SMARTPHONE USAGE AND THE NEED FOR CONSUMER PRIVACY LAWS

By Laura E. Gomez-Martin

Volume XII – Spring 2012

ABSTRACT

Many Americans use smartphones for a variety of personal, recreational, and business affairs. While the increasing popularity of smartphones and mobile technology has advanced communication, new uses have created privacy breaches of personal and consumer information. This article examines the different ways that American smartphone users use their mobile devices as well as the various types of data created.

This article also explores the vulnerabilities faced by smartphone users. Vulnerabilities occur through the use of traditional hacking and malware, but can extend to the collection and dissemination of personal and consumer information by smartphone applications. The article concludes by examining different solutions for privacy breaches. Some solutions may be implemented on an individual or institutional level. Other solutions to privacy breaches require the enforcement and extension of legislation upon telecommunication companies and application developers.

SMARTPHONE USAGE AND THE NEED FOR CONSUMER PRIVACY LAWS

By Laura E. Gomez-Martin

Volume XII – Spring 2012

The advent of cell phones revolutionized the way many individuals worldwide communicate. The increased use of smartphones, which serve multiple purposes and allow a user to be connected to e-mail and the internet, has led to a lot of personal information and consumer data being stored on mobile devices. While smartphone technology has opened the door for more efficient communication as well as recreational and business affairs, it has also led to privacy breaches of personal and consumer data. The trend towards "open development platforms" which facilitate user-created applications has added to breaches. These breaches have created new privacy issues that often occur so rapidly that legislation necessary to protect consumers cannot keep pace.

Many smartphone users are unaware that their mobile device acts as a small computer, subject to the same vulnerabilities as a large personal computer. This note will inform readers about the different capabilities of smartphones, the privacy issues that arise, as well as provide an examination of the existing and potential legislative solutions that could protect smartphone users from data breaches. Part I will summarize the data and information produced by users of smartphones to conduct personal, recreational, and business affairs. Part II will discuss some of the non-traditional and emerging risk factors faced by smartphone users along with a discussion on the privacy policies that exist for applications. Part III will focus on different solutions to solving smartphone privacy breaches. Some of these solutions are individually driven, some institutionally driven, and others require the enforcement and extension of legislation upon the telecommunication companies and application developers.

I. Smartphone Use

Today, many Americans utilize their cell phones to conduct personal, recreational, and business affairs. According to research by the Pew Internet and American Life Project, eighty-three percent of American adults have cell phones.[1] It is estimated that thirty percent of American mobile users have a smartphone, as opposed to a traditional cell phone.[2] The widespread use of cell phones has created new public safety issues due to talking and texting behind the wheel. In 2011, the National Safety Council (NSC) estimated that around twenty-three percent of all automobile accidents in the U.S. are caused when a driver is talking or texting.[3] With the increasing popularity of cell phone usage, many states have restricted the use of cell phones by drivers. According to the Governors Highway Safety Association, nine states currently ban the use of hand-held cell phones, while thirty-five states ban texting while driving.[4]

Many Americans use their cell phones for more than just the traditional means of communication. Applications, or apps for short, allow smartphone customers to use their phones for a variety of different functions. Available apps range from games, tutorials on various lifestyle topics, social networking, and banking – to name a few. Many companies that offer services and products, in stores and online, have created apps to appeal to mobile users' needs. Stores that offer app services include: Amazon.com, Overstock.com, H&R Block, Walmart, and Best Buy.[5] Currently, the iPhone app store has more than 500,000 available programs for users

[1] Kristen Purcell, Roger Entner & Nichole Henderson, *The Rise of Apps Culture*, PEW INTERNET AND AMERICAN LIFE PROJECT (Sept. 15, 2010), http://pewinternet.org/Reports/2010/The-Rise-of-Apps-Culture/Overview/Main-Findings.aspx.
[2] Amy Gahran, *Report: 90% of Americans Own a Computerized Gadget*, CNN (Feb. 03, 2011), http://articles.cnn.com/2011-02-03/tech/texting.photos.gahran_1_cell-phone-landline-tech-gadget?_s=PM:TECH.
[3] Kathy Lane, *National Safety Council Estimates that at Least 1.6 Million Crashes Each Year Involve Drivers Using Cell Phones and Texting*, NATIONAL SAFETY COUNCIL (Jan. 12, 2010), http://www.nsc.org/Pages/NSCestimates16millioncrashescausedbydriversusingcellphonesandtexting.aspx.
[4] *Cell Phone and Texting Laws*, GOVERNORS HIGHWAY SAFETY ASSOCIATION (Mar. 2012), http://www.ghsa.org/html/stateinfo/laws/cellphone_laws.html.
[5] *See Google Play*, GOOGLE, https://play.google.com/store (last visited Mar. 27, 2012).

to download.[6] It is estimated that twenty-nine percent of adult users have downloaded an app onto their cell phones.[7] Additionally, since the debut of the iPhone and Android app stores, an estimated forty billion apps have been downloaded.[8] Though the use of apps is extremely popular on smartphones, advancements in technology have also influenced other traditional cell phone functions.

Cell phones have been increasingly manufactured with more sophisticated cameras. Without taking into account the amount of time spent talking on a cell phone, using a cell phone to take pictures is the leading use of cell phones with seventy-six percent of users reporting that they use their phones to capture pictures.[9] Smartphones have allowed users to freely share these pictures easily via e-mail, social networking sites, and texts. According to a Pew Internet and American Life Project study, seventy-two percent of adult cell phone users send or receive text messages to their phone.[10] In the past few years, attention has concentrated around the use of text messages, primarily by young cell phone users, to send and receive sexually explicit pictures in a practice known as "sexting."[11] The existence of cameras on cell phones has allowed users to take, and potentially share, intimate and personal photos with their device.

Aside from being a form of communication, many businesses are now utilizing text messaging to reach their customer base. In 2010, TXT180.com created a website that offers text message marketing services to businesses.[12] The use of texting has also expanded to provide for

---

[6] *See The App Store*, APPLE, http://www.apple.com/iphone/built-in-apps/app-store.html (last visited Mar. 30, 2012).
[7] Purcell, *supra* note 1.
[8] Sarah Perez, *Flurry: Mobile App Usage Up To 94 Minutes Per Day*, TECHCRUNCH (Jan. 9, 2012), http://techcrunch.com/2012/01/09/flurry-mobile-app-usage-up-to-94-minutes-per-day/.
[9] Purcell, *supra* note 1.
[10] *Id.*
[11] Deborah Feyerick & Sheila Steffen, *'Sexting' Lands Teen On Sex Offender List*, CNN (Apr. 7, 2009), http://articles.cnn.com/2009-04-07/justice/sexting.busts_1_phillip-alpert-offender-list-offender-registry?_s=PM:CRIME.
[12] Text180, *Text180: A New Direction for Marketing*, TXT180 (2012), http://www.txt180.com/.

public safety. Some universities have set up emergency notification systems that allow the university to send out important messages via texts.[13] Some smartphone users may be used to receiving such notifications from trusted sources. Aside from advertisers and universities, banks have also attempted to capitalize on the increased smartphone use by Americans.

Smartphone technology now allows users to conduct mobile banking. Banks such as Wells Fargo and Bank of America allow users to download apps via the mobile markets.[14] Javelin Strategy and Research, a research and strategy consulting firm, predicts that within the next five years, eighty-six million users will conduct their banking via their mobile phones.[15] Some banks, such as Bank of America, allow their customers to receive periodic updates about accounts via text messaging; additional services include the ability for customers to text the bank for updates as necessary.[16] Other banks, such as Chase, allow users to set up notifications when their balance has reached a certain amount.[17] Chase also offers its customers the ability to deposit a check by taking a picture of it.[18] Another popular feature gaining momentum is the use of a "virtual wallet."[19] Virtual wallets, such as Google Wallet, store credit cards right on your phone for convenience. [20] The use of such technology means that smart phone users often have financial information stored on their device.

---

[13] *See* University of Pittsburgh, *Emergency Preparedness*, PITT.EDU (Nov. 18, 2011), http://www.pitt.edu/prepare.html.
[14] *Mobile Banking FAQs*, WELLS FARGO, https://www.wellsfargo.com/help/faqs/mobile (last visited Mar. 30, 2012); *Text Banking Is a Quick and Easy Way to Track Your Finances*, BANK OF AMERICA, http://learn.bankofamerica.com/articles/money-management/the-importance-of-managing-your-account-balances.html (last visited Mar. 30, 2012).
[15] Martha C. White, *What the Big Banks Think of Mobile Banking*, DAILYFINANCE (Apr. 04, 2011), http://www.dailyfinance.com/2011/04/04/what-the-big-banks-think-of-mobile-banking/.
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Claire Cain Miller, *For Hackers, the Next Lock to Pick*, THE NEW YORK TIMES (Sept. 27, 2011), http://www.nytimes.com/2011/09/28/technology/companies-see-opportunity-in-stopping-cellphone-hackers.html?_r=2&pagewanted=all.

Global positioning systems (GPS) are often used by mobile phones to provide directions and turn-by-turn navigation. Additionally, the use of GPS has offered some useful services for families to track family members. Specifically, services such as uLocate enable a user to view the locations of all family members from the website or a mobile app.[21] The use of GPS devices on mobile phones has also helped law enforcement in solving crimes. In 2003, after killing two real estate agents in Georgia, Stacey Ian Humphreys attempted to evade police by driving to Wisconsin; the police tracked his movement via his cell phone communications until he was able to be apprehended.[22] Moreover, cell phone records and GPS coordinates can help police build evidence linked to ongoing investigations.[23] Such advancements in mobile technology have increased the personal and consumer data available on smartphone devices; as a result, breaches of privacy may negatively impact consumers.

II. Smartphone Vulnerabilities

The increased use of smartphones has brought about emerging privacy concerns relating to personal and consumer data protection. A smartphone user's privacy can be compromised in a variety of ways: the loss of a phone, infection by malware, and by applications that can modify or monitor information on phones. Apps may also collect unnecessary information and share collected information with third-party companies and apps. Many mobile users are unaware of the different ways in which their privacy can be breached and what steps they can take to protect their data.

---

[21] President and Fellows of Harvard College, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 316 (2004).
[22] *Id.* at 310.
[23] *See* Mitch Stacy, *In Criminal Cases, GPS Units Can Mark the Scene of a Crime*, USA TODAY (Aug. 28, 2008), http://www.usatoday.com/tech/news/techinnovations/2008-08-28-gps-evidence-crimes_N.htm.

The easiest way a mobile phone user could have his or her privacy compromised is by inadvertently losing the device. Losing a smartphone makes the user vulnerable to a breach of privacy as the finder of the cell phone may be able to access texts, emails, contacts, pictures, and saved passwords. Researchers at Symantec, a computer security firm, recently conducted a study on lost smartphones.[24] In order to conduct the study, Symantec researchers "lost" fifty smartphones in cities around the U.S. with tracking capabilities that allowed the firm to see not only where the phone travelled but what functions were clicked.[25] According to the results forty-three percent of finders clicked on an app labeled "online banking."[26] Overall, eighty-nine percent of respondents clicked on a function that contained personal information and only fifty percent sought to return the device even though the "owner's" name was readily identifiable.[27] This study indicates that cell phones that are lost are vulnerable to data breaches. It is important for consumers to be aware of the information his or her smartphone stores and take steps to protect that information.

Besides breaches that may occur due to the loss of a cell phone, there are other security risks which smartphone users face while possessing their device. Another threat faced by smartphone users can result from the simple breach of privacy due to hacking. There are several ways in which an unauthorized user may intercept and record the mobile phone user's conversation. Recently, in the summer of 2011, the "News of the World" tabloid shut down after allegations by law enforcement that the magazine had a history of hacking into the cell phones of

[24] Bob Sullivan, *EXCLUSIVE: The 'Lost' Cell Phone Project, and the Dark Things It Says About Us*, MSNBC (Mar. 8, 2012), http://digitallife.today.msnbc.msn.com/_news/2012/03/08/10595092-exclusive-the-lost-cell-phone-project-and-the-dark-things-it-says-about-us.
[25] *Id.*
[26] *Id.*
[27] *Id.*

high profile individuals.[28] "News of the World" was accused of hacking into the voicemails of high profile celebrities, criminals, and crime victims.[29] This was accomplished in the early 2000's through the use of ID-spoofing.[30] While many mobile carriers now require passwords to check voicemail, analysts say that many users are still vulnerable because of their use of simple passwords that are often ascertainable from other publically available information.[31]

The use of cameras has also caused privacy concerns for many mobile users. In 2011, Christopher Chaney, a Florida man, was charged with hacking into the emails of Christina Aguilera, Mila Kunis, and up to fifty other celebrities.[32] The case gained the attention of the Federal Bureau of Investigation (FBI) when nude pictures from Scarlett Johansson's smartphone were posted on the internet.[33] Though not confirmed, it is speculated that Chaney was able to hack into mobile phones by guessing the user's passwords. This type of breach raises the risk of "sextortion," which occurs when a person who has obtained sexually explicit photos of a user threatens to post the picture online unless he or she receives cash.[34] This prospect is concerning to some smartphone users, given the personal and intimate photos that may be stored on such devices.

The popular feature of text messaging has also been a source of privacy breaches for many mobile users. Phishing is a way for hackers to obtain personally identifiable information

---

[28] The Associated Press, *News of the World Shutting Down Amid Scandal*, BLOOMBERG BUSINESSWEEK (July 7, 2011), http://www.businessweek.com/ap/financialnews/D9OAV9OO0.htm.
[29] Damon Poeter, *How Did News of the World Hack Victims' Cell Phones?*, PC MAGAZINE (July 6, 2011), http://www.pcmag.com/article2/0,2817,2388157,00.asp.
[30] *Id.*
[31] *Id.*
[32] Greg Risling & Robert Jablon, *Florida Man Arrested in Celeb Hacking Probe*, MSNBC (2011), http://today.msnbc.msn.com/id/44876558/ns/today-entertainment/t/florida-man-arrested-celeb-hacking-probe/#.TywU_8X2Zm8.
[33] *Id.*
[34] Jason Barry, *Sextortion Targets Cell Phone Users*, KPHO (Nov. 11, 2011), http://www.kpho.com/story/16012948/sextortion-is-latest-crime-trageting-cell-phone-users.

about a user by masquerading as a trustworthy source, such as a bank, social networking site, or other trusted entity.[35] Phishing is primarily done through the use of e-mail. However, this practice has extended to mobile phones and is known as "smishing," a tactic that uses text messages to initiate a scam.[36] Another way in which a mobile user can be targeted is by "vishing" which uses automated phone calls to entice the user to input personal information.[37] Peter Cassidy, the secretary general of the Anti-Phishing Working Group, says that such smishing and vishing attacks have increased in the past several years and are usually targeted at customers of local banks.[38] This is a vulnerability to those bank customers who routinely receive text messages from their bank and may be victimized by these schemes. The FBI stated that the personal information routinely obtained in these schemes could provide a criminal with enough information to steal money or make purchases from a user's account.[39]

Recently, the United States Supreme Court ruled on the legality of warrantless GPS tracking by police.[40] However, GPS and other identifiable information can still be accessed and used illegally by a number of individuals, organizations, and companies. There are some dangers in the use of GPS technology and the feature is not always beneficial to mobile users. There have been incidents where victims of domestic abuse have been located by their abusive spouses through the use of mobile GPS technology.[41] This is an "unintended result" of regulations

[35] *How to Recognize Phishing Email Messages, Links, or Phone* Calls, MICROSOFT SAFETY & SECURITY CENTER (2012), http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx.
[36] Angela Moscaritolo, *FBI Warns of SMS and Phone Based Phishing Scams*, SC MAGAZINE (Nov. 24, 2010), http://www.scmagazine.com/fbi-warns-of-sms-and-phone-based-phishing-scams/article/191565/.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] Mike Sacks, *Warrantless GPS Tracking Unconstitutional, Supreme Court Rules*, THE HUFFINGTON POST (Jan. 23, 2012), http://www.huffingtonpost.com/2012/01/23/warrantless-gps-tracking-_n_1224000.html (ruling that the installation of a GPS on a car by police constituted a search and therefore required a warrant).
[41] Justin Scheck, *Stalkers Exploit Cellphone GPS*, THE WALL STREET JOURNAL (Aug. 3, 2010), http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html.

intended to help mobile users who dial for emergency assistance from their mobile phones.[42] By the end of 2005, the Federal Communications Commission (FCC) required that "all cellular providers…make at least 95% of the phones in their networks traceable by satellite or other technologies."[43] A study conducted by the Wall Street Journal in 2011 showed that even when location is disabled, the iPhone stores location data from its users.[44] The inability to turn the GPS functions off may make users vulnerable to others who seek to take advantage of their location.

Smartphone users can also suffer privacy and information breaches due to the installation of viruses and worms that allow information to be read and sent to other devices. In August 2011, a Trojan was discovered that provided access to photos whenever a photo was taken.[45] This Trojan was also able to steal other information such as text messages, e-mails, and contacts.[46] Users whose personal information or pictures are intercepted by such malware may be subject to blackmail and "sextortion" schemes. Additionally, the rise of cell phone usage has made smartphones a lucrative target for hackers to steal and use financial or personally identifiable information.

By mid-2008, there existed an estimated 500 malicious apps that were targeted specifically to mobile devices.[47] Lookout, a mobile security startup company, says that up to a million people were afflicted by mobile malware in the first half of 2011. [48] According to

[42] *Id.*
[43] *Id.*
[44] Jennifer Valentino-DeVries, *iPhone Stored Location in Test Even if Disabled*, THE WALL STREET JOURNAL (Apr. 25, 2011), http://online.wsj.com/article/SB10001424052748704123204576283580249161342.html.
[45] *Mobile Malware to Steal Photos From Your Phone*, CNET (Aug. 16, 2011), http://forums.cnet.com/7726-7813_102-5187509.html.
[46] *Id.*
[47] Kimberly L. Rhodes, *Walking the Wire in the Wireless Word: Legal and Policy Implications of Mobile Computing*, 16 J. TECH. L. & POL'Y 25, 32 (2011).
[48] Cain Miller, *supra* note 20.

Lookout, the threat for Android users is two and a half times higher than it was just six months ago.[49] Recently, malicious apps have largely targeted the Android operating system.[50] The reason why the Android operating system is more vulnerable to attack by malware is that it is more of an "open development platform" than the iPhone operating system.[51] As a result, third parties are able to freely create apps whereas a closed platform is more controlled by the service provider.[52] However, other devices, such as iPhones are also vulnerable; in November 2011, a researcher discovered a bug in Apple's operating system which would allow hackers to take control of iPhone apps and use them to steal photos, contacts, and send messages.[53]

Besides the concern that apps are vulnerable to infection by viruses and worms, some users are concerned about the types and amount of data that apps can store. Some apps can modify SD cards, track GPS locations, and record audio. For instance, the Facebook Android app gives the company permission to access a user's texts.[54] Despite this intrusion into personal data, the Facebook app has been downloaded more than 100 million times.[55] Besides being able to monitor data and modify settings on a user's phone, the collection of data raises privacy issues since some apps send collected information to unauthorized third parties.

---

[49] *Id.*
[50] Robert Siciliano, *Beware of Malicious Mobile Apps*, MCAFEE (Jan. 6, 2012), http://blogs.mcafee.com/consumer/beware-of-malicious-mobile-apps.
[51] Wayne Jansen & Karen Scarfone, *Guidelines on Cell Phone and PDA Security: Recommendations of the National Institute of Standards and Technology*, UNITED STATES DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 1, 3-9 (Oct. 2008), http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf.
[52] *Id.*
[53] John D. Sutter, *Researcher: iPhone Bug Could Let Hackers Steal Photos, Contacts and Send Texts*, CNN (Nov. 08, 2011), http://articles.cnn.com/2011-11-08/tech/tech_mobile_apple-ios-bug-apps_1_apple-s-app-store-apple-app-store-ios?_s=PM:TECH.
[54] Jennifer Baker, *Mobile Network Operators Set Guidelines for App Privacy*, PC WORLD (Feb. 27, 2012), http://www.pcworld.com/printable/article/id,250773/printable.html.
[55] *Id.*

The Wall Street Journal conducted a study of the 101 most popular smart phone apps on both the iPhone and Android operating systems.[56] The Journal's results show that fifty-six apps sent the phone's "unique device ID" to other companies without the user's authorization.[57] Furthermore, forty-seven apps sent out information about the phone's location.[58] According to the results, forty-five of the apps did not have privacy policies.[59] Though privacy policies would not limit the apps' ability to collect data, it would inform the users of how data is collected and used. Additionally, the Journal stated "neither Apple nor Google requires app privacy policies."[60] Given the sensitive nature of the data that some smartphone users create and store on their phones, a lack of a privacy policy may result in vulnerabilities that they were unaware of.

The use of apps by smartphone users has led to consumer data transfers between companies and app software providers. Many apps share the consumer data it collects about users with other apps because data sharing is financially profitable. Arguments have been made that consumer data is worth more to the company if data is sold to third parties as opposed to merely collecting and retaining the information.[61] Many of these transfers occur because of the low cost of apps. For instance, many apps are available for free or at a low cost to consumers. This provides "an incentive to share user data with mobile-ad networks and other companies involved in ads or marketing."[62]

III. Privacy Law and Solutions to Smartphone Vulnerabilities

[56] Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, THE WALL STREET JOURNAL (Dec. 17, 2010), http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] DAVID H. HOLTZMAN, PRIVACY LOST: HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY 115 (2006).
[62] Shayndi Raice & Yukari Iwatani Kane, *Industry Weighs Policing of Mobile Apps*, THE WALL STREET JOURNAL (May 24, 2011), http://online.wsj.com/article/SB10001424052748704681904576315432274229752.html.

There are several ways that a person can protect themselves from a breach of privacy. The most highly advised step is to place a password protected screen lock on the phone.[63] It is imperative that a password is not easily discernible from other publicly available information, such as birthdates and names available on social networking websites.[64] These steps would protect a user in the event that he or she should lose the device. However, other steps can be taken to ensure that users who possess their devices are not victims of malware or hacking. A user should avoid storing personal and intimate pictures of his or herself on the device. To protect from smishing attacks, a user may want to open texts only from recognized numbers and contact institutions when he or she receives a suspicious text. In order to protect against GPS privacy breaches, an individual in a questionable situation should either turn off his or her cell phone or, if possible, get a new device.

There are several ways that individuals can protect themselves from vulnerabilities associated with malware and apps. One of these ways is to install antivirus software onto the device. Antivirus companies have started to focus on protecting smartphone data. McAfee recently introduced a package that would protect a user's smartphones, tablets, and computers.[65] The company also sells antivirus software targeted specifically for mobile phones to prevent "viruses, worms and spyware, Trojan horses, and battery-sapping malware."[66] Moreover, individuals should be extra cautious and aware of what functions the app has permission to perform upon installation.

---

[63] Zachary Kussin, *Just How Easy Is Phone Hacking?*, PBS (July 14, 2011), http://www.pbs.org/wnet/need-to-know/culture/just-how-easy-is-phone-hacking/10407/.
[64] *Id.*
[65] *McAfee Mobile Security*, MCAFEE (2012), http://home.mcafee.com/store/mobile-security?culture=en-us&cid=100453.
[66] *VirusScan Mobile*, MCAFEE (2012), http://www.mcafee.com/us/products/virusscan-mobile.aspx.

Individual data is not the only type of data that is vulnerable to data breaches. Many businesses use smartphones for employees and are vulnerable to data breaches as well. Some of this data can be critical to the company and may include budgets, plans, and client lists. The use of smartphone technology facilitates business; however, it is important for a business to protect its smartphones, and therefore its data, from unwarranted data breaches. Some protective measures that companies may choose to implement include the reduction of sensitive data, data backup, and encryption.[67]

Parties who are violated as a result of hacking incidents or malware can seek legal redress through the civil and criminal court system. An individual who violates another's personal data may face criminal charges for invasion of privacy, wiretapping, cyber-stalking, identity theft, and blackmail. While there is redress for an individual whose smartphone device has been the subject of a private attack, there is little availability of redress when the breach is caused as a result of information sharing by companies and apps.

The rapid growth of technology has eroded existing information privacy laws and leaves many consumers' information vulnerable to breach. One of the main threats comes from the ability of apps and companies to collect, store, and share data with third party companies. It is important for many companies to gather data about the consumer, indeed some companies would be unable to provide their services without doing so, but it is imperative that these consumers be informed of what data is being collected and how that data will be used.

The growing popularity of apps has led to many legislative attempts to protect digital consumer data. In 2011, three legislative proposals were introduced that would create a way to

[67] Jansen & Scarfone, *supra* note 51, at ES3.

allow users to turn off tracking on smartphones.[68] Digital consumer data is an issue because there is no uniform requirement for companies (and app providers) to have a privacy policy. The lack of consumer privacy laws has allowed private industry organizations and companies to implement their own standards with regard to consumer data. This has permitted some companies' apps to function on smartphone devices without the need for privacy policies to protect and limit how information is gathered, stored, and shared. A proposed solution is for smartphone operating systems to require apps to provide privacy statements and provide better policing of apps offered to users.

At a Senate Judiciary subcommittee meeting on privacy, technology and the law, Senator Al Franken urged Apple and Google, the providers of the iPhone and Android system, to require apps to display privacy policies.[69] Google's director of public policy, Alan Davidson, stated that Google would consider adopting Senator Franken's proposal.[70] Policing of apps would be most useful to the Android system which does not require as stringent of standards as the iPhone system before placing an app into the market.[71] Guy Tribble, Apple's vice president of software technology, stated during the meeting that Apple requires potential apps to have privacy policies; however, the company representative admitted that it has never "removed an app from its store for violating the agreement."[72] Apple's example shows that companies can choose whether to enforce consumer protection policies since there is no uniform federal standard.

Recently, California Attorney General, Kamala Harris, reached an agreement with six major mobile-device companies which agreed to provide privacy laws on apps to individuals

[68] Julia Angwin, *Apple, Google Take Heat*, THE WALL STREET JOURNAL (May 10, 2011), http://online.wsj.com/article/SB10001424052748703730804576315121174761088.html.
[69] *Id.*
[70] *Id.*
[71] *See id.*
[72] *Id.*

within the state of California.[73] These companies included: Apple, Inc., Google, Inc., Amazon.com, Inc., Hewlett-Packard Co., and Research in Motion Ltd.[74] The companies agreed to this requirement by acknowledging that California state law requires that apps have privacy policies.[75] This agreement is great for consumers within California, but the lack of a federal mandate for privacy policies leaves consumers in other states vulnerable to privacy data collection from apps without their knowledge.

Following the example of California, federal legislation should be introduced that requires privacy policies on apps that collect any personally identifiable data. Doing so would protect sensitive data in addition to providing more transparency to the apps available on the different smartphone operating systems. Mandating full disclosure privacy policies may also increase the credibility of apps available for download. However, the requirement of privacy policies alone may not be enough to protect consumers from data vulnerability.

Privacy policies are often written by lawyers and, as a result, are often hard for the average user to comprehend. [76] This leaves many consumers unaware as to the full extent their data is being collected or shared with other companies. One possible way to combat this is to implement legislation that echoes the Credit Card Accountability, Responsibility, and Disclosure Act of 2009 (Credit Card Accountability Act). The Credit Card Accountability Act was passed into law in order to protect credit card customers from unfair industry practices.[77] One of the main requirements to the Credit Card Accountability Act was to make credit card policies and

[73] Geoffrey A. Fowler, *Tech Giants Agree to Deal on Privacy Policies for Apps*, THE WALL STREET JOURNAL (Feb. 23, 2012), http://online.wsj.com/article/SB10001424052970203918304577239650306276074.html.
[74] *Id.*
[75] *Id.*
[76] HOLTZMAN, *supra* note 61, at 115.
[77] Press Release, Office of the Press Secretary, *Fact Sheet: Reforms to Protect American Credit Card Holders*, THE WHITE HOUSE (May 22, 2009), http://www.whitehouse.gov/the_press_office/Fact-Sheet-Reforms-to-Protect-American-Credit-Card-Holders.

monthly statements easier for consumers to read and comprehend.[78] Implementing standards that privacy policies have to be clear and concise for consumers would provide full disclosure and allow consumers to make informed decisions about what apps to download. Recently, Google implemented a new privacy policy which was meant to streamline data sharing between multiple Google websites as well as make the privacy policy easier for consumers to understand.[79] This new policy was challenged by thirty-six state attorney generals as being too intrusive of consumer privacy.[80] However, American officials were not alone in opposing these changes.

Google's new privacy policy was opposed by French regulators who argued that the new policy was in violation of the European Directive on Data Protection.[81] The European Directive on Data Protection provides consumer data protection to European citizens by setting guidelines for the collection of data. Among some of the requirements is the limitation on what type of data can be collected, how that data can be organized, and the requirement that the consumer be "unambiguously informed."[82] Another requirement of the Act is that the consumer has the right to access and make necessary corrections to the data collected by companies.[83] In the U.S., legislation regarding the collection of identifiable information is largely concentrated on the ability of the government to collect data. For example, the Patriot Act limits the quality of data that the government can collect about individual citizens.[84] However, there is no legislation

[78] *Id.*
[79] Fowler, *supra* note 73.
[80] *Id.*
[81] Jennifer Valentino-DeVries, *Google Privacy Policy Could Violate EU Law, France Says*, THE WALL STREET JOURNAL (Feb. 28, 2012), http://blogs.wsj.com/digits/2012/02/28/google-privacy-policy-could-violate-eu-law-france-says/.
[82] *Protection of Personal Data*, EUROPA (Jan. 2, 2011), http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm.
[83] *Id.*
[84] HOLTZMAN, *supra* note 61, at 113.

targeted solely for the protection of consumer data within the private industry. There are privacy laws that protect other data, such as children's information online through the Children's Online Privacy Protection Act (COPPA) of 1998, and health care information through the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[85]

The requirement of privacy policies would inform consumers and would provide them with a private right of action if their information was ever inappropriately shared. A number of websites have been sued for selling consumer and personal data to third parties in violation of their established privacy policies.[86] For example, a bankrupt toy store was sued in July 2000 in an effort to prevent the company from violating its privacy policing by selling its customer data to a third party.[87] Other companies that have been sued for violations of internally established privacy policies include: Procter & Gamble, Pfizer, and JetBlue Airways.[88] While consumers are able to bring suit against companies for violations of its privacy policy, the ability of a consumer to do so when no privacy policy exists in the first place is questionable.

Some legislation has been proposed that goes beyond the mere requirement of privacy policies. A possible solution to privacy breaches was offered in April 2011, when Senators John Kerry and John McCain proposed legislation called the Commercial Privacy Bill of Rights Act of 2011.[89] The new legislation would create new rules for companies that gather personal data.[90] In the announcement of the proposed legislation, Senator McCain specifically mentioned the Wall Street Journal report which discovered that fifty-six of the 101 most popular apps shared

[85] *Existing Federal Privacy Laws*, CENTER FOR DEMOCRACY & TECHNOLOGY (2012), https://www.cdt.org/privacy/guide/protect/laws.php#ecpa.
[86] See HOLTZMAN, *supra* note 61, at 116.
[87] *Id.*; See also, F.T.C. v. Toysmart,com, 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000).
[88] HOLTZMAN, *supra* note 61, at 116.
[89] Julia Angwin, *Senators Offer Privacy Bill to Protect Personal Data*, THE WALL STREET JOURNAL (Apr. 13, 2011), http://online.wsj.com/article/SB10001424052748703385404576258942268540486.html.
[90] *Id.*

information with third parties.[91] The proposed bill was supported by big technology companies such as Hewlett-Packard Co., Microsoft Corp., and Intel Corp.[92]

In detail, the proposed legislation by McCain and Kerry establishes guidelines for the "protection of personal data under the aegis of the Federal Trade Commission."[93] The bill was introduced to provide protection to consumers' personal data which does not currently exist under federal laws.[94] The proposal has a lot of cross over with the European Directive on Data Protection. For example, it requires covered entities to impose security measures to protect consumer information.[95] Additionally, the legislation requires that companies inform consumers about how data is collected, used, and stored in clear and precise terms.[96] This requirement will facilitate understanding and aide consumers in determining whether to conduct business with a certain company. Similar to European legislation, the data collected by these firms will be available to the consumer so that corrections can be made.[97] The legislation permits companies to collect data but the covered entities will only be able to collect as much data as necessary to fulfill its services.[98] Perhaps the most noted requirement of the bill is the "opt-out" option, which would allow consumers and users to opt-out of any information collection.[99] Senators are not the only government officials who seek change to consumer privacy.

---

[91] *Id.*
[92] *Id.*
[93] Commercial Privacy Bill of Rights Act of 2011, S.799, 112th Cong. (2011).
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] Chanley Howell, Daniel Muto & Andy Serwin, *Kerry-McCain Introduce Commercial Privacy Bill of Rights Act of 2011 to Senate*, FOLEY & LARNDER LLP (Apr. 13, 2011), http://www.privacysecuritysource.com/2011/04/13/kerry-mccain-introduce-commercial-privacy-bill-of-rights-act-of-2011-to-senate/.

The White House and the U.S. Department of Commerce support efforts to protect consumers' information.[100] The White House has stated that it "wants Congress to enact privacy legislation but is going to move forward with businesses and regulators to get the ball rolling even without congressional action."[101] Establishing universal guidelines for consumer protection is not an easy task due to the varying interests involved. For instance, there is disagreement among government officials and private industry groups as to proposals for "do not track" provisions, such as the "opt-out" option in the Commercial Privacy Bill of Rights Act of 2011.[102] This disagreement centers on the definition of what "do not track" should mean and also on finding an adequate balance between the interest of companies to collect data and the protection of consumer information.[103]

IV. Conclusion

Advancements in mobile technology have enabled individuals to communicate and transfer information faster than ever before. The various ways in which consumers use their smartphones creates data that can be susceptible to privacy breaches. These privacy breaches can occur due to hacking by other individuals, through malware embedment, or through the collection and transfer of personally identifiable and consumer information to third parties. Although consumers may be able to protect themselves through self-implemented steps and criminal laws which prosecute hackers and intruders, more needs to be done to protect consumers from data collection. As stated, other countries have taken steps to secure consumer information privacy for their citizens. There are multiple ways that American consumer privacy could be protected. First, making clear and concise privacy policies mandatory for companies

[100] Jennifer Valentino-DeVries, *White House Proposes Web Privacy Legislation*, THE WALL STREET JOURNAL (Feb. 24, 2012), http://online.wsj.com/article/SB10001424052970203918304577241502216430274.html.
[101] *Id.*
[102] *Id.*
[103] *Id.*

that provide apps would fully inform the consumer of exactly what the app is capable of doing. This would allow a consumer to make an informed decision as to whether he or she wants to give the app access to personally identifiable information and consumer data. In addition to this, legislative officials should strive to pass legislation that echoes the European Directive on Data Protection. Such legislation should allow a company to collect necessary data without intruding into data that is unnecessary to fulfill their company's mission. While American smartphone users enjoy the advancements of mobile technology, this enjoyment should not come at the expense of potential privacy breaches.