended to prevent electronic technology from invading legitimate privacy interests is now rickety and unequal to the task.").

20. The tort of invasion of privacy generally includes four distinct, but related concepts including: 1) intrusion into seclusion; 2) false light; 3) public disclosure of private facts; and 4) misappropriation. William L. Prosser, Privacy, 48 CAL. L. REV. 383, 389 (1960); *see also* Restatement (Second) of Torts, §§ 652A-652E; 5 Witkin, Summary of Cal. Law Torts (10th ed.) Torts, Section 651.

21. *See e.g., Cal. Civ. Code § 1708.8(b).*

22. CAL. CONST. art. I, § 1, states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy (emphasis added)." *See also* SASKIA KIM, CONSUMER PRIVACY AND IDENTITY THEFT: A SUMMARY OF KEY STATUTES AND GUIDES FOR LAWMAKERS (Cal. Senate Office of Research, 3d. ed. 2008).

Cyber Security. In doing so, he confirmed that Internet security threats continue and need to be taken seriously: the "cyber threat is one of the most serious economic and national security challenges we face as a nation . . . America's economic prosperity in the 21st century will depend on cybersecurity."[23] The President appointed a Cybersecurity Coordinator, who reports to both the National Economic Council and the National Security Council.[24]

Similarly, as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010,[25] Congress created the Consumer Financial Protection Bureau ("CFPB"). On July 21, 2011, the CFPB assumed responsibility for the enforcement of federal consumer protection laws.[26] On the state level, California is among a number of states that have enacted enhanced privacy laws that supplement traditional common law rules and even provide greater protections for state residents.[27] All of these developments are relevant to the question of how we might secure mobile technology and financial transactions.

III. WHAT IS MOBILE BANKING AND HOW IS IT USED?

With online banking, customers can access financial services through the Internet and without needing to visit a brick and mortar bank location. In contrast, mobile banking refers to a process whereby banks and other financial institutions set up systems that allow them to communicate with their customers specifically through the use of their cell phones. Banks in the United States typically offer their mobile services primarily in three ways that are distinct from online banking methods, including either communicating with clients and customers through: 1) SMS (text messages), 2) mobile web programs, and 3)

23. Press Release, National Security Council, Transcript of remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure ("It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. So cyberspace is real. And so are the risks that come with it. It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy.").

24. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

25. Dodd-Frank Act, Pub. L. No. 111-203, H.R. 4173 (2010).

26. Fred Rivera, *Consumer Financial Protection Bureau to Take Flight July 21, 2011*, FIN. SERV. LITIG. MONITOR, PERKINS COIE, LLP (Sept. 21, 2010), http://www.financialserviceslitigationmonitor.com.

27. For example, California's privacy laws protect individuals from intrusions by either governmental or by private entities. See, e.g., American Academy of Pediatrics v. Lungren 940 P.2d 797, 808 (Cal. 1997), citing Hill v. National Collegiate Athletic Association (1994) 865 P.2d 633, 641-46.

mobile client applications.[28]

Most large U.S. banks offer customers the ability to remotely access financial services which include, but are not limited to:

- Account alerts, security alerts and reminders;
- Account balances, updates and history;
- Branch or ATM location information;
- Bill pay; and
- Funds transfers.[29]

Bank of America ("BofA") has had online services in place for years, but now provides additional access to special services to customers who have certain smartphone applications ("apps") on their iPhones, Blackberries and Android phones. BofA allows customers to check account balances, transfer money, and pay bills on their mobile devices, and is testing their ability to allow customers to make deposits remotely.[30] Citibank has tested a real time person-to-person mobile payment service that allows people to link to an existing bank account and transfer funds to family and friends (usually Citibank subscribers or subscribers of the service) either by text message, through the mobile phone's web browser, or through a web application.[31] Similarly, in 2010, Wells Fargo announced a new "text banking" program, and now has a service (protected by the bank's own "Online Security Guarantee") that allows customers to deposit checks through their mobile phones.[32]

And it's not just the banks. A variety of players are competing to release mobile phone applications that may one day surpass, or eventually obviate entirely, the current consumer dependence on credit cards.[33] Mobile services offered by apps on Android, Blackberry, and iPhones have unique features that

28. Mobile Marketing Association, *Mobile Banking Overview (NA)* (Jan. 2009), http://www.mmaglobal.com/mbankingoverview.pdf.

29. *Id*.

30. Rimma Kats, *Bank of America Testing Functionality To Make Deposits Remotely*, MOBILE COMMERCE DAILY, Aug. 11, 2010, http://www.mobilecommercedaily.com/2010/08/11/bank-of-america-aims-for-convenience-with-mobile-banking-service.

31. Dan Butcher, *Citibank Tests Person-to-Person Mobile Payments*, MOBILE MARKETER, Oct. 15, 2008 ("Citi-Obopay is the first real-time, person-to-person mobile money transfer service with the ability to link directly to a bank account that has been offered in the U.S."), http://www.mobilemarketer.com/cms/news/banking-payments/1906.html; *see also* Press Release, Citigroup Inc., Citi and Obopay to Pilot Innovative Mobile Person-to-Person Payment Service (Feb. 28, 2007).

32. Press Release, *Wells Fargo Extends Text Banking to All Customers: Wells Fargo Becomes First Major U.S. Financial Institution to Enable Customers to Connect to Accounts with Text Banking, Without a Need to Have a Personal Computer or An Enrollment in Online Banking*, WELLS FARGO, Feb. 4, 2010, https://www.wellsfargo.com/press/2010/20100204_TextBanking.

33. Wasserman, *supra* note 5 ("As more Americans learn how to shop with their cellphones, Washington is trying to figure out who should answer the call to regulate this new form of commerce.").

are distinct from online banking, including:

> GPS-enabled locator service: This feature will locate the banking center or automated teller machine ("ATM") that is closest to the phone user (which means the application must determine the user's location and is then able to retain that information), and will then provide turn-by-turn directions to the ATM or bank location.[34]
>
> Photo-deposit capability: Using an application, a user can use their mobile phone to first take pictures of the front and back of an endorsed check and then send those pictures to the bank for a remote deposit.[35]
>
> Person to person payments: An application will allow a bank customer to send or receive payments from another person (who does not necessarily have to be another bank customer) through an email.[36]

The important point is that through smartphone apps, there are an increasing number of ways that consumers will be able to move money around. We are going to need a privacy regime that is flexible enough to manage the risks inherent in our current system as well as those that may emerge in the future.

IV. MOBILE BANKING AS GROWING TREND

> "*The preponderance of evidence shows that mobile phones directly contribute to significant GDP growth in all countries and produce the most growth in poor countries with previously low levels of phone penetration."*[37]

Mobile banking has taken off in the developing world and is now spreading to the United States.[38] According to an October 2010 study conducted by the Pew Institute, most Americans own cell phones, including approximately

34. *Cynthia J. Larose, Top 5 Commercial Data Security and Privacy Issues in 2012, THOMSON REUTERS, Jan. 30, 2012, http://newsandinsight.thomsonreuters.com/Legal/Insight/2012/01_-_January/Top_5_commercial_data_security_and_privacy_issues_in_2012/.*

35. Andrea Smith, *Now You Can Scan Your Deposit with Bank of America's App.*, MASHABLE, *Aug. 8, 2012, http://mashable.com/2012/08/08/now-you-can-scan-your-deposit-with-bank-of-americas-app/.*

36. Larose, *supra* note 34 ("The mobile payment technology, called near field communication, is expected to be integrated into most popular smartphones in the not-too-distant future—from the Blackberry to the iPhone and everything in between.").

37. Sullivan, *supra* note 1, at 149.

38. Jane J. Kim, *Mobile Banking Shifts into Higher Gear*, WALL ST. J., Feb. 21, 2007, at D1.

eighty-five percent of the U.S. adult population.[39] As mobile phone use spreads, more people will be able to utilize mobile phones for an increasing array of uses, including for banking and financial services. In 2011, the Federal Reserve commissioned a survey of 2,300 respondents regarding their use of mobile devices for banking and for shopping and comparing products.[40] The Federal Reserve released a report of the results of the survey,[41] including these specific findings:

- Nearly nine out of ten adults in the United States have a mobile phone, and two-fifths of those phones are smartphones with Internet connectivity;
- Among all mobile phone users, one out of five has used their phones to conduct some banking activity in the last 12 months;
- Users with traditional mobile phones access bank information via text messages, while smartphone users access their bank information by downloading their bank's application or via the bank's Internet site;
- Younger customers below age 29 have readily adopted mobile banking and make up almost 44 percent of all consumers surveyed who use these services;
- Hispanic and non-Hispanic blacks comprise a disproportionate share of those who utilize mobile banking services;
- The most common transactions performed by users of mobile banking were checking account balances, checking recent transactions or transferring money between accounts;
- Of those consumers who had not adopted mobile banking, the primary reason given was that they felt their banking needs were being met through more traditional means;
- Security concerns were the second most-cited reason for not using mo-

39. Privacy Rights Clearinghouse, *Fact Sheet 2: Wireless Communications: Voice and Data Privacy*, *available at* http://www.privacyrights.org/fs/fs2-wire.htm.

40. Sandra F. Braunstein, Director, Division of Consumer and Community Affairs, Testimony on Mobile Payments Before the Committee on Banking, Housing, and Urban Affairs (March 29, 2012), *available at* http://www.federalreserve.gov/newsevents/testimony/braunstein20120329a.htm.

41. BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, CONSUMERS AND MOBILE FINANCIAL SERVICES (March 2012), *available at* http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf.

> bile banking. Specifically, consumers expressed concerns about hackers gaining access to their phones and exposing their personal financial information. A little more than one-third of all mobile phone users reported that they do not know how secure mobile banking technology is for protecting their personal information, while an additional one-third rated the technology as unsafe;[42] and

- Among those consumers with any type of mobile phone, but who are not currently using mobile banking, one out of ten expects to be using it within the next year.[43]

Further, some predict that by 2016, for many people the cell phone will become the most common interface with a bank.[44] The use of mobile phones specifically as an advertising and marketing tool has also increased exponentially in recent years.[45] All of these findings are significant and show the growing importance of mobile financial services.

Again, although more people in the United States today still either access banking services in person or through computers and online banking rather than through their cell phones,[46] evidence suggests that this will soon change.[47] For example, industry insiders believe that Near Field Communications ("NFC") technology for smartphones will have a tremendous impact on the world market.[48] NFC technology essentially uses wireless frequencies to enable mobile phone users to purchase goods simply by positioning their phone close to their intended target:

> Near Field Communication technology is a short-range tool that operates on wireless frequencies similar to RFID chips and tags. It works by connecting a user's mobile device, equipped with an NFC antenna

42. *See* Ann Carrns, *Consumers Have Concerns about Mobile Banking Security, Survey Finds*, N.Y. TIMES, April 17, 2012, http://bucks.blogs.nytimes.com/2012/04/17/consumers-have-concerns-about-mobile-banking-security-survey-finds/.

43. *Id.*; *see also* Braunstein, *supra* note 40.

44. Mike Periu, *Small Business Banking in 2016*, OPEN FORUM, March 16, 2011, http://www.openforum.com/idea-hub/topics/money/article/small-business-banking-in-2016-1.

45. Bryan Clark & Blaine Kimrey, *Litigating Mobile Marketing Claims*, 27 COMMC'N. LAWYER 4 (July 2010) ("The popularity of the iPhone and other advanced mobile devices has opened up myriad new channels for advertisers, marketers and content providers.").

46. Braunstein, *supra* note 40.

47. Mobile Marketing Association, *supra* note 28, at 1 ("Although more U.S. consumers currently use PCs rather than mobile phones for banking…this gap [is] narrowing.") ("It took approximately ten years (1996-2006) to reach 40 million online banking users. According to the Online Banking report, it is expected to take 10 years to reach a similar penetration rate for mobile banking.").

48. Matt Hamblen, *2011 a 'pivotal year' for NFC payments, say RIM, Orange and KT execs: New NFC smartphones, growing payment ecosystem and industry partnerships should offer big boost to the emerging technology*, COMPUTERWORLD, Feb. 17, 2011, http://www.computerworld.com/s/article/9210038/2011_a_pivotal_year_for_NFC_payments_say_RIM_Orange_and_KT_execs?taxonomyId=15&pageNumber=1.

> or specially programmed SIM or SD data card, to a receiver, usually a few feet away. The idea is that consumer will be able to "wave" their handsets when they're buying something at a retail location.[49]

Not many phones in the U.S. presently have NFC capabilities; Google has taken the lead in this area.[50] Recently, Google launched a new payment system called Google Wallet, which is like an electronic wallet and uses an NFC chip on mobile phones.[51] As part of a "tap-and-go" process, customers can use the service to access coupons and redeem loyalty cards on their phones.[52] Google is just one of a long list of technology companies, financial service companies, banks and startups who are looking to use advances in NFC to facilitate mobile payments.[53] "Mobile payments allow consumers to buy products or transfer money with a quick text message or application downloaded to the phone,"[54] and there are other concerns, aside from privacy and data security, with this technology.[55] As more and more phones are starting to come equipped with NFC chips, it appears that NFC is the latest emerging trend to take off in the mobile commerce arena.[56]

Several companies have decided to adopt NFC technology, and through two associations, the NFC Forum and Global Platform, have partnered to work on setting standards to address potential security and functionality concerns.[57]

---

49. Sam Gustin, *Near Communications Big (Money) Moment*, WIRED, May 25, 2011, http://www.wired.com/epicenter/2011/05/wired-nfc-faq/.

50. *Id.* ("Silicon Valley titan Google is expected to announce a new mobile payments system at an event in New York City on Thursday. According to Bloomberg, Google is teaming up with Sprint, a longtime Google partner and the No. 3 wireless provider in the United States after Verizon and AT&T, to roll out a mobile-payments system based on Near Field Communication, or NFC, technology.")

51. Ryan Kim, *Google Launches its Wallet Platform To Jumpstart NFC Payments*, GIGAOM, May 26, 2011, http://gigaom.com/2011/05/26/google-tries-to-jumpstart-nfc-payments-with-wallet-platform/.

52. *Id.*

53. Gustin, *supra* note 49.

54. For a comprehensive analysis of mobile payment issues by consumer protection experts, see Suzanne Martindale & Gail Hillebrand, *Pay at Your Own Risk? How to Make Every Way to Pay Safe for Mobile Payments*, *27* BANKING & FIN. L. REV. 265, 2 *(2012).* Martindale and Hillebrand discuss specific examples of mobile payments—for example, sending donations for relief efforts following a major disaster to the American Red Cross by SMS text and then having the amount charged to a user's phone bill. *Id.* at 4.

55. As the focus of this Article is on data privacy and security, the Article will not discuss the usual concern with mobile payment issues, namely the right of consumers to get their money back in the event of theft (for example, "when a thief rather than the consumer waves the device, the wrong amount is billed, or the goods are not delivered as promised," *id.* at 5), or a payment dispute that arises when a consumer purchases a product using an application on their phone.

56. Cadie Thompson, *Near Field Communication the Next Mobile Boost?*, USA TODAY, Jan. 8, 2012, http://www.usatoday.com/tech/news/story/2012-01-08/cnbc-near-field-communication-mobile/52443756/1; *see also*, Sarah Kessler, *NFC Technology: 6 Ways It Could Change Our Daily Lives*, MASHABLE, May 6, 2010, https://mashable.com/2010/05/06/near-field-communication/.

57. Mike Clark, *NFC Forum partners with GlobalPlatform on NFC standards*, NFC WORLD, Apr. 3, 2012, http://www.nfcworld.com/2012/04/03/314917/nfc-forum-partners-with-globalplatform-on-nfc-standards/; *see also*, Sarah Clark, *EMVCo Takes First Step Towards NFC Payments Standards*, NFC WORLD, May 11, 2009, http://wwww.nfcworld.com /2009/05/11/31133/emvco-takes-first-step-towards-nfc-payments-standards/.

Nevertheless, it appears that the regulations (as discussed later in this Article) currently in place to protect consumers online do not appear to apply to NFC technology. This gap in protection might enable Google and other companies using this technology to track and store customer data without much oversight.

V. MOBILE BANKING AROUND THE WORLD . . .

"Mobile banking in developing countries is just the beginning of an expected avalanche of services and applications that collectively will constitute mobile commerce."[58]

Despite the risks and in some cases, despite outdated and insecure infrastructure, many financial service companies in developing countries, particularly in some countries in Africa and in the Philippines, are providing mobile commerce services to millions of customers.[59] Consumers in these countries are also learning to use mobile phones to make international money transfers.[60] Remittances "are the largest source of foreign currency in most poor countries—far outstripping aid and investment."[61]

Mobile commerce is probably one of the most important developments in the developing world. In fact, at least one scholar argues that the spread of cell phones in developing countries is revolutionary—much like the Industrial Revolution in the United States—and far more significant than the introduction of personal computers into the U.S. economy in the 1980s.[62] Studies also suggest that the growth of cell phone use and mobile banking has a direct and positive effect on a developing country's gross domestic product ("GDP"), and specifically that "adding ten phones per 100 people adds 0.6 percent to the GDP."[63] If true, these facts mean big business for software and tech companies willing to invest in overseas markets.

These companies, along with financial services providers and wireless telecomm carriers, are using capabilities unique to the mobile phone, including text

58. Sullivan, *supra* note 1, at 127.

59. Vamosi, *supra* note 7, at 186-187.

60. Amol Sharma, *Vodafone, Western Union Offer Transfers Via Cell*, WALL ST. J., Dec. 8, 2008, http://online.wsj.com/article/SB122869576629386747.html.

61. Sullivan, *supra* note 1, at 135 ("The World Bank estimates $200 billion in remittances annually, but the number may be much closer to $300 billion.").

62. *Id.* at 145 ("as new information technology rampages through the South, it is creating wealth and producing millions of new income opportunities in rural areas that translate into billions of dollars in a new national income"); *see also* Bethany Brown, *Mobile Phones: Reshaping the Flow of Urban-to-Rural Remittances*, 11 SUSTAINABLE DEV. L. & POLICY 50, 50 ("Mobile money transfers from person to person via mobile phones stand ready to revolutionize traditional remittance models, allowing a greater percentage of urban laborers' earnings to be remitted to rural recipients.").

63. Sullivan, *supra* note 1, at xxxiv (citing research from the London Business School. Sullivan further states that according to the U.N., one percent of GDP growth results in a two percent reduction in poverty.).

messaging, to connect their customers with vital payment services to which they might not otherwise have access. Cell phone owners are able to send and receive remittances, pay bills, and purchase items at retail outlets; customers can also receive microloans that are disbursed by phone from microfinance institutions, and may use their phones almost like a virtual ATM machine—in many cases with reduced delivery and transaction costs.[64]

Throughout Africa, cell phone ownership has skyrocketed, and has implicitly transformed the financial sector: "Africa is now the fastest growing region in the world in terms of mobile phones. There are more new mobile phone customers every week in Africa than in North America."[65] In Rwanda, citizens in rural areas who may not even have electricity in their homes still own cell phones (sometimes using a generator owned by someone else in their village).[66] In Zambia, Coca Cola both sends and receives payments via text message: customers can use their mobile phones to text payments to retailers, and Coca Cola uses mobile phones to text payments to its distributors.[67]

These developments are mirrored in many parts of Asia, where cell phones are also having a major impact on business and finance.[68] Ubox is a Chinese app that allows customers to make purchases at vending machines using their mobile phones.[69] In the Philippines, "people buy soap and pizza by phone," and in Bangladesh, "bank customers can check their accounts by phone."[70]

In South Africa, Kenya, and the Philippines, mobile banking is quickly surpassing traditional online banking methods: through M-PESA, a hugely popular and successful mobile payment service in Kenya,[71] a user can make payments via a mobile "wallet" that is installed on a SIM card in a cell phone. In the Philippines, there are 3.5 million mobile banking subscribers who are utiliz-

64. *Id.* at 127.

65. *See* Sullivan, *supra* note 1, at 124; *see also* S. LaFraniere, *Cell Phones Catapult Rural Africa to 21st Century*, N.Y. TIMES, Aug. 25, 2005, at 1; Rodrique Ngowi, *Cell Phone Use Changes Life in Africa*, ASSOCIATED PRESS, Oct. 16, 2005; N. Hano, *Africa's Cell Phone Boom Creates a Base for Low-Cost Banking*, CHRISTIAN SCIENCE MONITOR, Aug. 26, 2005, www.csmonitor.com; Russell Southwood, *Thank You For Your Purchase: A Mobile Phone Turns into a Credit Card Terminal*, ALLAFRICA, Dec. 20, 2005, http://allafrica.com/stories/200512190438.html.

66. Sullivan, *supra* note 1, at 125.

67. *Id.*

68. Madanmohan Rao & Lunita Mendoza, *India: The 'Mobile Party' Begins, But Wi-Fi Languishes*, *in* ASIA UNPLUGGED: THE WIRELESS AND MOBILE MEDIA BOOM IN THE ASIA-PACIFIC REGION 354-72 (New Delhi: Sage, 2005).

69. Steven Millward, *Ubox App + Vending Machines = Mobile Payments for Snacks and Drinks in China*, PENN OLSON BLOG (Sept. 6, 2011), http://www.penn-olson.com/2011/09/06/ubox-app-vending-machines/.

70. Sullivan, *supra* note 1, at 125.

71. M-Pesa has over 14 million users in Kenya, and according to the IMF, "M-Pesa now processes more transactions domestically within Kenya than Western Union does globally, and provides mobile banking facilities to more than 70 per cent of the country's adult population." Microfinance Africa, *Mobile Money Takes East Africa by Storm, Apr. 3, 2012, http://microfinanceafrica.net/tag/m-pesa/.*

ing similar, and increasingly expansive services.[72] In Haiti, where less than one percent of the country's population of eight million people has conventional fixed line service, there has been a surge in cell phone ownership.[73] In India, as in the Philippines, rural villagers have been receiving remittances or overseas cash transfers through their phones for years.[74]

This diverse utilization of mobile banking platforms can be viewed in both positive and negative ways. The benefit is that there is a wide variety of platforms available to consumers.[75] The downside is that regulation is entirely lacking in many parts of the developing world, so in some places where branchless banking has taken off like Kenya, M-Pesa had to start off without any clear regulation. Despite this fact, mobile banking is flourishing in some places. However, certain policy analysts at the World Bank-affiliated organization, the Consultative Group to Assist the Poor, are conducting studies regarding the scope of potential regulation and believe that further regulation in certain areas is needed in order for mobile banking to reach its full potential.[76] Although regulation on an international basis is also very important, it is beyond the scope of this Article.

VI. SOUNDS GREAT! WHERE IS THE RISK??

The most apparent safety concern is protecting personal data that either is stored in or flows through a mobile device—payment account numbers, PINs, security codes, passwords, etc. "Exposure of personal information over a wireless network can leave the consumer feeling vulnerable to theft. As a result, mobile payments have a higher hill to climb to assuage consumer concerns about security and privacy."[77]

The problem is that the incidences of electronic crime ("e-crime") are on the rise: "as with credit cards, the sensitive financial data stored on mobile

72. Vamosi, *supra* note 7, at 186-87.

73. Simon Romero, *A Cell Phone Surge Among World's Poor in Haiti*, N.Y. TIMES, Dec. 19, 2000, http://www.nytimes.com/2000/12/19/business/technology-cell-phone-surge-among-world-s-poor-haiti-entrepreneurs-suppliers.html (compare this with more than 95 percent of the U.S. population with fixed line service).

74. Sullivan, *supra* note 1, at 125.

75. Mobile Marketing Association, *supra* note 28.

76. *CGAP Report: Mobile Banking Could Be Key to Banking the Unbanked*, INSIDE MICROFINANCE, Oct. 24, 2011, http://www.insidemicrofinance.com/_cms/_news/cgap_report_on_ mobile_banking ("Challenges to the growth of branchless banking include reluctance on the part of banks to get involved, as well as outdated or inadequate regulations.").

77. *See* Bill Gajda, *Managing the Risks and Security Threats of Mobile Payments*, PYMTS.com (Feb. 2011), http://pymnts.com/managing-the-risks-and-security-threats-of-mobile-payments; *see also* Yukari Iwatani Kane & Scott Thurm, *Your Apps are Watching You*, WALL ST. J., Aug. 8, 2011, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html ("Few devices know more personal details about people than the smartphones in their pockets: phone numbers, current location, often the owner's real name—even a unique ID number that can never be changed or turned off. These phones don't keep secrets.").

phones will become targets for thieves and the unscrupulous."[78] Addressing e-crime is important, even where it does not specifically relate to mobile banking because as mini-computers, smartphones are equally vulnerable to electronic security breaches; if measures are not taken to specifically mitigate the risk of data losses due to e-crime generally, mobile banking customers will not trust banks' or telecommunications providers' abilities to secure sensitive financial information that is stored and transmitted via mobile banking applications. Without this trust, it is unlikely that mobile banking will be fully utilized by the vast majority of consumers in the United Sates.

In July 2009, a massive case of fraud was reported in South Africa where criminals used the Internet to intercept banking passwords sent to clients' mobile phones.[79] In August 2011, hackers successfully attacked the San Francisco Bay Area's Bay Area Rapid Transit ("BART") system on three separate occasions.[80] In one instance, confidential personal information of Bay Area commuters was leaked online: "The anti-BART hackers, angered at the agency's tactics to curtail previous protests, posted the names, street addresses, email addresses, phone numbers and passwords of at least 2,400 of the website's 55,000 email subscribers . . ."[81] In a separate attack, the group posted the private information of 102 BART Police Officers, including their home addresses, personal emails, and account passwords.[82]

Shortly afterwards, in September 2011, the Dutch government, "one of the most digitally advanced countries in Europe," was forced to investigate a major hacking scandal in which security breaches on government websites appeared to compromise the personal data of Dutch citizens.[83] It appeared that the personal information of consumers who filed their taxes or conducted other business online may have been compromised.[84] The situation took on a crisis-like

78. Wasserman, *supra* note 5 (quoting Harley Geiger, policy counsel for the Center for Democracy & Technology).

79. Mark Pickens, David Porteous & Sarah Rotman, *Scenarios for Branchless Banking in 2020*, CONSULTATIVE GROUP TO ASSIST THE POOR, OCT. 11, 2009 (focus note no. 57), *available at* http://www.cgap.org/p/site/c/template.rc/1.9.40599/.

80. Casey Newton, *BART Website Hacked, Customer Info Leaked*, SF GATE, Aug. 15, 2011, http://articles.sfgate.com/2011-08-15/news/29888344_1_jim-allison-hackers-phone-service.

81. Matt O'Brien, *Computer hackers expose BART riders' personal information*, CONTRA COSTA TIMES, Aug. 14, 2011, http://www.mercurynews.com/top-stories/ci_18680763.

82. Ned Potter, *BART Police Officers' Addresses Posted by Hackers Amid Protests Against San Francisco Transit System*, ABC NEWS, Aug. 17, 201, http://abcnews.go.com/Technology/bart-police-officers-addresses-emails-posted-hackers-attack/story?id=14326395.

83. Kevin O'Brien, *Dutch Widen Inquiry Into Hacking of Official Sites*, N.Y. TIMES, Sept. 6, 2011, http://www.nytimes.com/2011/09/07/technology/dutch-widen-probe-into-hacking-of-official-sites.html?_r=1; *see also* The Associated Press, *Hacking in the Netherlands Took Aim at Internet Giants*, N.Y. TIMES, Sept. 5, 2011, http://www.nytimes.com/2011/09/06/technology/hacking-in-the-netherlands-broadens-in-scope.html.

84. Kevin J. O'Brien, *Hacking in Netherlands Points to Weak Spot in Web Security*, N.Y. TIMES, Sept. 12, 2011, http://www.nytimes.com/2011/09/13/technology/hacking-in-netherlands-points-to-weak-spot-in-web-security.html.

dimension when it was revealed that the security breaches extended beyond Dutch government websites; the security certificates of 531 websites, including web domains owned by the Central Intelligence Agency in the U.S., by Mossad, Israel's intelligence agency, and by M16, the United Kingdom's Secret Intelligence Service, were all compromised.[85] How serious was the breach? One anti-virus researcher for a security firm called the attack the instigation of a "cyber war."[86]

Even before these reports surfaced, research showed that most U.S. wireless customers, citing security concerns, either did not trust mobile banking or failed to appreciate its potential value.[87] In many cases, those security concerns are well-founded. Due to their ability to access the Internet remotely and in unsecured environments, cell phones are vulnerable to the risks currently plaguing traditional desktop or laptop computers.[88] Unfortunately, there are additional risks that are specific to phones.

First, as cell phones are small and portable, they are easier to steal and conceal.[89] Second, just like computers, cell phones can become infected with viruses; with cell phones however, those viruses can be more easily spread to other cell phone users or to networked computers connected to the phones, allowing cybercriminals access to the information.[90] At least on a home computer, one is generally protected by anti-virus software such as Norton Antivirus, McAfee, or other programs that are familiar to most people who are purchasing computers. Even if many consumers do not regularly update their subscriptions to such security measures, at least most computers either come with such software installed, or with prompts to allow installation. James Lyne, a security expert for UK-based software developer Sophos, confirms that many people do not think about similar protection for their mobile devices.[91]

Another instance where computers are more secure than mobile phones is that on a computer, one can delete small tracking files called "cookies." Smartphone users have a limited ability to do the same with mobile applications.[92] In fact, some say that smartphones are "powerless" to limit tracking.[93]

85. Matt Liebowitz, *Cracked Digital Certificates Endanger 'Web of Trust'*, SECURITY NEWS DAILY, Sept. 7, 2011, http://www.msnbc.msn.com/id/44430823/ns/technology_and_science-security/.

86. *Id.* ("Most of our work is digital. But now we have to use notes, which is like a step back in time … For courts and lawyers, this is an administrative nightmare.").

87. *See* VAMOSI, *supra* note 7, at 188; *see also* Dan Nystedt, *Wireless Growth in Asia Leads to Security Woes*, IDG NEWS SERV., Dec. 13, 2006.

88. Cara Garretson, *Mobile Devices Expose Networks to Security Threats*, PC WORLD, Feb. 23, 2007, http://www.pcworld.idg.com.au/article/175124/mobile_devices_expose_networks_security_threats/.

89. Moskvitch, *supra* note 4.

90. Marcia MacLeod, *Success of Mobile Devices Builds Security Opportunities*, MICROSCOPE, Dec. 4, 2006.

91. Moskwitch, *supra* note 4.

92. Kane & Thurm, *supra* note 77.

Banking through wireless technology presents unique security concerns because wireless networks are much more difficult to secure than wired networks.[94] Unlike wired connections, wireless signals, like radio waves, travel through the air and can be easily intercepted.[95] This feature has wide-ranging implications for cell phone use—not only for threats to consumer security from criminal activities carried out by hackers who "are starting to pay more and more attention to handsets,"[96] but also for even innocuous operations by cell phone manufacturers and carriers. Once widely known, certain vulnerabilities implicit in cellular phone use may undermine consumers' willingness to trust the security of their phones for an entire range of activities; in particular, the failure to address these security issues will mean that consumers will be less likely to rely on their phones for completing financial transactions, including mobile banking.

Threats to privacy are not limited to cybercriminals however, as cell phone carriers are not only able to track the Internet surfing habits of their customers; they can also easily track the physical whereabouts of their customers.[97] Using a "signal triangulation process" and GPS, they can locate any individual customer by tracking the location of her cell phone.[98] Perhaps location-based tracking will not be a huge issue; after all, many consumers already willingly "check in" with their friends (and potentially millions of other people) by sharing their physical whereabouts through the use of popular cell phone applications like Foursquare.[99] It seems plausible however that bank customers making large or confidential deposits, or taking advantage of other financial services, would expect a higher measure of privacy in regards to these activities.

Cell phones are also susceptible to surveillance in ways that, while not necessarily impacting mobile banking specifically, may also have consequences for wide-scale adoption of applications that might jeopardize sensitive financial transactions. For example, cell conversations are also susceptible to eavesdropping: someone using a Bluetooth device and "Car Whisperer" software can listen in on a conversation happening in the car just ahead on the freeway (without the owner's knowledge and even when the driver's phone is not powered on);[100] cell phone microphones can be accessed and remotely turned on

93. *Id*.

94. Nystedt, *supra* note 87; *see also* Vamosi, *supra* note 7, at 186.

95. Vamosi, *supra* note 7, at 58.

96. Moskvitch, *supra* note 4.

97. BRETT KING, *BANK 2.0: HOW CUSTOMER BEHAVIOR AND TECHNOLOGY WILL CHANGE THE FUTURE OF FINANCIAL SERVICES* 121 (2010).

98. *Id*. at 123.

99. *Privacy 101*, FOURSQUARE LABS INC., https://foursquare.com/privacy/ (last visited Dec. 20, 2010); *see also* Vamosi, *supra* note 7, at 60, 161.

100. Vamosi, *supra* note 7, at 72.

through "roving bugs," or a microphone can be inserted into a cell phone to listen in on meetings.[101] Cell phone cameras can be accessed remotely, possibly recording your movements and likeness.[102]

While much of the public may be unaware of the full potential for remote access of their cell phones, in most instances, the technology is not new and is already utilized by automobile companies, wireless service providers, the FBI, and other law enforcement personnel.[103] The general public should be informed of the risks inherent in using cell phones for transmitting sensitive information of all kinds, whether oral or written. Banks, cell phone providers and wireless carriers should play a role in ensuring customer safety and the federal government should also require these providers to ensure certain minimum levels of security.

In an effort to access a myriad of services now available through their cell phones, consumers are willingly sharing their personal records with multiple parties,[104] including personal information that previously would have been more guarded. This information can be retained and stored by service providers, as well as by various unregulated third parties. Often, these parties are acting for proper purposes; they may store this information to help these companies increase efficiency and value for customers who are utilizing online services.[105] Third parties may also retain these records in an effort to confirm that appropriate transactions were initiated and properly authorized by customers.[106]

Yet personal financial records, health records, or other highly sensitive data stored remotely in large online databases, are prime targets for cybercriminals. Even though cell phone companies may well have a clear interest in keeping these records private, accidents and security breaches of consumer records in other similar contexts is not uncommon.[107] Most identity theft is usually com-

101. MacLeod, *supra* note 90.

102. Vamosi, *supra* note 7, at 182 ("Privacy as many of us grew up knowing it is gone forever, thanks to technology (think of pinhole video cameras and the spyware that turns on the camera and microphone on a cell phone).").

103. Declan McCullagh, *FBI Taps Cell Phone Mic as Eavesdropping Tool*, CNET, Dec. 1, 2006, http://news.cnet.com/2100-1029_3-6140191.html.

104. *See* Jeffrey L. Hare, *Regulatory Considerations for Mobile Banking*, 13 ELECTRONIC BANKING & COM. REP. 2, 7 (2008).

105. Robert Sprague & Corey Ciochetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 95 (2009).

106. Hare, *supra* note 104 at 7 ("There are multiple parties behind every bank SMS you receive, like software developers, wireless provider, telecommunications companies and third party vendors/ platforms").

107. J. Prynn, *Banks Blasted over Data Protection*, 7/11/07 BSX-EVSTND, 2007 WLNR 13142333 ("The 2006-7 report by the Information Commissioner's Office says12 high-street banks discarded customer data in unsecured outside bins."); *see also* Ian C. Ballon, *Security Concerns Over Online and Mobile Banking*, E-Commerce and Internet Law, *citing* Internet Crime Complaint Center, *IC3 2008 Annual Report on Internet Crime*, Mar. 31, 2008, http://www.ic3.gov/media/2009/090331.aspx ("For example, data breaches were responsible for losses exceeding $239 million in 2007 and $265

mitted by insiders who have access to confidential information, including credit reports or financial statements, usually by virtue of their position.[108]

Identity theft expert Robert Siciliano states that 70% of all identity theft is committed by insiders, including "bank employees, phone operators and government agencies." Other evidence indicates that besides the known cases, there are also many unreported cases of "insider-related" security breaches, including breaches by third parties who often have no direct contact with customers.[109] For all of the foregoing reasons, banks and other service providers that retain mass quantities of customer or patient information need to monitor any third parties and institute standards for the maintenance and security of these records.

The issue of securing privacy in the telecommunications world, and particularly on mobile phones, may soon begin to receive additional coverage in the news media. Recent evidence suggests that even though wireless providers have tried to find ways to ensure users' privacy, hackers are able to find ways around the few security protocols that are being utilized. In particular, many smartphone owners may not be aware that there is little that they can do to protect themselves.[110]

VII. VARIOUS APPROACHES TO ONLINE RECORD STORAGE AND DATA PROTECTION

"The EU approach to protecting privacy — comprehensive national laws, prohibitions against collection of data without a consumer's consent and requiring companies that process data to register their activities with government authorities — is in stark contrast to the U.S. approach, which to date has been more ad hoc and industry-based."[111]

Another problem is that U.S. consumers may be less secure than many of their counterparts in Europe and other parts of the developed world.[112] In an effort to increase convenience for the public, U.S. government agencies, hospi-

million in 2008.").

108. Tom Ahearn, *Insider Identity Theft: Could Your Co-Worker be an Identity Thief?* PRE-EMPLOY.COM (Nov. 6, 2009, 10:39 AM), http://www.pre-employ.com/blog/post/2009/11/06/Insider-Identity-Theft-Could-Your-Co-Worker-Be-an-Identity-Thief.aspx.

109. Kevin P. Kalinich, *Red Flags, Broken Hearts, and Data Breach Stimulus, Insurance for Breaches of Data Privacy and Information Security*, AON CORP., June 2009, http://one.aon.com /files/red_flags_broken_hearts.pdf.

110. Kane &Thurm, *supra* note 77 ("Smartphone users are all but powerless to limit the tracking. With few exceptions, app users can't 'opt out' of phone tracking, as is possible, in limited form, on regular computers. On computers it is also possible to block or delete 'cookies,' which are tiny tracking files. These techniques generally don't work on cell phone apps.").

111. Larose, *supra* note 34.

112. Nancy Feig, *Everyone's Ready for Mobile Banking Except Consumers*, BANK SYS. AND TECH, March 16, 2007, http://www.banktech.com/blog/227101289.

tals, banks, wireless, transit, and other service providers are expanding the availability of online services. Instead of filling out paper forms, in many places you can now purchase transit cards, complete and submit your taxes, access medical records and communicate with your health care provider, pay bills, and confirm or challenge financial transactions—all online.

The process of "going digital," or moving away from paper record-keeping to online file storage adds and will continue to add value to the lives of thousands of consumers. Imagine being able to access your prescriptions, medical records, and other basic health care services through your phone; further, imagine being able to communicate with your doctor without waiting weeks or months for your next scheduled appointment. You do not need to imagine it, because these services are already being piloted among certain health care facilities.[113] Unfortunately, moving from a system of paper records to electronic and digital file storage poses certain increased risks.[114]

The federal Health Insurance Portability and Accountability Act ("HIPAA") was passed by Congress in 1996.[115] Under HIPAA's "Privacy Rule," implemented in 2003, health plans, health care providers, and health care clearinghouses must follow certain minimum standards in maintaining the privacy of client records (whether those records are in paper form, oral, or electronic), and must disclose information regarding privacy policies to patients.[116] The "Security Rule" specifically protects health records that are stored in electronic form.[117] HIPAA does not have a set time period for the retention of these records, although states may choose to impose such time limits. Under California law for example, hospitals must retain patient (not including minors) records for a minimum of seven years following a patient's discharge.[118] Dur-

113. Blue Cross Blue Shield is just one of many health care providers who send real-time updates via text message to patients' phones. On their website, one message reads: "Text BABY to 511411. Get FREE messages on your cell phone to help you through your pregnancy and your baby's first year." BLUECROSS BLUESHIELD OF LOUISIANA, http://www.bcbsla.com/Pages/Home.aspx (last visited Nov. 15, 2012).

114. Privacy Rights Clearinghouse, *HIPPA Basics: Medical Privacy in the Electronic Age*, https://www.privacyrights.org/fs/fs8a-hipaa.htm (last visited Sept. 11, 2011) ("Today you have more reason than ever to care about the privacy of your medical information. Intimate details you revealed in confidence to your doctor were once stored in locked file cabinets and on dusty shelves in the medical records department. Now, sensitive information about your physical and mental health will almost certainly end up in data files. Your records may be seen by hundreds of strangers who work in health care, the insurance industry, and a host of businesses associated with medical organizations. What's worse, your private medical information is now a valuable commodity for marketers who want to sell you something.").

115. Heath Insurance Portability and Accountability Act of 1996 (HIPPA), Pub. L. No. 104-191; *see also* Privacy Rights Clearinghouse, *supra* note 114.

116. Privacy Rights Clearinghouse, *supra* note 114.

117. U.S. Dep't of Health & Human Serv., *Understanding HIPPA Privacy*, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html. For the full text of the "Security Rule," see http://aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf.

118. American Health Information Management Association, *Practice Brief—Retention of Health Care Records* (Table 4: State Laws or Regulations Pertaining to Retention of Health Information),

ing this time period and beyond, these records are available to many other entities besides the ones covered under the Act, including employers, life insurers, state, municipal agencies, and law enforcement agencies.[119]

Unlike many countries in Europe, confidential records in the United States like health records can be stored indefinitely by cell phone or other companies, who can then share or sell name, address and other information.[120] Recent reports highlight the risk of loss of confidential personal information through cell phone providers, including an investigation in April 2011 as to whether information gathered and shared by Pandora, an online music service, as well as by popular iPhone and Android smartphone applications, has been inadequately secured.[121] More specifically, the question is whether Pandora or these apps either illegally obtained and shared customer data without customer consent, or failed to notify customers that personal information about their phones, their location, and usage was being shared with advertisers, marketers and other parties.[122] In another case, mobile operators of Orange (a mobile phone carrier) shared customer log-in information, which was then easily accessed by unauthorized staff.[123]

The Wall Street Journal ("WSJ") conducted its own independent review of 101 mobile phone applications and found many instances where customer's personal data was vulnerable. Specifically, the WSJ found that:

- Fifty-six applications transmitted the phone's unique device ID to other companies without users' awareness or consent;
- Forty-seven applications transmitted the phone's location in some way;
- Five applications sent a user's age, gender, and other personal details to outsiders;
- Forty-five applications failed to provide any privacy policy whatsoever, either on their websites or inside the applications themselves; and
- An Android application for MySpace transmitted user's

available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_012547.pdf.

119. U.S. Dep't of Health & Human Serv., *supra* note 117.

120. Privacy Rights Clearinghouse, *supra* note 39; *see also* Vamosi, supra note 7 at 172.

121. Laurie Segall, *Pandora Targeted in Smartphone Privacy Probe*, CNN MONEY (Apr. 4, 2011, 4:51 PM), http://money.cnn.com/2011/04/04/technology/pandora_subpoena/index.htm.

122. Amir Efrati, Scott Thurm & Dionne Searcey, *Mobile-App Makers Face U.S. Privacy Investigation*, WALL ST. J., Apr. 4, 2011, http://online.wsj.com/article/SB10001424052748703806304576242923804770968.html.

123. Prynn, *supra* note 107.

income, ethnicity, and parental status information.[124]

The WSJ also discovered that even though Apple and Google affirmed that they require their applications to obtain customer consent before transmitting personal information, this was not always the case.[125]

Smartphone makers and telecommunications providers have tried to allay customer concerns, stating that most smartphone applications merely track information anonymously; they say that any data that is passed on is not, and cannot be linked to any particular user by name or other personally identifying information.[126] However, the investigators at the WSJ found that most smartphone users, without fully realizing the impact of their actions, unwittingly volunteer personal information, including age and gender, which could potentially be used, along with other information, to identify specific persons.[127] So even if companies are not actively seeking this data, your information is still out there in cyberspace and is available for others to locate and use without too much additional effort. Apple's co-founder, Steve Jobs, admitted that securing customer privacy in this area is a problem. He stated, "[applications] want to take a lot of your personal data and suck it up."[128]

Why are these companies releasing potentially sensitive consumer information? Industry insiders suggest that since advertisements that are targeted by location bring in "two to five times as much money as untargeted ads," some application developers' motives are most likely profit driven.[129] If these companies could see that they could also increase market share—and thus profits—by finding ways to guarantee a more secure environment, more Americans might worry less about security and more fully comprehend the value in mobile banking.

Again, certain companies, including Apple, claim that very little personally identifying information is actually released.[130] Perhaps many consumers would not care about the release of records stripped of name, or other personally identifying information. However, not everyone is comfortable with even this concession. In at least one suit, Lalo v. Apple, Inc., filed in December 2010 in the U.S. District Court for the Northern District of California, the claimants allege that these applications "have been transmitting their personal, identifying in-

124. Kane & Thurm, *supra* note 77 (The Wall Street Journal report found that one iPhone app, TextPlus4, "sent the phone's unique ID number to eight ad companies and the phone's zip code, along with the user's age and gender, to two of them.").

125. *Id.*

126. *Id.*

127. *Id.* (marketing companies can also use this information for advertising and promotional purposes).

128. *Id.*

129. *Id.*

130. *Id*.

formation ('PII') to advertising networks without obtaining their consent."[131]

In the U.S., these privacy and security threats have been mostly unheralded, and not enough has been done to alert and warn the unsuspecting public. Consequently, there is a lack of consumer awareness about data sharing policies, and a lack of consent, as might be manifested by prominent opt-in or opt-out policies. The United Sates Congress recently acknowledged:

> . . . As of 2011, the level of public awareness of cyber security threats is unacceptably low. Only a tiny portion of relevant cyber security information is released to the public . . . Information about attacks on private systems is ordinarily kept confidential.[132]

Policy analysts, aware of the pressing need to address these threats, confirm that the threat of e-crime could derail the growth of mobile financial services.[133] The development and spread of mobile banking will only succeed if there is sufficient consumer confidence and trust. Yet experts predict sharp increases in attacks against mobile devices as more financial institutions roll out mobile banking initiatives.[134] The various players—wireless providers, banks, cell phone companies—would be well-advised to issue warnings to consumers and get out ahead of these attacks, even if these warnings ultimately risk profits. Just as using a smartphone is often less secure than working on a traditional computer or wired network,[135] banking or completing financial transactions using mobile technology also presents unique security concerns than would be otherwise present in a physical bank or ATM location.[136]

Some warnings might advise mobile phone users to try to avoid the problem entirely by simply not using their cell phones to conduct any financial transactions while located in public places and using unsecured networks or unauthenticated Internet websites. Savvy consumers might also take affirmative steps to boost the security of their personal and financial data by installing firewalls and by purchasing encryption software.[137] Realistically however, it is unlikely that most people will take the time to even complete these simple steps.

131. Complaint at 2, Lalo v. Apple, Inc. et al., No. 5:10-CV-5878 (N.D. Cal. Dec. 23, 2010).

132. S. 813 112th U.S. Cong. § 2 (2011); *see also* Stu Sjouwerman, *U.S. Government Escalating Efforts to Fight Cybercrime*, *KNOWBE4*, May 16, 2011, http://blog.knowbe4.com/category/cybercrime-2/.

133. Pickens, *supra* note 79, at 11.

134. John Blau, *Experts: 2007 Bodes Ill for Mobile Banking*, IDG NEWS SERVICE, Jan. 22, 2007, http://www.computerworld.com/s/article/9008788/Experts_2007_bodes_ill_for_mobile_banking.

135. Garretson, *supra* note 88; *see also* Nystedt, *supra* note 87.

136. Nystedt, *supra* note 87; *see also* Vamosi, *supra* note 7, at 77.

137. Vamosi, *supra* note 7, at 76.

VIII. WHAT ARE OUR PRIVACY LAWS AND HOW HAVE THEY BEEN INTERPRETED?

"If you try to create privacy by passing more laws, there will always be people who will break those laws."[138]

The laws relating to privacy and security regarding mobile banking come from a range of sources. This section will first briefly address case law in this area, and then several federal and state statutes that should be updated to address privacy and security in the mobile and wireless arena.

In terms of case law, consumer privacy litigation has mostly consisted of class action lawsuits based on claims of intrusive marketing techniques by telemarketers in making unsolicited calls or sending messages to consumers.[139] Although there are very few reported decisions in this area, two types of claims predominate—complaints regarding spam received via text message, and complaints regarding unauthorized charges for unsolicited messages or calls.[140]

These cases address privacy concerns from the perspective of a consumer's right to not have her personal information collected and disseminated for marketing purposes: "Increasingly, individuals are being electronically 'shadowed' online, our actions and behaviors observed, collected, and analyzed so that we can be "micro-targeted."[141] This interest in having the right to opt out of bothersome "calls" made for the purpose of advertising specific goods and services is not the same as the interest in keeping personal financial data secure (from threats posed by weaknesses inherent in electronic data storage and retention methods used by financial institutions, health care providers, and wireless carriers), and is not the interest covered by this Article. Unfortunately, there is virtually no case law on the latter subject, but there are indications that this will soon change.

On the federal level, there are many statutes that address consumer protection and privacy rights. One problem is that when it comes to the regulation of privacy and data security, it is difficult to answer the question of which regulatory agency is in charge, and which law should apply. Ideally, there should be a more unified approach, particularly when it comes to concerns about emerging technologies. Yet those responsible for either providing or regulating mo-

138. Vamosi, *supra* note 7, at 182.

139. Clark & Kimrey, *supra* note 45 ("In 2010 alone, courts have approved class action settlements with funds of $36 million and $12.25 million. However, none of these cases has ever been tried."); *see also* Jeffrey Weinstein et al. v. AirIt2Me Inc., et al, No. 06 c 0484 (shoe company settles junk text class action for $7 million).

140. The complaints are typically for unjust enrichment, tortious interference, trespass to chattels, and violation of state consumer fraud statutes. Clark & Kimrey, *supra* note 45.

141. *Protecting Privacy, Promoting Consumer Rights and Ensuring Corporate Accountability*, CENTER FOR DIGITAL DEMOCRACY, http://www.democraticmedia.org (last visited Sept. 7, 2011).

bile banking services work across several industries, including the telecommunications industry (encompassing wireless carriers and telecom or mobile content providers), the banking and finance industry (including banks, credit unions, investment firms and brokerages), and a web of overlapping regulatory agencies working under competing state and federal laws. Jurisdiction is shared in this area by the Federal Trade Commission ("FTC"), the Federal Communications Commission ("FCC"), and the Department of Justice ("DOJ"), among a host of others.

A. Federal Laws

Current federal law generally protects consumers from a wide range of privacy intrusions, including those specifically facilitated through the use of the Internet and cell phones. Through these mediums, the public is exposed to additional risks, including invasions caused by intrusive solicitation through telemarketing calls and text messages, data mining and sharing of consumer information by marketing companies, and pornographic images and content. Most of the relevant federal statutory privacy protections stem from four federal laws, including:

I. The Telephone Consumer Protection Act of 1991 ("TCPA");[142]

II. The Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM");[143]

III. The Children's Online Privacy Protection Act of 1998 ("COPPA")[144]; and

IV. The Gramm-Leach-Bliley Act of 1999 ("GLB").[145]

These laws potentially provide a significant amount of protection for consumers—that is assuming the average consumer is able to figure out the particular law that might apply in a given situation and has the right to file suit under the law. However these laws are still being tested in the courts and are susceptible to legal challenges.

142. Telephone Consumer Protection Act, 47 U.S.C. § 227 (1991).

143. Controlling the Assault of non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7701 (2003).

144. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2001).

145. Gramm Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (1999).

1. TCPA

In enacting the TCPA, Congress explicitly stated that its goal was to protect consumer privacy.[146] The legislature thought that there ought to be a way to protect consumers against the hassle of receiving unsolicited and bothersome telemarketing calls at home.[147] As discussed below, the TCPA creates a private right of action, and confers exclusive jurisdiction on state courts to entertain it.[148]

At its outset, the TCPA was mainly intended to protect the privacy interests of residential telephone subscribers."[149] Congress felt that the public needed special protection from the types of calls that caused the most disturbance to the greatest number of people; they decided to target calls not initiated by human beings but made with mechanical assistance—either through the use of an "automatic telephone dialing system or with an artificial pre-recorded voice."[150] According to the TCPA, an automatic dialing system is one in which the equipment has the capacity to either "store or produce telephone numbers to be called, using a random or sequential number generator," or to dial such numbers.[151]

Their concern was that with the use of automatic dialers, telemarketers could make anonymous and repeated calls to the same numbers over and over again with little cost to themselves, but at great inconvenience and bother to recipients.[152] Legislators felt that these calls, if placed in the evening hours when recipients were most likely to be home, were especially intrusive.

The TCPA mandates that any person or company in the U.S. wishing to make telemarketing solicitation calls to individuals "using any automatic telephone dialing system or an artificial or prerecorded voice," in the absence of an emergency affecting the health or safety of the consumer, or with whom they

146. *See* Lozano v. Twentieth Century Fox Film Corp., 702 F. Supp. 2d 999, 1008 (N.D. Ill. 2010); *see also* Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 954 (9th Cir. 2009); Bonime v. Avaya, Inc., 547 F.3d 497, 499 (2nd Cir. 2008) ("Congress's stated purpose in enacting the TCPA was to protect the privacy interests of residential telephone subscribers.").

147. S. Rep. No. 102-178 at 5 (1991), *reprinted in* 1991 U.S.C.C.A.N. 1968, 1972-73 (1991) ("The Committee believes that Federal legislation is necessary to protect the public from automated telephone calls. These calls can be an invasion of privacy, an impediment to interstate commerce, and a disruption to essential public safety services.").

148. 47 U.S.C. § 227(b)(3) ("A person or entity may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State— (A) an action based on a violation of this subsection or the regulations prescribed under this subsection to enjoin such violation, (B) an action to recover for actual monetary loss from such a violation, or to receive $500 in damages for each such violation, whichever is greater, or (C) both such actions."); *see also* Italia Foods, Inc. v. Sun Tours, Inc., 927 N.E.2d 682 (Ill. Ct. App. 2010).

149. *Lozano*, 702 F. Supp. 2d at 1008; *see also Satterfield*, 569 F.3d 946 at 954; *Bonime*, 547 F.3d 497 (emphasis added).

150. 47 U.S.C. § 227(b)(1)(A).

151. 47 U.S.C. §227(b)(1)(A)(iii) (emphasis added).

152. R. 37-1, Ex. B, 102 Cong. S. Hrg. 102-918, at 68 (Oct. 10, 1991).

do not have a pre-existing relationship, must first obtain express consent from the recipient, [153] or face a significant fine from the FCC (up to $1,500 in some cases) for each violation.[154] More specifically, automated or prerecorded calls cannot be made to any emergency telephone line (e.g., '911' lines or emergency lines for hospitals, doctor's offices, fire departments, police stations, or poison control centers), nor to patients in hospitals, nursing home or other health care facilities, to any service where the party is charged for the call, nor to residential telephone lines.[155]

Under the law, "any person who has received more than one telephone call within any 12-month period by or on behalf of the same entity may sue in state court,"[156] or an action may be brought by states, via state attorney generals or designated state agencies.[157]

In terms of relief, remedies for the individual bringing the action may include an injunction, damages for any actual monetary loss due to the invasion (say, for example, if a consumer cannot place an emergency call because the line is tied up by the automated solicitation call), or $500 in damages per violation.[158] A party can defend against an action by proving that it used due care in implementing policies to prevent the prohibited telephone solicitations.[159]

Although by its terms, the language of the TCPA neither explicitly contemplates its application to messages received on mobile phones via text message, nor explicitly defines the term "call,"[160] the FCC has interpreted the statute to include text messages and calls to wireless numbers within the definition.[161] The FCC's interpretation of the statute, and specifically of the kinds of "calls" falling within its purview was challenged;[162] however, courts applying "Chevron Deference" to the FCC's interpretation that such calls should be included,[163] agreed to extend coverage: "While a text message may not tie up a call-

153. *Lozano*, 702 F. Supp. 2d at 1011 (quoting Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm. of NY, 447 U.S. 557, 566 (1980)); *see also* TCPA § 227(b)(1)(A).

154. TCPA § 227(f)(1).

155. TCPA § 227(b)(1)(A)(i)- (iii).

156. TCPA § 227(c)(5).

157. TCPA § 227(f)(1).

158. TCPA § 227(b)(3).

159. *Lozano*, 702 F. Supp. 2d at 1011

160. *Id.* at 1004 (the TCPA does not require a call to be oral).

161. *See In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 18 F.C.C.R. 14014 (2003); *see also* 47 U.S.C. §227 (b)(2) ("The TCPA grants the FCC the authority to "prescribe regulations" to implement the requirements of §227(b).").

162. *Lozano*, 702 F. Supp. 2d at 1008 (Telemarketing firms challenged the law in court on First Amendment grounds, stating that Section 227(a) of the Act represents an unconstitutional restraint on commercial speech, especially when applied to the actual use of a random autodialer, rather than to the mere capacity to store, produce or dial telephone numbers using a random or sequential number generator).

163. *Id.* at 1003 ("Courts must defer to agency interpretation of a statute where Congressional intent is unclear, and a statute affords an agency authority under the statute." (quoting Chevron v. Natural Res. Def. Council, 467 U.S. 837, 842-43 (1984))); *see also id.* at 1006 ("The Court refuses to give com-

er's cellular phone line for receipt of a voice call, text messages pose the same irritation, interruption and potential costs to consumers as voice calls."[164]

Accordingly, courts have interpreted the TCPA to cover not only calls made to residential numbers, but to also include voice and text-based calls to mobile phones.[165] Courts have said that the fact that mobile phone subscribers are often charged by their wireless service providers for such unsolicited text messages is relevant, and weighs in favor of expanding the prohibition of text messages under the Act.[166] This means that banks or financial institutions need to be cautious about seemingly innocuous automated or prerecorded messages, whether text or voice, to those who do not have a prior customer relationship with the bank or financial institution.

Generally, mobile banking is distinct from telemarketing or unsolicited advertising as it does not usually occur in the absence of an established client relationship. However, banks and other financial institutions need to confine such messages to existing customers, or to those with whom the institution already has a relationship and from whom consent has been obtained. In servicing both existing and potential customers, banks need to carefully safeguard customer information (including contact information, account numbers and passwords), and make sure that they do not share, whether inadvertently or not, customer information. For example, if a bank customer asked a bank to transfer funds to another person, the bank could run afoul of the Act by initiating a prerecorded or text-based "call" to the non-customer to ask for consent or for other information to complete the transaction.[167] The bank might have innocently attempted to accede to the customer's request, but in this way, a seemingly innocuous contact could be interpreted as a "solicitation" within the terms of the Act.

Although it is unlikely that by its terms, the TCPA would apply to banks who are conducting mobile banking, as banks expand the range and reach of their mobile banking services, there are situations where banks or other financial institutions could be implicated.

plete deference to the FCC (because the FCC failed to invite specific comments on the application of the TCPA to text messaging), but does afford limited deference because the FCC's interpretation is "reasonable and consistent with the language and purpose of the TCPA.").

164. *Lozano*, 702 F. Supp. 2d at 1008 (quoting Abbas v. Selling Source, LLC, No. 09 CV 3413, 2009 WL 4884471, *7 (N.D. Ill. 2009).

165. *Id.* at 1011 (quoting Central Hudson Gas & Electric Corp. v. Public Service Comm. of NY, 447 U.S. 557, 566 (1980)).

166. *Id.* at 1001.

167. Kristen Marshall, *Get It in Writing: Changes to the FCC Consent Rules*, COPILEVITZ & CANTER LLC *(May 2012)*, http://www.copilevitz-canter.com/resources/articles/get-it-in-writing-changes-to-the-fcc-express-consent-rules *(*Banks are now also subject to the same standard for prerecorded calls under FCC rules).

i. The Do Not Call Registry[168]

Under the TCPA, the FTC and the FCC were jointly charged by Congress with establishing and regulating the national "Do Not Call Registry."[169] Telemarketers are prohibited from calling (or sending unwanted text messages to wireless numbers if sent using an autodialer) consumers who have registered phone numbers on the list and indicated that they do not wish to receive solicitation calls.[170] Civil sanctions, enforced by the DOJ on behalf of the FTC, can include penalties of up to $11,000 per violation, injunctions against future violations, and the disgorgement of profits.[171] Through a complaint procedure, state and local law enforcement may access consumer information to aid in the enforcement of the statute.[172]

Do Not Call primarily appears to impact those institutions or companies making unsolicited advertising or promotional calls; again, calls made to customers with pre-existing relationships are likely excluded.

2. CAN-SPAM

Similarly, CAN-SPAM also relates to unsolicited marketing or advertising and supplements some of the protections carved out under the TCPA. Both the FCC and the FTC have adopted rules in this area—FCC rules prohibit sending unwanted commercial email messages to wireless devices without prior permission, and FTC rules restrict sending unwanted commercial email messages to computers.[173]

Under CAN-SPAM, companies may not send unsolicited commercial e-mail messages to consumers unless such messages are first labeled as advertising.[174] Under both CAN-SPAM and FCC regulations, a company also may not send any advertisements by text to wireless devices like cell phones unless the company expressly, either verbally or in writing, obtains prior consent in advance.[175] There must be an opt-out mechanism to allow recipients to choose to

168. Do Not Call Implementation Act, 15 U.S.C. § 6101 (2003).

169. Richard C. Balough, *The Do-Not-Call Registry Model is Not the Answer to Spam*, 22 J. MARSHALL J. COMPUTER & INFO. L. 79, 82 (2003).

170. FED TRADE COMM'N., *Annual Report to Congress for FY 2006 Pursuant to the Do Not Call Implementation Act on Implementation of the National Do Not Call Registry*, April 2007.

171. *Id*.

172. *Id*.

173. FEDERAL COMMUNICATIONS COMMISSION GUIDE, SPAM: UNWANTED TEXT MESSAGES AND EMAIL (2011), http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email.

174. Vivian L. Polak, *Balancing Technology and Privacy: Emerging Rules in Online Behavioral Advertising, Mobile Marketing, Social Networking and Other Electronic Commercial Communications*, 1006 PLI/Pat 439 (2010) (Westlaw).

175. Consent must also be specific. "For example, a consumer who authorizes that a car repair company send her a notice when the car repairs are complete has not provided blanket authorization to receive text ads from the company." *Id.*

avoid email solicitations.[176] Only a limited private right of action exists under the statute; only Internet Service Providers can sue[177] (although the Act does not provide for a private right of action by other recipients of spam, it does authorize the federal government, state attorneys general, and Internet service providers to bring actions against violators). [178] Consumers have the option of filing complaints directly with the FCC,[179] and remedies that states may receive on behalf of their residents include injunctive relief, statutory damages not to exceed $2,000,000, or aggravated damages for willful or knowing violations.[180]

CAN-SPAM has been used in class action litigation by those who claim injury due to the receipt of large amounts of "spam," including unsolicited, false or deceptive advertising messages. Specifically, the statute covers more than just bulk email:

> It covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," including email that promotes content on commercial websites. The law makes no exception for business-to-business email. That means all email – for example, a message to former customers announcing a new product line – must comply with the law.[181]

Notably, the statute does not implicate messages received by consumers who have pre-existing relationships with financial institutions or who have already consented to such contact (these are considered transactional or relationship messages rather than commercial advertising or promotion),[182] so mobile banking services generally would not come within the statute's reach. However, such services could pose a problem if considered to be a commercial solicitation.

Also, banks and other financial institutions might be subject to CAN-SPAM for transactional messages in cases where the institution uses deceptive or fraudulent information in the message or header of an email if the injury ris-

176. Liisa M. Thomas, *Balancing Technology and Privacy: Emerging Rules in Online Behavioral Advertising, Mobile Marketing, Social Networking and Other Electronic Commercial Communications, in* 1006 PRACTICING LAW INSTITUTE, PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 439, 425 (May 24-25, 2010).

177. *See, e.g.*, 15 U.S.C. §§ 7704(a)(1), 7704(b), or 7704(d) et seq.

178. 15 U.S.C. § 7106(f)(1).

179. Gordon v. Virtumundo Inc., 575 F.3d 1040 (2009) (Plaintiff did not have standing because he was not a provider of Internet service).

180. 15 U.S.C. § 7106(1-3).

181. Federal Trade Commission, CAN-SPAM Act: A Compliance Guide for Business, (Sept. 2009); *see also* Bureau of Consumer Protection, CAN-SPAM Act: A Compliance Guide for Business, http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business.

182. 15 U.S.C. § 7702(2).

es above the level of "mere annoyance."[183] This has been interpreted to mean that a bank must send so many promotional e-mails that it prevents consumers from using their mobile devices normally.[184] Further, the situation where a transfer is sent to a third person and a bank then sends a text message to the recipient's mobile phone would likely not present a problem under the statute because the message would not be considered a solicitation.[185] Also, the FTC has stated explicitly that a consumer-forwarded message is not subject to CAN-SPAM regulation.[186] For all of the foregoing reasons, it appears that the full force of this statute is inapplicable to financial institutions, and is therefore mostly unavailable to protect mobile banking consumers.[187]

3. COPPA

The FTC also assumes responsibility for regulating COPPA. The point of COPPA is to protect the privacy rights of children, aged 12 and under, from potential threats garnered through their use of the Internet: "Congress enacted COPPA in 1998 to limit the collection of personally identifiable information from youngsters without their parents' consent."[188] The statute requires that commercial websites directed to children specifically take affirmative steps to secure children's privacy online. These websites must post privacy policies, notify parents of any information collected regarding their children, and obtain consent before collecting or sharing such information with others.[189]

If a commercial website is generally not directed at children but nevertheless has "actual knowledge" that it is collecting personal information from children, it must comply with COPPA. Any failure to comply with the statute can lead to criminal sanctions. Since COPPA is limited by its own terms to websites that are directed at children, including websites that offer homework help, allow children to play games, or take part in quizzes and online contests,[190] it is unlikely that the statute will serve to protect adult consumers from the security and privacy threats that are of concern in this Article. Banks and other financial institutions generally do not direct their online or mobile appli-

183. *See* Cherny v. Emigrant Bank, 604 F. Supp. 2d. 605 (S.D.N.Y. 2009) (A bank has to send so many promotional emails that it impairs the consumer's ability to use their device normally).

184. *Id.*

185. Ballon, *supra* note 107 at 503.

186. *Id.* at 527.

187. *See* Cherny, *supra* note 183 (After providing bank with unique e-mail address, plaintiff began receiving spam messages on that account and sued but the court dismissed the case saying (1) there was no standing under CAN-SPAM because the injury needed to rise above the level of annoyance, and (2) plaintiff was not an Internet Service Provider.)

188. FED. TRADE COMM'N., *Protecting Children's Privacy Under COPPA: A Survey on Compliance* at 1 (April 2002).

189. *Id.*

190. FED. TRADE COMM'N., *supra* note 188 at 5.

cations to children. Further, even if a financial institution did happen to collect information regarding a minor child, it is likely that such information would be pursuant to a pre-existing customer relationship with the parent or subject to previously given parental consent.

In March 2010, the FTC announced plans to review and address emerging technological developments, especially those concerning mobile communications:

> Of special concern to the Commission is the expanded use of mobile technology to access the Internet, and whether it should broaden the definition of "Internet" to specifically include the new interactive and mobile technologies.
>
> As to privacy, the Commission is investigating whether web operators and network advertising companies have the ability to use information collected from children online, including persistent IP addresses, mobile geolocation information, and data assembled from behavioral advertising programs.[191]

Significantly, the FTC has urged that COPPA should be updated to account for the need to address new mobile technologies and online practices, including location tracking, facial recognition software, and the prevalence of tracking cookies on websites.[192] It remains to be seen whether the proposed updates will address all of the issues posed by these technologies, but at least there appears to be a widespread recognition that the law is outdated.

4. Gramm-Leach-Bliley

> *"It is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers' nonpublic personal information."*[193]

One purpose of GLB is to protect consumer privacy by establishing guidelines regarding disclosures and consents that financial institutions must give and obtain in order to secure the confidentiality and integrity of their customers' information.[194] Through the statute, the FTC imposes specific disclosure obligations to govern relationships between financial institutions and their cus-

191. JOSEPH B. FAZIO, INTERNET LAW AND PRACTICE § 19:25 (July 2011) (emphasis added).

192. John Moe, *FTC Urges Update to COPPA*, AM. PUB. MEDIA TECH REPORT BLOG, (Sept. 16, 2011, 8:38 AM), http://www.publicradio.org/columns/marketplace/tech-report/2011/09/ftc-urges-update-to-coppa.html.

193. Gramm-Leach-Bliley Act § 501.

194. GLB also allows certain entities, including banks and financial services providers, to consolidate their activities. *See* 15 U.S.C. § 6801 (1999); *see also* Gramm-Leach-Bliley Act §501(b) (directing regulatory agencies to "set standards: 1) to insure the security and confidentiality of consumer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and 3) to protect against unauthorized access to, or use of such records or information which could result in substantial harm or inconvenience to any customer.").

tomers. The definition of "financial institution" clearly includes banks, but could also cover other businesses that maintain consumer financial information, including car dealerships, home repair contractors, and real estate agents. [195]

Under GLB, at the start of a relationship with any financial institution, customers are entitled to: 1) an initial disclosure statement which discloses their rights and obligations; and 2) continuing annual reminders of the institution's privacy policies.[196] GLB provides that within these disclosures, a financial institution that intends to share confidential and personal customer information with any third party must provide the customer with the right to opt out, along with a notice of that right.[197] The statute states that the definition of "nonpublic personal" information includes "any information that is associated with a person who can be identified, which a customer gives the financial institution in connection with a transaction or service."[198]

Under the statute, customer information is still protected even if such information is publicly available elsewhere. Financial institutions are only allowed to disclose customer information in order to comply with federal, state or local laws in conjunction with a civil, criminal or regulatory investigation by federal, state or local authorities.[199] GLB does not provide or imply a private right of action, but must be enforced by federal or state authorities.[200] Significantly, GLB also provides room for further state action; Section 507(b) allows individual states to enact legislation that would provide an even greater level of privacy protection for customer financial data than is provided under the Act itself.[201]

IX. STATE LAWS: FOCUS ON CALIFORNIA

Some states have suggested that liability for security breaches should not rest on banks but on the parties directly responsible, where such individuals can be found.[202] Banks are already heavily regulated; perhaps there should be in-

195. Gramm-Leach-Bliley Act § 509(3) (Financial institution is defined broadly and includes "any institution, the business of which is engaging in the financial activities described in BHCA [the Bank Holding Company Act] Section 416 (which includes banking, securities, underwriting, investment advisory and insurance services.)").

196. Gramm-Leach-Bliley Act § 7.03.

197. *Id.*

198. *Id.*

199. *See* Gramm-Leach-Bliley, *supra* note 201, at § 502(e)(8). Examples cited by the statute include discovery requests in aid of a child support enforcement action (§521(g)), or in prosecution of certain financial crimes, including insurance fraud (§ 521(e)).

200. *See* Bowler v. Green Tree Servicing, LLC, 2011 WL 320398 (E.D. Cal. 2011); *see also* Dunmire v. Morgan Stanley DW, 475 F.3d 956, 960 (8th Cir. 2007).

201. Gramm-Leach-Bliley Act § 507(b) (this is referred to as the "Sarbanes Amendment" of Section 507).

202. Rebecca Dent, *The Role of Banking Regulation in Data Theft & Security*, 27 REV. BANKING & FIN. L., 381, 392 (2008).

creased focus on law enforcement efforts, including more international cooperation between national security agencies, to combat data theft and cybercrime. On the local level, California may provide a model of how states may pass more laws to protect their citizens.

As stated above, GLB gives states the ability to add more stringent protections than are offered at the federal level.[203] In fact, "[i]n the vacuum of federal guidance, twenty-two (22) states (at last count) have enacted their own regulatory guidelines."[204] Many states, for example, specifically require companies to notify customers of security breaches of their information.[205] California, once ranked third among other states in the number of identity theft victims,[206] has been proactive in crafting legislation to protect consumers' privacy rights, and was also the first state to establish a statewide "Office of Privacy Protection."[207]

Further, California has a long list of statutes that are intended to address consumer privacy, including:

The California Online Privacy Protection Act of 2004 (Assembly Bill 1950 amends Cal. Civ. Code 1798.81.5(b)(c)) provides that businesses that own or license personal information about California residents must implement and maintain reasonable security measures. The statute also provides that a specific provision be included in contracts in which sensitive personal information will be shared with third parties. Regarding mobile banking, banks will have to implement and maintain reasonable security measures to protect customer information, and can require third parties (wireless carriers) to carry out the safety procedures as well. Cal. Civ. Code § 1798.81.5(b)(c).

Sections 22948.5 – 22948.7 of the California Business and Professions Code (formerly California Assembly Bill 2415) requires wireless home networking equipment manufacturers to warn consumers about the dangers of unsecured Wi-Fi networks. Specifically, manufacturers of wireless network devices must include a warning label on how to protect the wireless network connection from unauthorized access.[208]

203. Gramm-Leach-Bliley, *supra* note 201, at § 507.

204. Peter Mucklestone and Stuart Louie, *The Uncertain Landscape of Data Breach Notification*, PRIV. & SEC. L. BLOG (Jan. 10, 2006), http://www.privsecblog.com/2006/01/articles/security-breaches/the-uncertain-landscape-of-data-breach-notification ("The problem is that many of these state laws conflict with one another, define breaches differently and offer varying thresholds for notification triggers.").

205. Those states include: Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, North Carolina, North Dakota, Nevada, New Jersey, New York, Ohio, Rhode Island, Tennessee, Texas and Washington. Cohn, Armstrong & Heiman, *supra* note 10, 28.

206. Kim, *supra* note 22.

207. *Id.* at 131.

208. *See* Naomi Graychase, *California Law to Require Wi-Fi Warnings*, WI-FI PLANET, Oct. 19, 2006, http://www.wi-fiplanet.com/news/article.php/3638936; Nate Anderson, *California Wants WiFi*

The California Financial Information Act allows a consumer to direct a financial institution to not share personal information. Note that the Ninth Circuit has held that part of this Act was pre-empted by FCRA in American Bankers Ass'n v. Lockyer, 541 F.3d 1214 (9th Cir. 2008).

The California Identity Theft Statute (Cal. Civ. Code §1798; see also Penal Code § 530.5) requires state agencies and other California businesses to disclose any security breaches regarding information of California residents. Cal. Civ. Code §1798.

California Business and Professions Code § 17529.5 regulates unlawful activities relating to commercial email advertisements.

In addition, under California's Financial Information Privacy Act,[209] bank customers in the state may exercise more control over their financial records than under federal law: a consumer must provide consent before a bank may share any personal information with a non-affiliated third party.[210]

In terms of the protection of health care records, as of January 2003, under the Confidentiality of Medical Information Act, California imposes security standards that are more protective than those required under federal law and HIPAA. These rules mandate that patients must be notified within five days of any breaches of their health information.[211] Anyone who illegally uses, discloses, or accesses private medical records can face either civil penalties, including actual and punitive damages (up to $2,500 for negligent disclosures, from $2,500 up to $25,000 per violation for knowing and willful violations, and up to $250,000 for disclosures for financial gain), or criminal sanctions.[212]

California's response to the problem of data breaches of private consumer information is the appropriate course of action; it is targeted to address electronic threats and is comprehensive—it includes financial institutions of varying stripes, private companies, health care providers and facilities, state agencies, and wireless carriers. Currently, at least forty-three other states also require notice to individuals of security breaches regarding their personal information.[213] These developments bode well for efforts to protect information stored on portable devices like cell phones, and for the future of mobile bank-

Warning Stickers, ARS TECHNICA, Aug. 31, 2006, http://arstechnica.com/uncategorized/2006/08/7633/.

209. Cal. Fin. Code § 4052(a) (2004) (A consumer must provide consent before a bank can share any personal information with a non-affiliated third party. This "opt-in" procedure is different from the "opt-out" method under Gramm-Leach Blilely.); *see also* Kim, *supra* note 22.

210. Cal. Civ. Code § 1798.81.5(b)(c) (2006). (Note: This is an "opt-in" statute, as opposed to federal "opt-out" regulations under Gramm-Leach-Bliley.).

211. Privacy Rights Clearinghouse, *supra* note 114.

212. *Id*.; *see also* Cal. Civ. Code §§ 56-56.10 (2011) (The Confidentiality of Medical Information Act), *available at* http://www.ohi.ca.gov/calohi/MedicalPrivacyEnforcement.aspx.

213. California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information*, May 2008, at 6.

Securing Mobile Technology & Financial Transactions in the United States

ing.

X. SCOPE OF REGULATION: SETTING STANDARDS FOR CONSUMER PROTECTION

Some media commentators blame the problems underlying the most recent financial crisis on deregulation. In the U.S. at least, there has been an outcry against what many perceive as the banks' failure to police themselves and the financial industry:

> Responsible finance is much in the news these days, as the fallout from irresponsible financial practices and products in the United States and other developed markets continues to affect global finance . . . . One silver lining of the global financial crisis is that more attention is being paid to financial consumer protection.[214]

Setting comprehensive, uniform, and clear standards regarding mobile banking is a challenge precisely because there are so many parties involved — regulatory agencies, wireless carriers, wireless providers, merchants, and financial institutions—in addition to a significant number of overlapping regulations.[215] Regulators at the Federal Reserve have acknowledged the conflict:

> There is certainly a great concern within the group about what the regulatory oversight structure is for mobile payments. I mean, you have now entering into the payment stream the mobile operators, who are typically overseen by the FCC. But the FCC doesn't oversee, historically, payments activity . . . And so I think that's an important issue that comes out, and it would sure be nice to get ahead of something, rather than figure it out afterward this time . . . [216]

The primary challenge in advocating for a change in laws to protect mobile banking customers is to know where, and how, to start. Historically, the organizations that protect consumers have been distinct from those that guide and regulate financial institutions, and this fragmentation complicates any effort to combine the two aspects. In addition, the significant number of players on the business side also complicates matters: "A variety of competing business sectors — from telecoms to financial institutions to Internet companies — are launching pilots of new technology they hope will replace consumer reliance

214. Laura Brix & Katherine McKee, *Consumer Protection Regulation in Low-Access Environments: Opportunities to Promote Responsible Finance*, CONSULTATIVE GROUP TO ASSIST THE POOR, Feb. 2010 at 1 (focus note).

215. VENABLE LLP, MOBILE BANKING (2008) [hereinafter VENABLE WHITE PAPER], http://www.venable.com/files/Publication/3188a11e-fbaa-45fe-a7be-0089cd384c3c/Presentation/ PublicationAttachment/52cc19ac-dd18-4cf6-b471-0863ee93a47d/2010.pdf.

216. Interview with Richard Oliver, Executive V.P., Fed. Reserve Bank of Atlanta, *Fed's Predictions for the Future of U.S. Mobile Payments*, PYMNTS.COM (April 15, 2011), http://pymnts.com/Exclusive-Interview-Fed-s-Predictions-for-the-Future-of-U-S-Mobile-Payments-Transcript/.

on credit cards with the wave or tap of a mobile phone. The problem is, no one knows which agency should regulate."[217]

The National Telecommunications and Information Administration, an executive branch agency that is mainly responsible for advising the President on telecommunications and information policy issues, is coordinating a dialogue between the business sector and privacy groups to develop standards regarding privacy and mobile phones.[218]

The CFPB is tasked with providing additional oversight of financial products, services, and transactions for American consumers.[219] Under Section 1031 of the Dodd-Frank Act, the CFPB has the authority to write rules regarding unfair, deceptive or abusive acts or practices.[220] The Federal Financial Institutions Examination Council ("FFIEC") establishes standards and provides guidance to financial institutions.[221] The Office of the Comptroller of the Currency charters, regulates, and supervises all national banks and federal savings associations. Within the telecommunications industry, organizations like the Mobile Marketing Association ("MMA") and the Wireless Association have set forth standards for safeguarding consumer privacy. These standards are not enforceable however, and are more akin to suggested "best practices" for the industry. Ultimately, all are concerned with the same goal—how to make sure that in the midst of changing times, consumer protections are maintained.

In a recent Politico article, author Elizabeth Wasserman confirms the general sentiment in the industry that no one is really sure how to effectively regulate mobile banking: "As more Americans learn how to shop with their cellphones, Washington is trying to figure out who should answer the call to regulate this new form of commerce . . . "[222] James Wester, a frequent contributor on the website "Mobile Payments Today: Technology, Trends and Insights," concurs that the topic of regulation of mobile banking is complicated: "The fact is mobile payments represent the forced marriage of two of the most

217. Wasserman, *supra* note 5 ("Mobile payments may cross regulatory domains covered by many different federal agencies. The Federal Reserve Board, Federal Deposit Insurance Corp., Office of the Comptroller of the Currency and other agencies regulate banking. The Federal Communications Commission has authority over wireless carriers. The Federal Trade Commission, meanwhile, protects consumers from fraud and privacy violations.").

218. Brendan Sasso, *Report Calls for Tougher Rules to Protect Cellphone Location Data*, HILLICON VALLEY, Oct. 11, 2012, http://thehill.com/blogs/hillicon-valley/technology/261575-report-calls-for-tougher-rules-to-protect-cellphone-location-data.

219. "The central mission of the Consumer Financial Protection Bureau (CFPB) is to make markets for consumer financial products and services work for Americans—whether they are applying for a mortgage, choosing among credit cards, or using any number of other consumer financial products." CONSUMER FIN. PROTECTION BUREAU, http://www.consumerfinance.gov/the-bureau/ (last visited Nov. 14, 2011).

220. *See* Dodd-Frank Act, *supra* note 25.

221. Hare, *supra* note 104 at 5.

222. Wasserman, *supra* note 5.

unregulated industries we have: telecommunications and financial services."[223]

It does seem clear, however, that attempts to set best practices by the MMA should be supported by enacting or strengthening consumer protection provisions aimed specifically at mobile banking and the provision of mobile services. The Payment Card Industry Security Standards Council ("PCI Council"), a global forum launched in 2006 consisting of global payment brands (like American Express, MasterCard, and Visa), is responsible for the development of standards to help keep data secure for mobile payment systems.[224] Unfortunately, the PCI Council has no power to enforce these standards.

As explained above, the FCC, the FTC, the Federal Reserve and other regulators are all overseeing the financial and banking sectors.[225] Yet despite the plethora of regulatory oversight, security issues concerning mobile payments do not currently seem to be a top priority: "That's a lot of regulatory authority hovering over the industry and yet there's an Alfred Newman, "What, me worry?" attitude toward the topic. Why worry when mobile payments are still a nascent technology, right?"[226] Still, there are those within the government and in consumer protection agencies that recognize the problem and are actively working towards a solution.

XI. RECOMMENDATIONS: EXPAND REGULATORY OVERSIGHT AND STREAMLINE AGENCY ACTION

"I think what we'd love to see is the various regulators—the FTC, the FCC, the banking regulators, commerce, who has privacy concerns right now, and maybe even the new Consumer Financial Protection Bureau—kind of come together and figure out, when you look at a mobile payments application, where's the jurisdictions that are going to look at various parts of it, and how it's going to be regulated then."[227]

A. Recommendations for the Federal Government . . .

The Federal Reserve is cognizant of the hurdles to getting mobile payments off the ground in the United States.[228] One of the most basic pre-requisites for

223. James Wester, *What, me worry?* MOBILE PAYMENTS TODAY, Apr. 15, 2011, http://www.mobilepaymentstoday.com/blog/5633/What-me-worry.

224. *PCI Issues New Guidance for Mobile Payment Apps*, MOBILEPAYMENTSTODAY.COM, http://www.mobilepaymentstoday.com/article_print/182200/PCI-issues -new-guidance.com (last visited Nov. 14, 2011); *see also* PCI, *About the PCI Security Standards Council*, https://www.pcisecurity standards.org/organization_info/index.php.

225. Wester, *supra* note 223.

226. *Id.*

227. Interview with Richard Oliver, *supra* note 216.

228. *Id.* According to Richard Oliver, an executive vice president with the Federal Reserve Bank

success of the mobile banking model is client protection. If mobile banking is to become a success, banks and other financial institutions must focus on protecting client privacy. What seems clear is that until the various players find a way to work together to help further develop mobile banking systems, solutions will have to be tailored to the different constituents. There are, however, promising signs that meaningful change is on the horizon. The FTC recently released a report on online consumer privacy,[229] and called for legislation that would give consumers access to information collected by "data brokers."[230] Also, federal regulators, members of advertising trade groups and technology companies said that they would support a consumer privacy bill of rights, and even a voluntary "do not track" system whereby consumers could prevent the collection of their personal data as they surf the Internet.[231]

Similarly, at least one scholar, Professor Sandy Pentland of the Massachusetts Institute of Technology, believes that the privacy and security issues that come with new technologies are so important that there should be a "New Deal" on data privacy.[232] This New Deal, similar to the transformative economic policies introduced by U.S. President Franklin D. Roosevelt in response to the Great Depression and rampant poverty, could be instrumental in realigning the national consciousness with regard to the emerging data security and privacy issues implicit with the spread of mobile technologies.

Specifically, Professor Pentland offers the following recommendations:

- Users should own the information generated by "gadgets;"
- Users should have the right to state how and when they want data collected through opt-in and/or opt-out procedures;
- Companies that collect user data should create a file, allowing you to see your data at any time; and

of Atlanta, the three biggest hurdles to getting mobile payments off the ground include: 1) There is no general agreement on business model that applies to all the parties in the system; 2) Managing increased expenses that merchants will have to incur to upgrade terminals to accept mobile payments and getting people to want to use smartphones in order to do their banking; and 3) Standards—there doesn't appear to be much agreement on what standards should be used. *Id*.

229. Federal Trade Commission Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 2010).

230. Tanzina Vega, *FTC Seeks Privacy Legislation*, BRADENTON HERALD, Mar. 26, 2012, http://www.bradenton.com/2012/03/26/3962731/ftc-seeks-privacy-legislation.html.

231. *Id.* The FTC has suggested that consumers should be able to access information collected by companies whose purpose is to sell the data for marketing purposes, and that these companies should explain their data collection policies to consumers. These proposals would not affect small businesses or companies that collect information from fewer than 5,000 people and do not sell data to third-parties. *Id*.

232. Vamosi, *supra* note 7, at 183; *see also* Jia-Chaun Kwok, *Sandy Pentland on the Future of Mobile*, ENTREPRENEURSHIP REVIEW BLOG (Sept. 24, 2010, 4:58 PM), http://miter.mit.edu/article/sandy-pentland-future-mobile.

- Europe has use-limitation laws, the U.S. does not. In Europe, personal account information cannot be sold or stored for more than two years.[233] The U.S. should enact similar protections.[234]

Another recommendation is that those who either own or license customer data, including wireless carriers and providers, should be required to report security breaches of customer data directly to customers.[235] One solution would be to require telecommunications providers and mobile phone manufacturers to distribute and enforce privacy policies for all smartphone applications using their platforms. The previously cited WSJ Report found that of the 101 applications tested, 45 did not have a privacy policy in place.[236]

The federal government could mandate that the mobile industry come up with a standard set of guidelines and practices that should regulate the industry.[237] Already, the FTC has taken action and is calling for industry trade groups "to accelerate the pace of self-regulation."[238] Self-regulation by the industry is entirely feasible as international mobile operators like Vodafone, Coca Cola and Turner Broadcasting have all agreed to adopt guidelines "designed to give customers more control over how data about them is used."[239] These companies have recognized the importance of addressing valid privacy concerns and the potential impact on consumer confidence.

B. Recommendations for the Mobile Phone Industry . . .

Most cellular telephone companies currently operating in the United States use Global System for Mobile ("GSM") security technology.[240] This is despite the fact that almost all mobile platforms using GSM encryption for mobile banking, mobile commerce, and other financial transactions can be easily compromised: "Some security analysts claim that there is not even a pretense of secrecy in GSM."[241] Many industry experts believe that one solution is to change to [Qualcomm] Code Division Multiple Access ("CDMA"), which would make intercepting or eavesdropping on a call almost impossible.[242] Currently, Sprint

233. Vamosi, *supra* note 7 at 183-184.

234. *Alex Pentland, Reality Mining of Mobile Communications: Toward a New Deal on Data*, The Global Information Technology Report, 2008-2009, World Economic Forum, at 79.

235. Cohn, Armstrong & Heiman, *supra* note 10, at 36.

236. Kane & Thurm, *supra* note 77.

237. *Id*. ("Lack of standard practices means different companies treat the same information differently").

238. Vega, *supra* note 230.

239. *Privacy Controls to be Adopted by Mobile Phone Operators*, BBC NEWS, April 25, 2012, http://www.bbc.co.uk/news/technology-17833302.

240. Vamosi, *supra* note 7 at 51.

241. *Id.*

242. *Id.*

and Verizon are the only wireless carriers who use CDMA technology.[243] Upgrading existing cellular towers and accompanying equipment requires additional resources and is not easily accomplished.[244]

On the other hand, while updating and implementing more secure encryption technology is clearly a priority, on the international level, mobile phone companies in Europe (including Orange, Vodafone and Deutsche Telekomare) are leading the charge by focusing on applications they produce. They have agreed to follow new privacy guidelines by the GSMA that would give customers notice about app privacy policies and allow customers more control over the use of their information.[245]

Current federal laws like the ones discussed in this Article are inadequate in that they do not fully address security issues implicit in emerging technologies, including threats particular to portable mobile devices. Michelle Jun, a staff attorney at Consumers Union states: "Federal law protects consumers in the event their credit card or debit card is lost, stolen or misused, but current protections are 'badly fragmented' and do not necessarily extend to all types of emerging mobile payments."[246] Existing criminal laws—which address threats to cybercrime presented by hackers and other malicious Internet users—provide a means of security, but as the recent example from the Netherlands demonstrates, rising incidents of sophisticated cybercrime present a problem that is clearly not dissipating.

As it stands now, many consumers are inadequately protected by current industry standards. The good news is that the FTC has signaled that it is making both the development and enforcement of industry-wide codes of conduct a priority, and that it is also coordinating efforts with the White House and the Commerce Department.[247]

C. Recommendations for States . . .

As mentioned above, under GLB §507(b), states have the power to provide more protective measures for their residents than are granted under federal law as GLB §507(b) states:

243. *Id.*

244. *Id.* at 53.

245. *Mobile Firms Back New GSMA App Privacy Guidelines*, BBC NEWS, Feb. 28, 2012, http://www.bbc.co.uk/news/technology-17178954.

246. Kate Fitzgerald, *Mobile Payments May Pose Fraud Threat, Consumer Advocacy Group Warns*, PAYMENT SOURCE BLOG *(Aug. 25, 2010)*, http://www.paymentssource.com/news/mobile-payments-fraud-threat-consumer-advocacy-group-3003054-1.html.

247. Tanzina Vega and Edward Wyatt, *U.S. Agency Seeks Tougher Consumer Privacy Rules*, N.Y. TIMES, March 26, 2012, http://www.nytimes.com/2012/03/27/business/ftc-seeks-privacy-legislation.html ?_r=1. (Independent from any action endorsed by the FTC, Senators John Kerry and John McCain introduced a bill in the Senate in April 2011 to require companies to tell consumers what data is being collected and allow them to opt out of the practice.).

> (b) Greater Protection Under State Law. For purposes of this section, **a State statute, regulation, order, or interpretation is *not* inconsistent with the provisions of this subtitle if the protection such statute, regulation, order, or interpretation affords any person is *greater than the protection provided under this subtitle and the amendments made by this subtitle*,** as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under section 505(a) of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.[248]

Individual states should therefore take advantage of this provision in order to play a significant role in devising appropriate legislation to protect consumers from the distinct threats associated with mobile technology. In particular, states should follow the lead of California in devising laws that force mobile carriers and applications to create and widely disseminate privacy policies regarding their collection, storage and potential transmission of customer data to third parties.

As discussed above, California has been innovative in requiring businesses to maintain reasonable security measures, in requiring wireless equipment manufacturers to warn consumers about unsecured wireless networks, and in requiring state agencies and local businesses to disclose security breaches involving residents' information directly to consumers. Where federal law allows, state law should fill in the gaps to provide addition protection to state residents.

D. Recommendations for Businesses . . .

> *"Consumers will ultimately seek out companies that pro-actively work to create a privacy-respecting experience."*[249]

Businesses that collect consumer data and information, including those that share or sell that information with third parties, should clearly state their privacy policies and make sure that such policies are widely disseminated so that consumers can make informed decisions regarding the types of transactions they wish to conduct using mobile devices.[250] These companies should also provide opt-out procedures for consumers who do not wish to be tracked or to have their information stored or sold. Companies should do this not only

248. Gramm-Leach-Bliley, supra note 201, at § 507(b) (emphasis added).

249. *Mobile Firms Back New GSMA App Privacy Guidelines*, BBC NEWS, Feb. 28, 2012, http://www.bbc.co.uk/news/technology-17178954.

250. *Clarity Call for Mobile and Internet Privacy*, BBC NEWS, May 24, 2011, http://www.bbc.co.uk/news/business-13522071.

to protect consumers, but also to protect their own bottom-line, as failure to act could serve to preempt the development of new technology in the future.[251]

One international privacy group specifically called out the "Big Three"—Google, Apple and Microsoft—to "develop technical solutions that prevent apps from having unwarranted access to personal information in the first place."[252] While this would indeed be a great start, other businesses that share or sell consumer information on a large-scale should also be proactive and self-regulate.

Businesses should also take greater precautions when they issue, or require employees to use company smartphones. Pixel Electronics, a Belarusian company that gave all 50 of its employees smartphones, has addressed their concern with data security by requiring each employee to register their mobile devices with the company's IT department, to get a pass code, and to have anti-virus software installed on their phones.[253]

E. Recommendations for Consumers . . .

Some say that privacy is becoming an increasingly outdated concept.[254] Nevertheless, there should be more public education about the security of mobile devices. Some consumers use their mobile phones in unsecured public areas like Internet cafes or airport lounges without realizing that it is fairly easy for an attacker to gain access to their devices. Consumers should be warned to either avoid using their smartphones or laptops to log into their bank accounts or to conduct financial transactions while in such public places, or to make sure to install strong firewalls and password protections on such devices.[255]

XII. CONCLUSION

"Demographic and technological trends suggest that financial institutions can't afford to sit out the Mobile Banking wave waiting for a number of technical, legal and regulatory issues to be sorted out."[256]

251. *Id*. Bob Warner, Chairman of the Communications Consumer Panel, states, "A lack of confidence in how private information was handled could curtail the development of new technology."

252. *Mobile Firms Back New GSMA App Privacy Guidelines*, BBC NEWS, Feb. 28, 2012, http://www.bbc.co.uk/news/technology-17178954.

253. Moskvitch, *supra* note 4.

254. This is the argument of Sam Biddle, a technology writer for Gizmodo.com: For the smartphone customer "it's a trade-off in terms of privacy versus service. Following you around is just part of the service." *See* Brian Wheeler, *How Much Privacy Can Smartphone Owners Expect?*, BBC NEWS, Nov. 22, 2011, http://www.bbc.co.uk/news/magazine-15730499.

255. Vamosi, *supra* note 7 at 76; *see also* G. Fest, *Authentication: Can You Protect Me Now?*, 2007 WLNR 21527657 (Nov. 1, 2007).

256. VENABLE WHITE PAPER, *supra* note 215.

The main concern of this Article is with both the privacy and security of consumer financial information with respect to mobile devices. On the one hand, the growth of mobile banking can be partly attributed to the use of targeted advertising which is dependent on the collection and storage of information about consumers.[257] On the other, the collection and retention or sharing of this information poses increased privacy and security risks for consumers as this information is often "shared more broadly than understood or intended by consumers or used for purposes not contemplated or disclosed at the time of collection."[258]

Where not already existing, consumers should be not only put on notice about these collection practices, but should also be granted a private right of action for data breaches that lead to the disclosure of confidential and personally identifying information. This right should stem, especially in states that already recognize a right to privacy, from existing common law; in states that do not already recognize a common law or constitutional right to privacy, this right should stem from new state statutory law.

As financial institutions, telecommunications providers, and cell phone manufacturers are unlikely to voluntarily agree on a single set of standards, Congress should step in with new legislation to help address the problem. Although there are many agencies with jurisdiction in this area, all of these agencies are authorized by Congress to act and a new mandate regarding privacy and mobile or wireless devices is advisable. In fact, some of these agencies now acknowledge that there is a need for enhanced privacy protection for consumers with respect to mobile devices, as well as the need for coordinated efforts among and between themselves.[259] If mobile banking takes off in the U.S. as it has in many other parts of the developed and the developing world, there will be a sufficient federal stake in regulating the industry for the benefit of all U.S. consumers. The point is not to wait until there is a scandal or public outcry "to focus the minds of politicians and telecom executives."[260]

Under existing laws, many institutions are already legally required to secure the personal information of U.S. consumers in other contexts. There are federal laws, including GLB and HIPAA, and others mentioned in this Article that apply to a broad spectrum of financial institutions. On the state level, California has taken laudable steps to protect consumer privacy and has established

257. Federal Trade Commission Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 2010), at 21.

258. *Id*., at 21-22.

259. For example, the FTC announced that it would hold two workshops to "address data privacy on mobile devices and social media Web sites and by Internet service providers and operating systems." The agency also agreed to "work with the Department of Commerce to create enforceable self-regulatory codes of conduct for companies that collect data in specific sectors, such as mobile and social media." Vega, *supra* note 230.

260. Wheeler, *supra* note 254.

a plethora of laws all aimed at securing electronic systems. These laws, especially those that recognize and address concerns regarding weaknesses in electronic systems and data breaches, serve an important purpose.

However, emerging technologies, and mobile banking in particular, need additional attention. On the one hand, some would say that privacy and data security issues are already garnering a great deal of debate at the national level; there is just disagreement as to which body should assume primary responsibility.[261] One might surmise that the reluctance and inability to enact comprehensive national legislation protecting privacy,[262] (and our current legislative formula of overlapping statutes with varying jurisdictional limitations) might be attributed to deference to the First Amendment, states' rights or the Commerce Clause: "*The U.S. privacy model is a mixture of laws, regulations and industry self-regulation rather than a single, comprehensive federal data protection law. Free market and freedom-of-speech principles predominate.*"[263]

Perhaps these issues will be resolved if the White House's Office of Cybercrime and the CFPB decide to utilize their mandate to not only address cybercrime, but to also tackle the separate issue of data security and mobile banking. On the other hand, our failure to enact additional legislation might be attributed to a fear of overregulation. Some might argue that it is not appropriate to ask the federal government to address issues that might rightly be left to states, banks, telecommunications providers and private companies.

Regardless of the source of authority, it seems clear that much more can be done to secure mobile financial transactions for the average U.S. consumer. We could expand regulatory oversight of the wireless industry and clarify and streamline existing standards and legislation in order to address vital privacy

261. Larose, *supra* note 34 ("A dozen bills have been filed in Congress. A leading measure in the Senate would force companies to bolster data security practices and notify consumers whose information is stolen . . . lawmakers are divided over what information should be covered, the role of the Federal Trade Commission in enforcing a new law and the relationship of the federal law with existing state laws on data breach notification.").

262. For example, the Electronic Frontier Foundation and the American Civil Liberties Union of Northern California ("ACLU") struggled to pass legislation in California, *the Location Privacy Act of 2012* (formerly Senate Bill 1434), that would have prohibited law enforcement from monitoring the movements of U.S. mobile phone owners (via phone companies who can easily track the location of their customers) without a warrant. Although the bill was passed by the California Senate and Assembly, the bill was vetoed by Governor Brown. *See* Chris Conley, *Governor Brown Vetoes Location Privacy Act*, ACLU, Sept. 30, 2012 https://www.aclunc.org/issues/technology/blog/governor_brown_vetoes_ location_privacy_act.shtml. In contrast, the U.S. Supreme Court found in *U.S. v. Jones* that attaching a GPS device to a vehicle and then using the device to monitor the vehicle's movements constitutes a search under the Fourth Amendment, perhaps setting the stage for future federal legislation on the issue. *See* Dahlia Lithwick, *Alito v. Scalia: The Two Conservative Supreme Court Justices Brawl over Technology and Privacy*, SLATE, Jan. 23, 2012, http://www.slate.com/articles/news_and_politics/ jurisprudence/2012/01/u_s_v_jones_supreme_court_justices_alito_and_scalia_brawl_over_technology_and_privacy_.html.

263. Larose, *supra* note 34. *See e.g.*, Levitt v. Fax.com, Inc., 383 MD. 141, 857 A.2d 1089 (2004) (TCPA does not violate the Commerce Clause or the Tenth Amendment).

and security concerns. We should do this, not because there is a problem that has already grown out of hand, but because we recognize the potential for additional progress and growth. The expansion of mobile banking services is particularly attractive as an instrument of financial access and inclusion for disadvantaged and low-income populations, who use alternative financial service providers such as check cashers or payday lenders,[264] but ultimately it will benefit all U.S. consumers. Rather than burying our collective heads in the sand in regards to existing and later emerging risks, we should be proactive and act now to make mobile technology more secure for financial transactions.

264. Braunstein, *supra* note 40. Sandra Braunstein, testifying before the U.S. Senate Committee on Banking, Housing and Urban Affairs stated: "Such technologies also hold the potential to expand access to mainstream financial services to segments of the population that are currently unbanked or underbanked. That said, the technologies are still new, and important concerns, such as consumers' expressions of unease about the security of these technologies, must also be addressed for consumers to feel confident about adopting these new services." *Id.*