TOURO LAW
Touro College Jacob D. Fuchsberg Law Center

Touro Law Review

Volume 31 | Number 4 Article 17

August 2015

Data Privacy Regulation in the Age of Smartphones

Matthew Hettrich

DATA PRIVACY REGULATION IN THE AGE OF SMARTPHONES

*Matthew Hettrich**

I. INTRODUCTION

The need for privacy has always been an important principle in the United States legal system. Technology has evolved exponentially over the last decade, and with it, our need to protect private information. Devices that we carry with us on a daily basis contain information that is vital to our lives, and perhaps nothing contains quite as much information as a person's cellular phone. Think for a moment about the amount of data that is likely stored on your cellular phone and the repercussions of having some (or all) of that data compromised, either by an unauthorized company's application or by some other outside force, such as a hacker. Clearly, the thought of something of that nature happening is one that a person would not like to imagine or experience.

A cellular phone is a "[s]mall wireless device that has at least the same functions of a standard wired telephone but is smaller and more mobile. A cell phone requires a subscription to a service provider and either a prepaid or monthly billing setup."[1] Two primary types of cellular phones are used by the consuming public. The first is referred as a conventional cellular phone, which is designed for basic use such as making phone calls and sending text messages.[2]

* J.D. Candidate 2016, Touro College Jacob D. Fuchsberg Law Center; B.A. 2009 in Political Science, Stony Brook University. I would like to give special thanks to Professor Rena C. Seplowitz for her guidance and insight on my Comment. I would also like to thank the *Touro Law Review* staff, especially Alyssa Wanser, for her constructive criticism and assistance in shaping my Comment.

[1] *Cell Phone*, BUSINESSDICTIONARY.COM, http://www.businessdictionary.com/definition/cell-phone.html (last visited May 10, 2015).

[2] *Cell Phone & Service Buying Guide*, CONSUMER REPORTS, http://www.consumerreports.org/cro/cell-phones-services/buying-guide.htm (last visited Feb. 24, 2015).

The second, and increasingly popular, version is a smartphone. A smartphone adds more storage space, larger displays, and generally can perform the same functions as a desktop computer or laptop.[3]

According to the Pew Research Center, as of 2013, ninety-one percent of American adults now own a cell phone.[4] Further, approximately "[fifty-six percent] of American adults" use smartphones.[5] This second statistic is particularly interesting due to the sheer amount of data that this represents. Smartphones contain "sensitive information like addresses and phone numbers, passwords, account numbers, email, voicemail, and text message logs."[6] This does not begin to tell the whole story. Smartphone users are also able to install third party applications ("apps") that grant the ability to perform actions similar to those performed on a computer.[7] These apps range in functionality and provide services such as games, news, and email. Other apps allow easy access to popular social networking services such as Facebook, Twitter, and Instagram.

While a majority of these apps may seem harmless, many collect large amounts of data from users, and in some instances, do so without the user's knowledge.[8] This information may include "email contacts, call logs, internet data, calendar data, data about the device's location, the device's unique IDs, and information about how [the user uses] the app itself."[9] This information, collected by app developers, is often shared with other companies, which may use the data for their own purposes.[10] For example, one popular application, *Angry Birds*, has been guilty of such practices.[11] The application, which has been downloaded over a billion times, stores users' loca-

---

[3] *Id.*

[4] Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, PEW RESEARCH CTR. (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

[5] *Id.*

[6] *Disposing of Your Mobile Device*, FTC, http://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device (last visited Feb. 24, 2015).

[7] Cory Janssen, *Mobile Application (Mobile App)*, TECHOPEDIA, http://www.techopedia.com/definition/2953/mobile-application-mobile-app (last visited Feb. 24, 2015).

[8] *Understanding Mobile Apps: Questions & Answers*, ONGUARD ONLINE, http://www.onguardonline.gov/articles/pdf-0004-mobile-apps.pdf (last visited Feb. 24, 2015).

[9] *Id.*

[10] *Id.*

[11] Kevin J. O'Brien, *Data-Gathering via Apps Presents a Gray Legal Area*, N.Y. TIMES (Oct. 28, 2012), http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html?_r=0.

tion data so that they can be targeted with different advertisements at a later date.[12] According to the *New York Times*, in a survey of forty users, all but two were unaware that the application was storing this data.[13] Situations such as this pose a major privacy issue and represent only one among many different privacy problems facing lawmakers today.

The law as it currently stands in the field of data privacy is largely outdated and lacking in substance. Many of the laws that govern in this area were enacted at a time before the popularity of computers and the existence of smartphones, and thus, have required reinterpretation to apply to more technologically complex situations. Privacy has always been important to Americans, and although not expressly stated, a broad "right of privacy has been inferred in the Constitution."[14] This right has developed alongside a handful of statutes designed to protect the public's privacy.[15] The Federal Trade Commission (the "FTC" or "the Commission") is primarily in charge of enforcing the statutory right of privacy, and while there are not currently any laws or regulations specifically designed to regulate the right of privacy when it comes to mobile data, several laws dealing with privacy in general overlap with this area.[16] These include the Children's Online Privacy Protection Act (the "COPPA"),[17] the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the "CAN-SPAM Act"),[18] the Fair Credit Reporting Act (the "FCRA"),[19] and the Computer Fraud and Abuse Act (the "CFAA").[20]

This Comment examines the rules and regulations which relate to mobile data privacy, and argues that a single comprehensive statute should be enacted by Congress to combat the inadequate protection currently afforded to consumers. Specifically, this Comment focuses on smartphones, as they contain the highest amount of stored data. Section II begins with an overview and analysis of the current state of mobile data privacy law. Next, Section III investigates con-

---

[12] *Id.*

[13] *Id.*

[14] *Privacy: Right of Privacy, An Overview*, CORNELL UNIV., http://www.law.cornell.edu/wex/privacy (last visited May 8, 2015).

[15] *Id.*

[16] *Id.*

[17] 15 U.S.C. §§ 6501-6505 (2006).

[18] 15 U.S.C. §§ 7701-7713 (2006); 18 U.S.C. § 1037 (2006).

[19] 15 U.S.C. § 1681 (2006).

[20] 18 U.S.C. § 1030 (2006).

troversies in the area of mobile data privacy and efforts to resolve the issues presented. Section IV examines possible solutions, and explores the attempts being made to promote change. Finally, Section V proposes recommendations.

II. MOBILE DATA PRIVACY AS IT STANDS TODAY

The law surrounding mobile data privacy is small compared to other areas in our legal system. In fact, no statutes specifically apply to this field of law. As a result, the current legal landscape consists of a patchwork system of regulations and best practices that have been established through laws governing a general right of privacy and guidelines made by organizations like the FTC.[21] These guidelines are directed primarily to companies which collect data from consumers, and outline ways in which these companies can conduct their businesses to comply with privacy statutes.[22] The FTC also seeks to educate consumers, advising them on how best to secure their personal data on their mobile devices.[23] These suggestions, while helpful, fall far short of becoming a concrete solution in the battle to keep consumer data private.

A. The Role of the Federal Trade Commission

The FTC is an independent agency in the United States, charged with protecting consumers against unfair commercial practices.[24] The Federal Trade Commission Act established the FTC, largely in response to questions about trusts and antitrust issues which existed at the time.[25] The FTC was designed to help prevent

---

[21] *Data Protection in United States: Overview*, PRACTICAL LAW, http://us.practicallaw.com/6-502-0467 (last visited Feb. 20, 2015).

[22] *FTC Issues Final Commission Report on Protecting Consumer Privacy*, FTC (Mar. 26, 2012), http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

[23] FTC, 2014 PRIVACY AND DATA SECURITY UPDATE 15 (2014), *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

[24] *Id.* at 1.

[25] FTC, FEDERAL TRADE COMMISSION 90TH ANNIVERSARY SYMPOSIUM 3 (2004), *available at* http://www.ftc.gov/sites/default/files/attachments/ftc-90-symposium/90thanniv_program.pdf [hereinafter 90TH ANNIVERSARY SYMPOSIUM]. These concerns arose from *Standard Oil Co. v. United States*, a United States Supreme Court decision in which the Court ruled that the Standard Oil Company constituted a monopoly of the petroleum industry. 221 U.S. 1, 79-80 (1911). The creation of the FTC was in response to the fear of other companies form-

"unfair or deceptive practices" in business, but the FTC's role has greatly expanded to reach the level of responsibility that it carries today.[26] The Commission now has the authority to enforce "a variety of sector specific laws,"[27] including the COPPA, the CAN-SPAM Act, and the FCRA.[28] The Commission has several tools at its disposal to carry out this task. These include the implementation of privacy programs, assessments by experts in the privacy industry, and monetary redress to users whose information has been compromised by offending companies; it can also seek civil monetary penalties from companies for violations of privacy statutes.[29] While much of the FTC's work involves the online environment consisting of computers and mobile devices, bringing actions against many prominent companies such as Google, Microsoft, Facebook, and Twitter, the Commission also has a significant presence in the offline world.[30] For example, the Commission gives consumers suggestions about the storage of important documents, such as social security cards, banking statements, and health plan information.[31]

Another important tool that the FTC utilizes is public educa-

---

ing monopolies, and it was designed to help fight against "unfair methods of competition." 90TH ANNIVERSARY SYMPOSIUM, at 6.

[26] PRIVACY AND DATA SECURITY UPDATE, *supra* note 23, at 1.

[27] *Id.*; *see also* 15 U.S.C. § 45 (2014):

> The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C. 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C. 227 (b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

Id.

[28] PRIVACY AND DATA SECURITY UPDATE, *supra* note 23, at 1.

[29] *Id.*

[30] *Id.*; *see also Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises*, FTC (Nov. 29, 2011), http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep; *FTC Gives Final Approval to Settlement with Google over Buzz Rollout*, FTC (Oct. 24, 2011), http://www.ftc.gov/news-events/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout.

[31] *How to Keep Your Personal Information Secure*, FTC, http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure#offline (last visited Nov. 30, 2014).

tion. While it is not required to do so, the FTC views educating the public as an essential part of its purpose in regulating data privacy.[32] To raise awareness of privacy issues, the Commission issues reports about privacy studies, hosts public workshops educating the public about privacy issues, and develops materials to be distributed to consumers and businesses.[33] These materials cover a variety of topics, such as identity theft, mobile privacy, and computer security.[34] While the FTC's primary goal is to protect consumers in the United States, much of its work also has positive impacts for internationally based consumers.[35]

B. Current Privacy Regulations

As previously mentioned, several privacy regulations currently in place help to protect mobile data privacy. Most of these were developed at a time before lawmakers were aware of the importance of smartphones and mobile devices in general in the daily lives of consumers. Consequently, they have been re-interpreted by the FTC and the courts to apply to the mobile world.

1. The Children's Online Privacy Protection Act

In the early 1990s, concerns arose regarding websites that appealed to children through the use of cartoon characters, which could lead them to submit personal information without parental knowledge.[36] In 1998, in response to this threat, Congress enacted the Children's Online Privacy Protection Act "to put parents in the driver's seat" in controlling what information websites could collect about their children.[37] Specifically, the COPPA imposes require-

---

[32] PRIVACY AND DATA SECURITY UPDATE, *supra* note 23, at 15.

[33] *Id.*

[34] *Id.*

[35] *Id.* at 16 (stating that this cooperation is largely accomplished through informal consultations and memoranda exchanged with international counterparts; for example, the FTC has an agreement with the United Kingdom "to engage in mutual assistance and the exchange of information in connection with the enforcement of applicable privacy laws").

[36] Courtney Banks, *Understanding the Children's Online Privacy Protection Act*, WALL ST. J. BLOG (Sept. 17, 2010, 7:49 PM), http://blogs.wsj.com/digits/2010/09/17/understanding-the-childrens-online-privacy-protection-act/.

[37] *Children's Online Privacy Protection Rule: Not Just for Kids' Sites*, FTC, http://www.business.ftc.gov/documents/alt046-childrens-online-privacy-protection-rule-not-just-kids-sites (last visited Nov. 30, 2014).

ments concerning the disclosure of personal information collected by websites and online services targeted towards children aged 13 and under.[38] Personal information can be interpreted to mean many different things, and the COPPA gives the FTC a broad scope to operate, listing some examples as first and last name, physical address, and telephone number.[39] The statute was amended in 2013 to expand the definition of personal information to include geolocation data, photographs, video, and audio files.[40] This change is particularly important because this information is among the most common to be found on a consumer's smartphone and it allows the FTC a broader reach in bringing actions against offenders.[41] Further, the COPPA applies to mobile apps as well, since they fall under the statute's category of online services.[42] This has serious implications for application developers, as they are now compelled to ensure that their apps comply with the updated COPPA rule.[43] To ensure that this is done,

---

[38] 15 U.S.C. §§ 6501-6505.

[39] 15 U.S.C. § 6501. The term "personal information" means individually identifiable information about an individual collected online, including:

> (A) a first and last name;
>
> (B) a home or other physical address including street name and name of a city or town;
>
> (C) an e-mail address;
>
> (D) a telephone number;
>
> (E) a Social Security number;
>
> (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
>
> (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier in this paragraph.

Id.

[40] *Complying with COPPA: Frequently Asked Questions*, FTC, http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions (last visited Nov. 30, 2014).

[41] Hunton & Williams LLP, *Amended COPPA Rule Comes into Effect*, HUNTON PRIVACY BLOG (July 1, 2013), https://www.huntonprivacyblog.com/2013/07/articles/amended-coppa-rule-comes-into-effect/; *see also* Julia M. Siripurapu, *The COPPA Enforcement Actions Are Here! – Children's Online Privacy Protection Act*, NAT'L L. REV. (Sept. 17, 2014), http://www.natlawreview.com/article/coppa-enforcement-actions-are-here-children-s-online-privacy-protection-act (writing that since the amendment has come into effect, the FTC has implemented more "vigorous enforcement" of the COPPA).

[42] *Complying with COPPA*, *supra* note 40.

[43] Liisa M. Thomas & Stephen E. Wieker, *FTC Warns Mobile App Industry about Potential for COPPA Rule Violations*, LEXOLOGY (June 3, 2013), http://www.lexology.com/library/detail.aspx?g=7948cfd8-4668-4f34-a49b-9ebafde95ca2.

the FTC sent letters to companies that created apps which may have violated the amended version of the COPPA.[44]

Websites and apps covered under the COPPA must follow a set of regulations that are outlined within the Act.[45] These regulations include displaying an online policy describing the practices for gathering information from consumers, as well as providing "direct notice to parents" before collecting any personal information from a child.[46] Further, the regulations state that personal information gathered online from a child should be kept for "only as long as is necessary to fulfill the purpose for which it was collected" and then the information should be deleted "using reasonable measures to protect against its unauthorized access or use."[47]

The COPPA is certainly a step in the right direction for privacy protection. It serves an important purpose to protect children who may not think twice before they submit personal information about themselves or their families. The amended version of the COPPA provides the FTC with greater flexibility in bringing action against those who may be targeting these vulnerable individuals, and Section III examines relevant cases in further detail. However, children are not the only individuals who warrant this kind of protection. People of all ages deserve the type of protection that the COPPA provides to children under age 13, and in many cases, the information that an adult provides to these companies may be more valuable than that of a child. More comprehensive legislation should be passed to make possible a greater degree of protection for all people.

2. The CAN-SPAM Act

In 2003, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act in an attempt to regulate spam email.[48] Specifically, Congress passed the CAN-SPAM Act "to address the rapid growth" of unsolicited commercial email.[49]

---

[44] *Id.*

[45] *Complying with COPPA*, *supra* note 40. The COPPA sets forth the requirements websites and apps must follow, and the FTC is responsible for enforcement. *Id.*

[46] *Id.*

[47] *Id.*

[48] *What Is the CAN-SPAM Act?*, CORNELL UNIV., http://www.law.cornell.edu/wex/inbox/what_is_can-spam (last visited May 10, 2015).

[49] *FCC Encyclopedia: Unwanted Commercial Electronic Mail*, FCC, http://www.fcc.gov/encyclopedia/can-spam (last visited May 10, 2015).

The CAN-SPAM Act works to protect consumers from "deceptive commercial email and requires companies to have opt out mechanisms in place."[50] The statute applies to "deceptive or misleading information and subject headings," and "requires identifying information such as a return address in email messages."[51] Smartphones have the ability to receive email messages and, as such, these devices fall under the protection of the CAN-SPAM Act. This is not to say that the Act regulates only email. The Act states that the FTC should develop rules with the goal of protecting consumers from "unwanted mobile service commercial messages."[52] In other words, the FTC also has the power to issue rules to prevent the transmission of unauthorized text messages to consumers' wireless devices.

In 2008, the FTC issued new regulations to implement the CAN-SPAM Act.[53] These new regulations arose from the FTC's request for comments on particular sections of the Act and clarification for some of the statute's overly broad wording.[54] Among these new provisions were a definition of the word "person" and the prohibition of "the imposition of any fee or requirement to provide personal information or any other obligation as a condition for processing a recipient's opt-out request."[55] Defining "person" was necessary because of the frequent use of the word in the text of the act despite the absence of a definition until this point.[56] In addition, judicial interpretation has expanded the CAN-SPAM Act beyond the realm of traditional email messages. In 2011, the United States District Court for the Northern District of California held that commercial messages on

---

[50] 15 U.S.C. §§ 7701-7713 (2006); 18 U.S.C. § 1037 (2006); *see also* PRIVACY AND DATA SECURITY UPDATE, *supra* note 23, at 12. Opt-out mechanisms allow consumers to remove themselves from mailing lists, effectively limiting the amount of unwanted information they receive through email. *What Does "Opt-Out" Mean?*, LISTBOX, https://www.listbox.com/helpspot/index.php?pg=kb.page&id=186 (last visited Feb. 20, 2015).

[51] *What Is the CAN-SPAM Act?*, *supra* note 48.

[52] *FCC Encyclopedia*, *supra* note 49. Commercial messages refer to those containing commercial content that advertise or promote "a commercial product or service," or are transactional in nature. *CAN-SPAM Act: A Compliance Guide for Business*, FTC, http://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business (last visited May 10, 2015).

[53] *Federal Trade Commission Issues New CAN-SPAM Act Regulations*, MORRISON FOERSTER (May 19, 2008), http://www.mofo.com/resources/publications/2008/05/federal-trade-commission-issues-new-can_spam-act__.

[54] *Id.*

[55] *Id.* (defining "person" as "an individual, group, unincorporated association, limited or general partnership, corporation, or other business entity").

[56] *Id.*

users' Facebook walls, news feeds, and message inboxes fell within the scope of the CAN-SPAM Act.[57] In doing so, the court indicated that advertising campaigns through social networks such as Facebook may now fall under the protection of the CAN-SPAM Act.[58]

The CAN-SPAM Act is important in assisting the FTC in regulating the protection of personal data, particularly in the mobile space. Spammers can send unwanted emails and messages through social networking sites in an attempt to steal data from users; most notably, the communications can be used to appropriate a user's email address.[59] These messages can also contain hyperlinks that have the ability to infect the user's device with "malicious code," which can access the user's device contents and steal important information.[60] While this problem is certainly more prevalent on personal computers like laptops and desktops, it can also be an issue on smartphones, particularly those running Google's Android operating system due to the user-friendly, open-source nature of the platform.[61] Many users fail to understand the threat that exists and view their devices merely as phones, when they should consider them as portable, intelligent computers.[62]

While CAN-SPAM has many positive aspects, overall, the statute has not accomplished its purpose of deterring spammers. As

---

[57] Facebook, Inc. v. MaxBounty, Inc., 274 F.R.D. 279, 283-84 (N.D. Cal. 2011); *see also Facebook Is Off-the-wall*, FACEBOOK (July 27, 2007), https://www.facebook.com/notes/facebook/facebook-is-off-the-wall/3532972130 (stating that the Facebook wall is a place on a user's Facebook page where friends can leave messages, photos, or video recordings); *Facebook Gets a Facelift*, FACEBOOK (Sept. 5, 2006), https://www.facebook.com/notes/facebook/facebook-gets-a-facelift/2207967130 (showing that a news feed is an aggregation of the latest headlines gathered from a user's friends).

[58] Stuart D. Levi, *Application of the CAN-SPAM Act to Social Networking Sites*, SKADDEN (May 12, 2011), https://www.skadden.com/insights/application-can-spam-act-social-networking-sites.

[59] Carolyn Duffy Marsan, *CAN-SPAM: What Went Wrong?*, NETWORKWORLD (Oct. 6, 2008, 1:00 AM), http://www.networkworld.com/article/2276180/security/can-spam--what-went-wrong-.html.

[60] *Id.*

[61] Dan Graziano, *Protect Your Android Device from Malware*, CNET (June 25, 2014, 2:00 PM), http://www.cnet.com/how-to/protect-your-android-device-from-malware/. Phones running the Android operating system account for more than half of all smartphones. *Id.* As a result of this large adoption rate, cybercriminals tend to target the Android operating system more than the others that are available to consumers. *Id.* Further, because the Android operating system is open-source, cybercriminals find it easier to obtain personal information from Android owners. *Id.* For a more detailed discussion on the open-source nature of the Android operating system, *see generally The Android Open Source Project*, ANDROID, https://source.android.com/ (last visited May 10, 2015).

[62] *The Android Open Source Project*, *supra* note 61.

of 2010, "approximately [9] out of every 10 emails are spam," an illustration of the overall ineffectiveness of the statute.[63] Perhaps part of the problem is that spam and data privacy present global issues which are not isolated within the United States. Legislation in the United States may not be efficient in solving what has clearly become an international problem. What is required appears to be global cooperation to keep users' data secure from these types of threats. This solution, among others, is discussed in further detail in Section IV below.

3. The Fair Credit Reporting Act

First enacted in 1970, the Fair Credit Reporting Act represents the federal government's first statute concerning the consumer reporting industry.[64] A consumer reporting agency is one that collects "information and provide[s] reports on consumers that are used to decide whether to provide consumers credit, insurance, or employment, and for other purposes."[65] These agencies include large well known credit reporting companies, such as Equifax, Experian, and Trans Union.[66] Congress, recognizing the importance that companies gathering this information act with a higher level of responsibility and respect towards a consumer's right to privacy, enacted the FCRA.[67] The FCRA sets forth guidelines for companies which use data to "determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants."[68] In other words, the FCRA governs how various agencies handle consumers' credit information.[69]

---

[63] Martin Lee, *Six Years Later, CAN-SPAM Act Leaves Spam Problem Unresolved*, SC MAG. (Feb. 16, 2010), http://www.scmagazine.com/six-years-later-can-spam-act-leaves-spam-problem-unresolved/article/163857/.

[64] 15 U.S.C. § 1681 (1970).

[65] LIST OF CONSUMER REPORTING AGENCIES, CONSUMER FIN. PROT. BUREAU 1 (Jan. 2015), http://files.consumerfinance.gov/f/201501_cfpb_list-consumer-reporting-agencies.pdf.

[66] *Credit Reporting Agencies*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/consumers/consumer/ccc/reporting.html (last visited May 10, 2015).

[67] *About FCRA/FACT Act*, *supra* note 64. While larger credit reporting agencies like Equifax typically collect information about transactions with businesses, smaller specialty reporting agencies can gather more sensitive information like bank accounts, medical records, insurance claims, and employment records. *What are Specialty Consumer Reporting Agencies and What Kind of Information Do they Collect?*, CONSUMER FIN. PROT. BUREAU (Jan. 21, 2015), http://www.consumerfinance.gov/askcfpb/1813/what-are-specialty-consumer-reporting-agencies-and-what-kind-information-do-they-collect.html.

[68] PRIVACY AND DATA SECURITY UPDATE, *supra* note 23, at 6.

[69] Stephanie Lane, *What is the Fair Credit Reporting Act?*, NOLO, http://www.nolo.

While the FCRA was passed at a time well before smartphones, or even cellular phones, were prevalent, the FTC has applied this law to the mobile space. The FTC has warned companies that mobile apps which collect data for background screening could potentially fall under the umbrella of the FCRA.[70] The FTC stated, "[u]nder the FCRA, operations that assemble or evaluate information to provide to third parties qualify as consumer reporting agencies, or CRAs. Mobile apps that supply such information may qualify as CRAs under the Act."[71] The FTC reasoned that persons accessing the reports must have a permissible purpose.[72] Further actions taken by the FTC in this respect are discussed in detail in Section III.

As with the other regulations discussed, it is important for lawmakers to continue expanding the type of protection that is afforded to mobile devices. The FCRA still offers protection that is too narrow for users of smartphones and, therefore, needs to be amended accordingly. The FCRA simply was not created with the current level of technology in mind. While amendments would perhaps be the easiest course of action, the ultimate goal should be the creation of a single privacy statute that would regulate the mobile space.

4. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act, enacted in 1986, is the primary law in the United States governing cybercrimes.[73] This act was intended to protect against unauthorized access to large computers, primarily those under government supervision.[74] At the time, there was serious concern about the threat of computer hacking, especially surrounding the systems that had control over the country's nuclear weapons.[75] Initially, the scope of protection offered by the CFAA was very limited, applying primarily to computers under con-

com/legal-encyclopedia/what-is-the-fair-credit-reporting-act.html (last visited Jan. 30, 2015).

[70] *FTC Warns Marketers that Mobile Apps May Violate Fair Credit Reporting Act*, FTC (Feb. 7, 2012), http://www.ftc.gov/news-events/press-releases/2012/02/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting.

[71] *Id.*

[72] *Id.*

[73] James Hendler, *It's Time to Reform the Computer Fraud and Abuse Act*, SCIENTIFIC AM. (Aug. 16, 2013), http://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/.

[74] *Id.*

[75] *Id.*

trol of the federal government.[76] However, as the public's use of computers increased and as a response to a rise in cyber-attacks, the CFAA was amended several times.[77] Amendments in 2008 expanded certain sections to criminalize actions such as "conspiring to commit a computer hacking offense," and broadening the scope of what constituted a protected computer to "those computers used in or affecting interstate or foreign commerce or communication."[78] Even further, courts have held that the CFAA considers personal computers to be protected computers, and thus fall within the statute because of the ability to connect to the internet.[79]

In *United States v. Kramer*,[80] the Eighth Circuit Court of Appeals found that smartphones constitute a protected computer governed under the CFAA.[81] The court recognized that data stored on smartphones is just as important to protect because "data stored on smartphones is no different from data stored on a desktop [computer]."[82] With this holding, the court opened the door to the CFAA's protection of future technologies which consumers may use.[83]

As it stands now, it seems as though the CFAA is the most important statute for protecting smartphone privacy in the United

---

[76] PROSECUTING COMPUTER CRIMES, DEP'T OF JUSTICE 1-2 (2010), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

[77] Hendler, *supra* note 73 (noting that the act was expanded by the post-9/11 enactment of the Patriot Act).

[78] PROSECUTING COMPUTER CRIMES, *supra* note 76, at 2.

[79] United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (holding that a connection to the internet allows a computer to communicate interstate, and thus, be a part of interstate commerce).

[80] 631 F.3d 900 (8th Cir. 2011), *cert. denied*, 131 S. Ct. 2977 (2011).

[81] *Id.* at 902-03 (reasoning that since a phone has the capability to perform arithmetic, logical, and storage functions, it should be considered a computer under the broad definition of the CFAA); 18 U.S.C. §1030(e)(1) defines the term computer to mean:

> [A]n electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device . . . .

Id.

[82] Shawn Tuma, *Smartphones and the Computer Fraud and Abuse Act – Already Covered?*, BUS. CYBER RISK (Apr. 13, 2011), http://shawnetuma.com/2011/04/13/smartphones-and-the-computer-fraud-and-abuse-act-already-covered/.

[83] *Id.* The court in *Kramer* recognized that the language of the CFAA would lead to other devices falling under its protection, stating that "[a]s technology continues to develop, § 1030(e)(1) may come to capture still additional devices that few industry experts, much less the Commission or Congress, could foresee." *Kramer*, 631 F.3d at 903-04.

States. With that being said, more consideration should be given to the implications of this statute on the mobile space. The decision in *Kramer* was an important one, but it appears that the court preferred a narrower definition as to what constitutes a mobile computer. The court acknowledged that the definition of a computer in the CFAA is broad, and that while a normal cellular phone may not easily fall under the "colloquial definition" of a computer, it was bound to follow the definition set forth in the CFAA.[84] This language implies that the court believed that the CFAA provided for a narrower definition of the term "personal computer," which would be detrimental to a more uniform policy on mobile data privacy. In other words, the court in *Kramer* seemed reluctant to treat a normal cellular phone as a personal computer due to the statute's wording which demonstrates how outdated the statutes governing mobile data privacy are. Narrow definitions should not be used for this type of consumer protection, and courts should be expanding, not restricting, protection afforded to smartphones and mobile devices.

5. The Supreme Court on Smartphone Data Privacy

In *Riley v. California*,[85] the United States Supreme Court issued a monumental decision in the smartphone privacy landscape, holding that police must obtain a warrant to search information on an arrestee's cellphone, greatly increasing protection of mobile data afforded to Americans.[86] *Riley* involved two cases, consolidated for appeal, which dealt with law enforcement's warrantless search of the defendants' cellular phones upon arrest.[87] These searches ultimately produced incriminating evidence against the defendants.[88] The officers argued that searching phones was analogous to searching any other physical items that would be on an arrestee's person.[89] Chief Justice John Roberts authored the opinion, noting that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those

[84] *Kramer*, 631 F.3d at 903-04 (noting that while a smartphone may easily qualify as a personal computer, a regular cellular phone is more difficult to come within the definition of a personal computer, which would be protected by the CFAA).

[85] 134 S. Ct. 2473 (2014).

[86] *Id.* at 2495.

[87] *Id.* at 2480.

[88] *Id.* at 2480-81.

[89] *Id.* at 2488-89.

implicated by the search of a cigarette pack, a wallet, or a purse."[90] The Court went even further, noting that "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[91] In so deciding, the Court stressed that while a decision of this magnitude was sure to impede some investigations, an individual's rights sometimes outweigh the convenience of law enforcement and the government, and that "[p]rivacy comes at a cost."[92]

This ruling may have consequences in regard to questions that may surface as technology advances.[93] It is impossible to know how technology will change in just a few short years, and even a decision such as *Riley* may find itself quickly outdated. Evolving technology requires mobile data privacy to be held to a higher standard, a principle now recognized by the highest court in the United States. Further, this ruling could set the stage for the Court's resolution of future innovative cases. For instance, how would the Court view newer technology that could store even more sensitive data than consumers already carry on their smartphones? The Court is moving in the right direction, benefitting individuals and their data. The legislature should take note of the progress being made by the courts and enact legislation to protect technology more comprehensively as it evolves.

III. DATA PRIVACY CONTROVERSIES—FTC ENFORCEMENT

The FTC's responsibilities for promulgating regulations and enforcing current laws which apply to data privacy are generally in-

[90] *Riley*, 134 S. Ct. at 2488-89. Justice Roberts noted that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Id.* at 2489. Phones could easily be analogized to cameras or other electronics, and further, the amount of data that a modern cell phone can store is immense. *Id.* People cannot physically carry every picture, book, or article with them, and if they did, it would result in the person's carrying around a large storage container which would require a warrant to search. *Id.* This is contrasted with the small size and storage capacity of a cigarette container the Court used as a counter example to a cellular phone. *Id.*

[91] *Riley*, 134 S. Ct. at 2490. Justice Roberts reasoned that modern cell phones may contain a great deal of private information for many Americans, and that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* at 2495.

[92] *Id.* at 2493.

[93] Jess Bravin, *Supreme Court: Police Need Warrants to Search Cellphone Data*, WALL ST. J. (June 25, 2014, 7:50 PM), http://www.wsj.com/articles/high-court-police-usually-need-warrants-for-cell-phone-data-1403706571.

sufficient. In most instances, its enforcement actions do not go to trial; rather, monetary settlements are agreed on between the FTC and the offending company.[94] As of a 2014 security update published by the FTC, the Commission has brought hundreds of cases to protect consumers.[95] Specifically, the FTC has addressed a wide variety of privacy issues, "including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile."[96] These particular matters include over 170 cases related to consumer privacy.[97] For violations of official FTC orders, the Commission can seek civil monetary penalties, and the same is true for violations of statutes like the COPPA and the CFAA.[98] Overall, the FTC has done an adequate job of protecting the privacy interests of consumers; however, it can take additional steps to improve consumer protection.

A. FTC Settles with HTC America

HTC America ("HTC"), one of the leading mobile device manufacturers in the United States, manufactures smartphones that run on Android, Windows Mobile, and iOS operating systems.[99] Google, Microsoft, and Apple developed these mobile operating systems, respectively.[100] In 2013, the FTC filed a claim, charging HTC for failing to secure software on phones that were shipped to the United States.[101] These security flaws that existed on users' devices placed sensitive information about millions of people at risk of being compromised by potential third-party app developers.[102]

The flaw at issue affected primarily devices running Google's Android operating system, as third-party app developers were able to bypass Android's permission-based security to gain access to sensi-

---

[94] PRIVACY AND DATA SECURITY UPDATE, *supra* note 23, at 1.

[95] *Id.*

[96] *Id.* at 2.

[97] *Id.*

[98] *Id.* at 1.

[99] *HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers*, FTC (Feb. 22, 2013), http://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile.

[100] *Top 10 Mobile Phones Operating Systems*, SHOUTMELOUD (Jan. 24, 2015), http://www.shoutmeloud.com/top-mobile-os-overview.html.

[101] *HTC America Settles*, *supra* note 99 (noting that this action was brought based on HTC's violation of the Federal Trade Commission Act).

[102] *Id.*

tive personal information of the user.[103] According to Google's security guidelines, "[a]pplications statically declare the permissions they require, and the Android system prompts the user for consent at the time the application is installed. Android has no mechanism for granting permissions dynamically (at run-time) because it complicates the user experience to the detriment of security."[104] In other words, the only time a user can grant an app permission to access certain parts of his or her smartphone is when the user first installs the application from Google's application market, called the Google Play Store.[105] The information at risk in this particular case included text messages, audio, and calendar entries.[106] What is more, the flaw made it possible for the installation of malicious applications on the user's smartphone without the user's permission, which was capable of recording and transmitting data such as financial information, medical information, and geolocation data.[107]

HTC ultimately reached a settlement with the FTC, requiring the company to establish "a comprehensive security program."[108] Further, the settlement required HTC to "develop and release software patches to fix vulnerabilities found in millions of HTC devices."[109] As part of the FTC's education outreach, the Commission encouraged users to apply the patches as quickly as possible in order to

---

[103] *Id.*

[104] *System Permissions*, ANDROID, http://developer.android.com/guide/topics/security/permissions.html (last visited Feb. 27, 2015).

[105] *Review App Permissions*, GOOGLE, https://support.google.com/googleplay/answer/6014972?hl=en (last visited Feb. 27, 2015). The Google Play Store is an application marketplace where users can download "music, movies, books, and Android apps and games," and comes pre-installed on devices running the Android operating system. *Find the Google Play Store App*, GOOGLE, https://support.google.com/googleplay/answer/190860?hl=en (last visited May 10, 2015).

[106] *HTC America Settles*, *supra* note 99.

[107] *Id.* This was a pre-emptive measure taken by the FTC. There was no evidence presented showing that users' devices had been infected, but rather stated that there was a possibility that this could happen.

[108] *Id.* This security program would work "to address security risks during the development of HTC devices," and requires the company "to undergo independent security assessments every other year for the next 20 years." *Id.*

[109] *Id.* The decision and order issued by the FTC states that these software patches apply to devices released "on or after December 2010." *In re* HTC Am., Inc., FTC File No. 122-3049, 2013 WL 3477025, at *4 (F.T.C. June 25, 2013). These patches were required to "provide users of the affected covered devices with clear and prominent notice regarding the availability of the applicable security patch(es) and instructions for installing the applicable security patch(es)." *Id.*

prevent the risk of further vulnerability.[110]

This action was part of the FTC's effort to help instruct companies on how to secure devices that are sent to their users.[111] For example, the Commission introduced a business guide providing app developers with guidelines to achieve reasonable data security.[112] This type of action is important to foster better awareness surrounding data security in smartphones, and the FTC should continue to be a leader in educating consumers and businesses on the best practices of data privacy.

B. FTC Action against COPPA Violations

The Commission has also been active in bringing cases against companies that may be in violation of the COPPA, and "[s]ince 2000, the FTC has brought over 20 COPPA cases and collected millions of dollars in civil penalties."[113] An update to a regulatory rule used to implement the COPPA allows the FTC to address new technological advancements, "such as social networking, smartphone internet access, and the ability to use geolocation information," if children's privacy concerns are implicated.[114] For instance, the FTC brought actions against Yelp, Inc. ("Yelp"), TinyCo, Inc. ("TinyCo"), and the social networking service "Path" for COPPA violations.[115]

In the action against online review website Yelp, the FTC alleged that over several years, the company improperly collected information from children using the Yelp app on mobile devices.[116] This information was obtained without parental notification or consent in violation of the COPPA.[117] When users (including both chil-

---

[110] *HTC America Settles*, *supra* note 99.

[111] *Id.*

[112] *Id.*

[113] PRIVACY AND DATA SECURITY UPDATE, *supra* note 23, at 7.

[114] *Id.*

[115] *Yelp, TinyCo Settle FTC Charges Their Apps Improperly Collected Children's Personal Information*, FTC (Sept. 17, 2014), http://www.ftc.gov/news-events/press-releases/2014/09/yelp-tinyco-settle-ftc-charges-their-apps-improperly-collected.

[116] *Id.* Yelp is a company founded in 2004 and offers a website designed to assist people in finding local businesses. *About Us*, YELP, http://www.yelp.com/about (last visited May 10, 2015). The service has a mobile application available on smartphones, which uses automated software to give recommendations to consumers based on reviews left by users of the Yelp application. *Id.*

[117] *Yelp, TinyCo Settle*, *supra* note 115.

dren and adults) registered for the service through the mobile application, they were prompted to provide their birth dates.[118] According to the FTC's complaint, "several thousand registrants provided a date of birth showing they were under 13 years old."[119] Yelp obtained information from these children, including "name, email address, and location, as well as any information that they posted on Yelp."[120] Also listed in the complaint were allegations that Yelp did not properly screen registrants so that children under the age of 13 could register, and that Yelp did not adequately test the app to prevent such registration.[121] Yelp settled with the FTC and was required to pay $450,000 in civil penalties, as well as delete all of the information collected from users who entered birth dates indicating they were 13 years old or younger.[122]

The FTC's complaint against application developer TinyCo alleged that the company's popular apps were targeting children.[123] Specifically, the complaint named "Tiny Pets, Tiny Zoo, Tiny Monsters, Tiny Village and Mermaid Resort" as the applications alleged to be engaging in these practices.[124] The FTC claimed that these names appealed to children, and as such, were directed at children who were under the age of 13.[125] The apps in question were able to collect email addresses from children under the age of 13, as well as other users.[126] An added incentive to provide users with "extra in-game currency" existed to convince users to provide their email addresses.[127] This in-game currency would enable users playing the games to buy items or advance through the game more quickly than they otherwise might have been able.[128] TinyCo settled with the

---

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] *Yelp, TinyCo Settle*, *supra* note 115.

[123] *Id.* TinyCo is a company based in San Francisco, and develops mobile games for smartphones. *About TinyCo*, TINYCO, http://www.tinyco.com/about/ (last visited May 10, 2015). The company's "games have been downloaded more than 85 million times worldwide." *Id.*

[124] *Yelp, TinyCo Settle*, *supra* note 115.

[125] *Id.*

[126] *Id.*

[127] *Id.* In-game currency refers to "any game-based token or means of exchange." Paula Gilardoni, Emma Ringland & Angela Ha, *In-game Currencies: In the Line of Fire?*, LEXOLOGY (Aug. 19, 2014), http://www.lexology.com/ library/detail.aspx?g=8d743082-b318-451f-b606-0930b91f152b.

[128] *Yelp, TinyCo Settle*, *supra* note 115.

FTC, agreeing to pay $300,000 in civil penalties, as well as delete all the information collected in violation of the COPPA.[129] Further, the FTC required TinyCo to submit a report one year from the settlement, describing how it had complied with the FTC's terms.[130] It remains to be seen whether TinyCo has complied with the FTC's terms, as the report will not be submitted until late 2015.

The operator of the social networking application, Path, collected personal information from users' contact directories on their mobile devices without the knowledge or consent of the user.[131] Path is a social network service in which users can create a journal detailing parts of their life, and then share what they create with friends and family.[132] The app allowed users to upload photos, written "thoughts," geolocation data, as well as music users are listening to while creating the content they enter into the app.[133] The FTC alleged that Path's iOS application did not give consumers a choice when it came to collecting personal information.[134] The Path application offered a feature in which users had the ability to find friends by using either their contact information stored on the users' mobile device, searching through the users' Facebook account, or by inviting a friend through email or text message.[135] However, the Path application would always collect and store contact information from the users' address books on their phones or mobile devices.[136] This would occur regardless of which option the users selected.[137] The application "automatically collected and stored any available first and last names, addresses, phone numbers, email addresses, Facebook and Twitter usernames, and dates of birth" found on the devices.[138]

---

[129] *Id.*

[130] *Id.* In addition to this compliance report, TinyCo is required to respond to any written request for information pertaining to this order within 14 days of receipt. Stipulated Order for Permanent Injunction and Civil Penalty at 12, United States v. TinyCo, Inc., No. 3:14-cv-4164 (N.D. Cal. Sept. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140917tinycostip.pdf.

[131] *Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books*, FTC (Feb. 1, 2013), http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Path Social Networking App Settles*, *supra* note 131.

[137] *Id.*

[138] *Id.*

Path's collection of data violated the provisions of the COPPA. Approximately 3,000 of the users who had information collected were children under the age of 13, who gave that information without parental consent.[139] Specifically, the FTC's complaint stated that Path had violated the COPPA by not clearly stating its policy on collection of children's personal information, not giving parents notice that it was collecting this information, and "not obtaining verifiable parental consent before collecting [the] information."[140] Similar to the instances above, Path agreed to pay $800,000 in civil penalties as well as delete the information that it gathered from all children who were under the age of 13.[141] Further, Path was prohibited from making "any misrepresentations about the extent to which it maintains the privacy and confidentiality of consumers' personal information."[142]

Undoubtedly, the FTC will continue to monitor companies for COPPA violations. As part of each of the above settlements, the FTC has required the companies to comply with COPPA in the future, as well as submit compliance reports outlining the adjustments made to particular apps or programs.[143] Whether these infringers actually follow through with these requirements remains to be seen. In nearly all cases, the FTC has the ability to request updates regarding the status of enforcement but more power may be needed to prevent similar violations by such companies in the future. This issue is addressed in Section IV below.

C. FTC Enforcement of the FCRA

The FTC is also charged with enforcement of the Fair Credit Reporting Act ("FCRA").[144] In doing so, "[t]he FTC has brought 100 FCRA cases against companies for credit-reporting problems and has collected over $30 million in civil penalties."[145] Among these cases

---

[139] *Id.*

[140] *Id.*

[141] *Path Social Networking App Settles*, *supra* note 131.

[142] *Id.*

[143] *Yelp, TinyCo Settle*, *supra* note 115. The compliance reports are to be submitted one year from the date that a settlement was reached with the various offenders and, as such, are not yet available for analysis. It remains to be seen whether the offending companies will comply with the FTC's orders.

[144] PRIVACY AND DATA SECURITY UPDATE, *supra* note 23, at 1.

[145] *Id.* at 6.

was a suit against a mobile app developer, Filiquarian Publishing LLC, which collected and sold criminal records through an application that it developed.[146]

The FTC filed a complaint alleging that Filiquarian did not check the accuracy of information collected through its mobile app, and the company did not give users of these criminal records reports of their FCRA obligations.[147] The complaint also alleged that the company did not ensure that the information would be used "only for legally permissible purposes."[148] Consumers were able "to access hundreds of thousands of criminal records and conduct searches on potential employees."[149] The application in question cost 99 cents and allowed a user who downloaded it to perform unlimited searches for these records.[150]

Filiquarian claimed that the application contained a disclaimer indicating the lack of FCRA compliance, and cautioning that its products should not be used to screen applicants for employment or for insurance or credit screening purposes.[151] The disclaimer further noted that anyone using the information for this purpose would assume "sole responsibility for FCRA compliance."[152]

The FCRA, while arguably not the most important of the data privacy statutes, is still necessary for consumer protection. Mobile applications are becoming increasingly more capable of collecting and storing sensitive information. As these applications become more advanced, greater protection should be afforded to consumers. In applying the FCRA to the mobile space, the FTC has taken an important first step towards increasing consumer protection; however,

---

[146] *Marketers of Criminal Background Screening Reports to Settle FTC Charges They Violated Fair Credit Reporting Act*, FTC (Jan. 10, 2013), https://www.ftc.gov/news-events/press-releases/2013/01/marketers-criminal-background-screening-reportsto-settle-ftc.

[147] *Id.* The application's users were businesses that were looking for new employees. *Id.* The application description stated, "[a]re you hiring somebody and wanting to quickly find out if they have a record? Then Texas Criminal Record Search is the perfect application for you." *Id.*

[148] *Id.*

[149] *Marketers of Criminal Background*, *supra* note 146.

[150] *Id.*

[151] *Id.* In its complaint, the FTC noted, "these disclaimers are not enough to avoid liability under the FCRA because the company advertised and expected that its reports could be used for employment purposes." *Id.*

[152] *Id.* The FTC settled with Filiquarian, barring the company "from furnishing a consumer report to anyone they do not have reason to believe has a 'permissible purpose' to use the report," creating a heightened standard for distribution of these reports. *Marketers of Criminal Background*, *supra* note 146.

companies such as Filiquarian may continue to maintain insidious practices to steal data unless more comprehensive legislation is passed.

D. Notable Unresolved Controversies

While the instances mentioned above have all been resolved, there are still many potential controversies concerning data privacy and smartphones. Millions of mobile applications are available to smartphone users, and as of 2014, applications have been downloaded 75 billion times from the Apple App Store alone.[153] Many of these apps request permissions to access data that may have little or no relevance to the function of the app itself.[154] For instance, there have been ongoing issues surrounding a piece of software called Carrier IQ and Facebook's use of a messenger application installed on smartphones.[155]

Carrier IQ is software developed by a company using the same name and, as of December 14, 2011, it had been installed on approximately 150 million mobile phones.[156] The company is under federal investigation for allegedly having used the software to track activities of users on their phones and then having sent that information to cellphone companies without permission.[157] The controversy arose when security researcher Trevor Eckhart found evidence that the Carrier IQ software installed on smartphones tracked "every keystroke and text message written by users and sent the information

---

[153] *Statistics and Facts about Mobile App Usage*, STATISTA, http://www.statista.com/topics/1002/mobile-app-usage/ (last visited May 10, 2015).

[154] Howard Solomon, *Many Mobile Apps Still Ask for Unexplained Access to Device Data*, IT WORLD CANADA (Sept. 11, 2014), http://www.itworldcanada.com/article/many-mobile-apps-still-ask-for-unexplained-access-device-data/97219. Examiners from multiple countries found that approximately one-third of applications required access to certain unrelated information on devices, such as geolocation and photographs. *Id.* Many of these applications did not explain why access to this information was needed, and those that offered an explanation did so in small print contained in lengthy privacy policies that consumers are not likely to read. *Id.*

[155] *See* Sari Horwitz, *Carrier IQ Faces Federal Probe into Allegations Software Tracks Cellphone Data*, WASH. POST (Dec. 14, 2011), http://www.washingtonpost.com/business/economy/feds-probing-carrier-iq/2011/12/14/gIQA9nCEuO_story.html; Reed Albergotti, *Facebook Messenger Privacy Fears? Here's What to Know*, WALL ST. J. BLOG (Aug. 8, 2014, 9:13 AM), http://blogs.wsj.com/digits/2014/08/08/facebook-messenger-privacy-fears-heres-what-you-need-to-know/.

[156] Horwitz, *supra* note 155.

[157] *Id.*

on the handsets to carriers."[158] These cellular carriers are alleged to include three of the four major cell phone providers in the United States, namely AT&T, Sprint, and T-Mobile, though they deny that the use of the software violates their respective privacy policies.[159] A spokesperson for the fourth major carrier, Verizon Wireless, claims that the company does not use the Carrier IQ software on any of the provider's devices, and thus is not engaging in any deceptive practices.[160]

This issue has drawn the interest of the United States Senate, with Senator Edward Markey requesting that the FTC "investigate the practices of Carrier IQ as possibly unfair or deceptive."[161] In particular, Senator Markey is concerned that the software was secretly collecting users' personal information, most notably text message contents.[162] He noted that "[c]onsumers and families need to understand who is siphoning off and storing their personal information every time they use their [smartphones]."[163]

Carrier IQ is currently faced with several class-action lawsuits filed on behalf of consumers, which were all consolidated into one suit in the United States District Court in San Francisco.[164] As of February 27, 2015, Carrier IQ has agreed in principle to a settlement to resolve the lawsuit.[165] Details of the settlement, which have not been finalized, are not yet available. Several smartphone manufacturers were also named in the class-action suit but have not agreed to a settlement.[166] These include large companies, such as Samsung, HTC, and LG Electronics.[167]

Another notable issue surrounds the social networking website Facebook. In recent months the company has come under fire for permissions requested by the Facebook Messenger application on

---

158 *Id.*

159 *Id.* (noting that AT&T, Sprint, and T-Mobile concede that this software is used on their wireless devices, but claim that the use of this software is not in violation of any privacy policies).

160 *Id.*

161 Horwitz, *supra* note 155.

162 *Id.*

163 *Id.*

164 Wendy Davis, *Carrier IQ Agrees to Settle Privacy Battle*, MEDIAPOST (Nov. 4, 2014, 4:11 PM), http://www.mediapost.com/publications/article/237608/carrier-iq-agrees-to-settle-privacy-battle.html.

165 *Id.*

166 *Id.*

167 *Id.*

mobile devices, particularly those for use with the Android operating system.[168] These permissions include the ability for the application to access photos, text message information, as well as the mobile device's microphone.[169] In an article in the *Huffington Post*, Sam Fiorella notes that the application has the ability to take direct control of a user's phone, going so far as being able to make phone calls without the user's authorization.[170] The application has over 200,000 active users each month, and it is likely that a majority of these users are not even aware of the privacy concerns that surround the app. As Fiorella notes, "[t]he fact that so many people have agreed to these permissions is an alarming insight into the future of mobile apps and personal security."[171]

Facebook has countered these allegations by stating that these privacy concerns are based on misinformation, and as a result, are being overanalyzed.[172] When downloading an app on the Android operating system, a user must agree to all permissions at one time, as opposed to Apple's iOS, in which users can agree to permissions on a case-by-case basis.[173] Facebook argues that as a result, the company has less control over how the application's permissions are represented to consumers, and the language used in the application is limited to generic terms provided by Android.[174] In other words, the permis-

---

[168] Albergotti, *supra* note 155. Facebook's Messenger application allows users to use their mobile phones to access messages received on their Facebook accounts. *What Is the Messenger App and Why Am I Being Asked to Install It?*, FACEBOOK, https://www.facebook.com/help/237721796268379 (last visited May 10, 2015). The Messenger functionality was previously contained in Facebook's main application, but the company notified users that they would no longer be able to see their messages unless they downloaded the additional Facebook Messenger Application. Albergotti, *supra* note 155. Users had no choice but to download the new application with insidious permission requirements, otherwise they would no longer have access to their messages on their mobile devices. *Id.*

[169] *Id.*

[170] Sam Fiorella, *The Insidiousness of Facebook Messenger's Android Mobile App Permissions*, HUFFINGTON POST BLOG (Aug. 11, 2014, 5:59 PM), http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face_b_4365645.html. Jonathan Zdziarski, a forensics and security researcher, stated that "Messenger appears to have more spyware code in it than I've seen in products intended specifically for enterprise surveillance." Matthew Braga, *Facebook's Messenger App Is Tracking a Lot More of Your Data than You Think*, MOTHERBOARD (Sept. 10, 2014, 2:35 PM), http://motherboard.vice.com/read/facebooks-messenger-app-is-tracking-a-lot-more-of-your-data-than-you-think. Zdziarski further noted that he was unaware that this type of access was even possible, and that Facebook was "running analytics on nearly everything it possibly can monitor on your device." *Id.*

[171] Fiorella, *supra* note 170.

[172] Albergotti, *supra* note 155.

[173] *Id.*

[174] *Id.* Facebook argues that because the company is unable to create its own privacy

sions do not "necessarily reflect the way the Messenger app and other apps use them."[175] This issue has yet to receive any attention from federal investigators and it does not appear likely that it will because Facebook has not violated any law. In addition, these security vulnerabilities seem to be theoretical at this point; there is no conclusive data showing that anyone has taken advantage of flaws in the code. This is troubling, as investigators should not wait for an incident to occur before taking action. Organizations like the FTC should work harder to take preventative action before consumers' data becomes compromised.

The controversies detailed above illustrate the currently flawed system the United States uses to regulate data privacy on mobile devices; there simply is not a uniform law or system in place. The regulations that are currently in effect do not offer the proper protection consumers need from companies that are seeking to obtain and abuse information to give them a competitive edge in today's growing market of the mobile space. For instance, monetary penalties placed on offending companies may not entirely deter them from taking the same type of insidious actions in the future. For many of these companies, fines may be a small price to pay in exchange for gaining a competitive advantage over others. Consumers require greater protection from these types of practices. Some potential solutions to this growing issue are discussed in Section IV below.

IV. WHAT ELSE CAN BE DONE?

The statutes mentioned above fall far short of providing consumers adequate protection of their data on mobile devices. Because the system consists primarily of older statutes that did not originally protect smartphones and other mobile devices, there are gaps that allow controversies such as the ones mentioned above to occur. Had there been a uniform law regulating data privacy in the mobile space, some of these controversies may have been avoided completely. For instance, uniform regulations on the presentation of application permissions to the consumer could have avoided the controversy with Facebook Messenger.

If not a single law, then several new data privacy laws should

permission language, the permissions of the application do not reflect how the Android application actually uses the permissions. *Id.*

[175] *Id.*

be enacted that specifically apply to the mobile space. These statutes should focus on disclosure and allowing consumers to make educated choices as to when companies can obtain access to data on their devices. Improved laws should also provide better guidance to manufacturers of these devices and to the application developers that have been taking advantage of the lack of current protections. This change is necessary because antiquated statutes which have been retrofitted to apply to the mobile space simply are inadequate to tackle contemporary and future problems.

A. The Consumer Privacy Bill of Rights

Perhaps the most obvious solution would be the creation of a set of guidelines for maintaining data privacy. While this may seem like a daunting task, there appears to be some movement on this front. In February 2012, the White House released a document dealing with consumer data privacy in response to the growing global digital economy.[176] In a memo at the beginning of the document, President Obama noted that "[n]ever has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones," as well as stating that we should "apply our timeless privacy values to the new technologies and circumstances of our times."[177] At the forefront of this document was a guideline for setting forth a Consumer Privacy Bill of Rights, which would implement "a baseline of clear protections for consumers and greater certainty for companies."[178]

The Consumer Privacy Bill of Rights would apply "globally recognized Fair Information Practice Principles ("FIPPs")[179] to the interactive and highly interconnected environment in which we live and work today."[180] Essentially, these FIPPS would provide companies with general principles to follow at their own discretion when

[176] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1 (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter CONSUMER DATA PRIVACY].

[177] *Id.*

[178] *Id.*

[179] *The Fair Information Practice Principles*, NAT'L INST. OF STANDARDS & TECH., http://www.nist.gov/nstic/NSTIC-FIPPs.pdf (last visited Feb. 27, 2015) (noting that the FIPPs are a "widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy").

[180] CONSUMER DATA PRIVACY, *supra* note 176, at 1.

dealing with consumers' data.[181] The idea is that allowing these companies flexibility in implementing these principles would "help promote innovation," and "encourage effective privacy protections by allowing companies, informed by input from consumers, . . . to address the privacy issues that are likely to be most important to their customers and users, rather than requiring companies to adhere to a single, rigid set of requirements."[182]

The document stresses that Congress should pass legislation which would adopt the Consumer Privacy Bill of Rights.[183] Further, it states that in the legislation, Congress should provide the FTC with the ability to "enforce these rights directly."[184] The same power should be granted to State Attorneys General so that states could provide resources in enforcement actions as well.[185] Granting this type of power would provide the FTC with greater flexibility to respond to emerging privacy issues "through specific enforcement actions," which would be governed through statute and not just FTC guidelines.[186]

There has not been a great deal of movement on the issue until recently, when at an FTC event on January 12, 2015, President Obama announced a proposal for several "new cyber security initiatives," perhaps the most important of which would include the Consumer Privacy Bill of Rights.[187] The President noted that "consumers feel like they no longer have control over their personal information and that needs to be addressed."[188] It remains to be seen whether this will indeed become a law or whether a bill will be introduced at all. If enacted, this would represent a giant step in the right direction toward better privacy protection in the United States. Smartphone users would be protected by concrete regulations that were specifically tailored towards protecting data in the mobile space, supported by an

---

[181] *Id.* at 2.

[182] *Id.*

[183] *Id.* at 35.

[184] *Id.*

[185] CONSUMER DATA PRIVACY, *supra* note 176, at 35 (noting that granting the State Attorneys General this type of power would give the states the ability to enforce violations of these guidelines directly).

[186] *Id.* at 36.

[187] Ruth Reader, *President Obama Proposes 'Consumer Privacy Bill of Rights,'* VENTUREBEAT (Jan. 12, 2015, 10:06 AM), http://venturebeat.com/2015/01/12/president-obama-proposes-consumer-privacy-bill-of-rights/.

[188] *Id.* (noting that "[w]e pioneered the Internet, but we also pioneered the Bill of Rights").

organization (the FTC) with the ability to enforce violations with a greater degree of discretion.

B. The Mobile Device Privacy Act

The Consumer Privacy Bill of Rights is not the only legislation that has been recently proposed to help regulate mobile data privacy. In 2012, then Massachusetts Congressman Edward Markey introduced H.R. 6377, entitled the Mobile Device Privacy Act ("the MDPA").[189] The goal of the MDPA is to require that carriers and smartphone manufacturers inform consumers about software that may monitor or obtain their personal information and gain users' consent before "collecting and transmitting information from phones."[190] Further, the legislation would provide companies with required policies to follow when receiving personal information from consumers' mobile devices.[191] This bill was largely in response to the Carrier IQ controversy.[192]

Unfortunately, this legislation stalled in congressional committee meetings.[193] Congress may still move on this particular bill but as of now, there has been no sign of any renewed interest among members of the Legislature. This type of legislation is exactly the kind that is currently needed to help regulate smartphone privacy, and this is something that the enactment of the Consumer Privacy Bill of Rights could effectuate. If Congress considers such a bill, the focus should be on harsher penalties for companies that violate the statute. Perhaps the monetary penalties imposed on violators could be increased or more injunctive relief could be available, resulting in a greater loss in profit for the offending company. Actions such as these may be a larger deterrent for potential offenders.

V. CONCLUSION

Privacy issues will always be a controversial topic in Ameri-

---

[189] H.R. 6377, 112th Cong. (2012).

[190] Jon Brodkin, *"Mobile Device Privacy Act" Would Prevent Secret Smartphone Monitoring*, ARSTECHNICA (Jan. 31, 2012, 10:53 AM), http://arstechnica.com/tech-policy/2012/01/mobile-device-privacy-act-would-prevent-secret-smartphone-monitoring/.

[191] *Id.*

[192] *Id.*

[193] *H.R. 6377 (112th): Mobile Device Privacy Act*, GOVTRACK, https://www.govtrack.us/congress/bills/112/hr6377 (last visited May 10, 2015).

ca. Apple CEO Tim Cook recently said, "[n]one of us should accept that the government or a company or anybody should have access to all of our private information. This is a basic human right. We all have a right to privacy."[194] This sentiment is certainly shared by many Americans. Issues surrounding data privacy continue to be an ongoing and evolving issue in the United States. It is clear that the current level of protection that is afforded to consumers' smartphones is not sufficient. As technology has evolved through the years, the problem has only become more severe, and little has thus far been done to comprehensively address the issue. Smartphones present a particularly complex problem due to the sheer amount of information they hold, creating opportunity for companies to obtain and manipulate the information for their own benefit. The existence of multiple operating systems on smartphones adds to the problem, as differing permission guidelines make it difficult for developers to inform consumers about the level of access that applications require. This problem will only become more severe as technology continues to advance in the coming years.

The FTC is currently doing the best that it can with the rules and regulations in place. Uniform rules governing smartphones and mobile devices in general are necessary to enable the Commission to improve the protection of consumers' data. The patchwork system currently in place consisting of the FCRA, COPPA, CAN-SPAM, and CFAA allows companies that have a large consumer presence to use questionable practices to avoid FTC involvement, and the penalties in place are not harsh enough to deter companies from these actions; the risk does not outweigh the potential reward. These companies make millions of dollars in profit each year, and a few thousand dollars in FTC penalties are not an effective deterrent. Until something more substantive is done, companies will continue to profit from stealing consumer data.

Legislation such as the Consumer Privacy Bill of Rights is vital to achieving this goal of uniform data privacy regulation, and without it, consumer data will continue to be compromised by the insidious practices of third parties. Uniform protection would cause companies to become accountable for their actions in the mobile space and would help deter previous offenders from taking the same

[194] John Callaham, *Tim Cook Says Data Privacy Is a Basic Human Right*, IMORE (Feb. 28, 2015, 9:32 AM), http://www.imore.com/tim-cook-says-no-one-should-give-their-right-keep-their-data-private.

actions in the future. While the FTC has certainly been an advocate for data privacy, the Commission should be at the forefront of the battle for stronger regulation. This burden should not fall entirely on the FTC, but other entities such as Congress and the courts should take this matter more seriously. With decisions such as *Riley* and *Kramer*, it certainly seems that change is gradually coming. If the highest court in the United States can recognize the protection that mobile devices require, then perhaps legislators will follow suit. The FTC and members of Congress should rally behind the proposed Consumer Privacy Bill of Rights and create a safer environment for consumer data on smartphones.