YOUR HEAD IS IN THE CLOUD: THE APPLICATION OF OUTDATED PRIVACY LAW TO RAPIDLY CHANGING TECHNOLOGIES

ABSTRACT

On a daily basis, the majority of Americans casually grant sweeping permissions for mobile applications to collect massive amounts of personal information about them. Few are even aware they are doing this, and even fewer contemplate what these companies are doing with their private information. The reality is, there is virtually no federal law regulating who this information can be given or sold to. And it is not surprising—the federal law governing digital communications is older than the Internet itself.

"When current law affords more protections for a letter in a filing cabinet than an email on a server, it's clear our policies are outdated."[1] *In today's world, technology advances faster than we can keep up with, and with new technology comes an inevitable tension with personal privacy. Americans should not have to choose one or the other—it is time that Congress acknowledge this prevalent issue and address it on a nationwide basis.*

TABLE OF CONTENTS

1. Peter Whippy, *Lawmakers Introduce Bipartisan Privacy Reform Legislation*, U.S. HOUSE REPRESENTATIVES (Feb. 2, 2015), https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=397869 (statement of Suzan DelBene).

I. INTRODUCTION

We live in an age where 95 percent of the U.S. population has a cellphone,[2] and the majority of these users casually authorize companies to collect massive amounts of our personal information on a daily basis.[3] Virtually everything we do leaves a digital trail.[4] The quantity and sensitivity of the data companies store about us is frightening—it includes contact lists, location information, and web browser histories, to name a few.[5] What is more frightening yet is the lack of privacy law regulating who this information can be given or sold to.[6] For instance, without a user's affirmative consent, a mobile application (app) may collect location data tracking the user's daily routes and sell this information to an undisclosed third party.[7] Without criminal or civil liability, an app developer can create and sell a hidden app designed to spy on a cellphone user, equipping cyberstalkers with easy access to prey on their victims.[8] Few would consider

2. *Mobile Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.

3. *See* Will Schmidt, *Fact: Free Apps Sell Your Personal Data to Make Money*, TECHCO (June 3, 2015), http://tech.co/marble-security-privacy-hawk-app-2015-06 (statement of Dave Jevans) ("With little thought to the consequences, smartphone users casually give sweeping permissions to mobile apps to upload and use private information stored on their devices.").

4. Alexandra Rengel, *Privacy-Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights*, 8 INTERCULTURAL HUM. RTS. L. REV. 177, 185 (2013).

5. Schmidt, *supra* note 3. ("What [smartphone users] do not understand is that once uploaded, personal data is frequently sold to advertisers around the world. That data, in turn, can be easily stolen or purchased by cybercriminals, hackers, hostile governments, and aggressive advertising networks to mount highly targeted phishing and social media attacks.").

6. *See* discussion *infra* Part IV.

7. *See id.*

8. *See* Grant Gross, *Mobile Spying Apps Fuel Domestic Violence, U.S. Senator Says*, PCWORLD (June 4, 2014), http://www.pcworld.com/article/2360060/mobile-spying-apps-fuel-domestic-violence-us-senator-says.html (statement of then-Senator Al Franken arguing that although stalkers can be arrested, "[n]othing happen[s] to the companies making money off of the stalking.").

the legality of this type of activity desirable. This Note will discuss current federal laws governing digital privacy in Part II, analyze the inevitable tension between the innovation of new technology and protection of individual privacy in Part III, assess the impact the current lack of privacy has on Americans in Part IV, and call for the legislature to take action to bring necessary reform to federal privacy laws in Part V.

II. HISTORY OF FEDERAL LAWS THAT GOVERN PRIVACY IN INTERNET TECHNOLOGY AND MOBILE APPLICATIONS

Like many areas of the law, privacy law is failing to keep up with current technologies, and courts struggle to apply outdated laws to rapidly changing technology.[9] The Fourth and Fifth Amendments have important implications regarding privacy in government actions and criminal investigations;[10] however, this Note will focus on privacy laws that regulate private parties. In addition to a constitutional right to privacy, Americans also enjoy electronic privacy protection granted by federal and state statutes.[11] Though technology is quickly changing and current federal law is ineffective at addressing many of the issues, the concept of electronic privacy is not new.[12] For decades there have been laws regulating electronic communications via telephones and the Internet,[13] but no federal law directly addresses mobile phones or mobile apps.[14]

A. *Electronic Communications Privacy Act of 1986*

The primary source of federal electronic privacy law is derived from the Electronic Communications Privacy Act of 1986 (ECPA).[15] It is not surprising that a law passed 30 years ago, when "there was no World Wide Web, nobody carried a cell phone, and the only 'social networking' two-year-old Mark Zuckerberg was doing was at pre-school or on play dates[,]" is extremely outdated.[16] The ECPA significantly modified three federal

9. *See Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, https://www.aclu.org/feature/modernizing-electronic-communications-privacy-act-ecpa (last visited Feb. 23, 2017).

10. JAMES GRIMMELMANN, INTERNET LAW: CASES & PROBLEMS 205 (Ver. 4.0 2014).

11. *Id.* at 233.

12. *See* Katherine Gnadinger, *The Apps Act: Regulation of Mobile Application Privacy*, 17 SMU SCI. & TECH. L. REV. 415, 418 (2014).

13. *See, e.g.*, 18 U.S.C. §§ 2707, 2510–2511 (2012).

14. Gnadinger, *supra* note 12, at 418–19.

15. GRIMMELMANN, *supra* note 10, at 233.

16. *Modernizing the Electronic Communications Privacy Act (ECPA)*, *supra* note 9.

statutes: the Stored Communications Act (SCA), the Wiretap Act, and the Pen Register and Trap and Trace statute.[17] The ECPA was passed in an effort to statutorily protect the privacy of electronic communication occurring through third parties[18] by broadening the scope of privacy protection in federal laws.[19]

Privacy issues arising from modern technology are primarily governed by the Wiretap Act and the SCA, but it can be difficult to determine how these acts apply to technologies they never anticipated.[20] The SCA governs "disclosure of electronic communications stored with technology providers"[21] and prohibits "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service."[22] Today, the SCA is relevant to the privacy concerns surrounding emails and other electronic communications, but it can be difficult to apply to technologies such as cloud-computing and remote hosting, as courts struggle to determine whether documents stored remotely fall within the scope of the SCA.[23] As modified by the ECPA, the SCA provides for private civil liability, in addition to criminal liability, for violations.[24]

Likewise, under the ECPA, the Wiretap Act also provides for both criminal and private civil liability.[25] The Wiretap Act governs when wire, oral, or electronic communications are "intercepted."[26] Distinguishing when

17. *See* 18 U.S.C. §§ 2707, 2510–2511 (2012); GRIMMELMANN, *supra* note 10, at 233.

18. Michael E. Lackey, *Understanding the Electronic Communications Privacy Act*, LEXIS ADVANCE RES. (June 22, 2015) [hereinafter Lackey, *Understanding*], https://advance.lexis.com/document?crid=9f2e7739-241a-443b-9461-21cbc092a0b3&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5DC1-XPM1-JSRM-64V7-00000-00&pdcontentcomponentid=126170&pdmfid=1000516&pdisurlapi=true.

19. Gnadinger, *supra* note 12, at 419.

20. *See* Lackey, *Understanding*, *supra* note 18.

21. Michael E. Lackey, *Navigating the Stored Communications Act*, LEXIS ADVANCE RES. (June 22, 2015) [hereinafter Lackey, *Navigating*], https://advance.lexis.com/open/document/lpadocument/?pdmfid=1000522&crid=6f9015c5-2775-4b10-9c8d-f38dfd38eb3e&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5DC1-XPM1-JSRM-64V6-00000-00&pdcomponentid=126170&ecomp=5rbg&earg=1%3A7&prid=b286f274-3656-4039-84fc-f3cb9c4ec686.

22. 18 U.S.C. § 2702(a)(1) (Supp. III 2015).

23. Lackey, *Navigating*, *supra* note 21.

24. 18 U.S.C. § 2707 (2012); *see also* Lackey, *Navigating*, *supra* note 21.

25. 18 U.S.C. § 2520(a) (2012); *see also* Lackey, *Understanding*, *supra* note 18.

26. 18 U.S.C. § 2510(4) (2012) (defining "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the

a communication is intercepted can be difficult, and courts have struggled drawing lines.[27] For example, electronic communications retrieved from storage are not intercepted under the Wiretap Act, but electronic communications acquired during transmission are.[28] There are also a number of exceptions to the Act, such as when one party consents to interception of the communication.[29]

B. *Wireless Communications and Public Safety Act*

Though the legislature has made efforts to broaden the protection of electronic privacy through the ECPA,[30] other federal laws have weakened the protection of consumer electronic privacy. Under the Wireless Communications and Public Safety Act of 1999, all mobile devices created after 2000 were required to have the capability to map a user's address for use in emergency situations.[31] The benefit of this Act is indisputable: 911 operators are given the ability to locate callers in distress via global positioning systems.[32] However, the concerns for consumer privacy cannot be ignored. Since the implementation of this law, mobile telephone users can be located at any time, and with that comes the potential for abuse of the technology.[33]

III. THE TENSION BETWEEN NEW TECHNOLOGY AND PRIVACY

With new technological advances comes an important question: should people be willing to give up their privacy in exchange for the convenience that this technology brings? New technology brings instant access to information, and this must be weighed against what people are sacrificing in privacy.[34] While some might find the tradeoff worthwhile or accept the

use of any electronic, mechanical, or other device"); *see also* Lackey, *Understanding*, *supra* note 18.

27. *See* Lackey, *Understanding*, *supra* note 18.

28. O'Brien v. O'Brien, 899 So. 2d 1133, 1136 (Fla. Dist. Ct. App. 2005).

29. *See* Lackey, *Understanding*, *supra* note 18.

30. *See* Gnadinger, *supra* note 12, at 419.

31. Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286.

32. *Existing Federal Privacy Laws*, CDT (Nov. 30, 2008), https://cdt.org/insight/existing-federal-privacy-laws/ (explaining the Wireless Communication and Public Safety Act of 1999).

33. *See id.*

34. *See* Joel Stein, *Data Mining: How Companies Now Know Everything About You*, TIME (Mar. 10, 2011), http://content.time.com/time/magazine/article/0,9171,2058205-1,00.html (discussing the extensive invasion of privacy many companies conduct).

diminution of their privacy as inevitable, others may not.[35]

Most Americans know very little about what personal information is being collected, how it is being used, or what they can do to stop it.[36] In an investigation about data mining, *Time Magazine* author Joel Stein provided his name and email address to Reputation.com, an online reputation management company.[37] Within a few hours, the company called him back and read him his social security number.[38] Companies have unprecedented access to consumer data and though it may serve useful purposes, misuse of it could lead to dangerous results.[39]

A. *The Pros: New Technology*

Without doubt, there are countless benefits to new technology. It is difficult to imagine life today without a cell phone or its applications. Services like Google Maps provide useful location-based information, and in effect have obsoleted the need for paper maps. Computer databases have vastly increased the ability to collect, store, and analyze information,[40] and even the collection of data as applied to more individualized and useful online advertising brings some benefit.[41]

An interesting new technology that is likely to have a profound impact on privacy laws is the commercial use of drones.[42] Already, farmers are using drones to monitor fields, photographers are using them to capture spectacular views, law enforcement is using them for surveillance, and others are predicting that they will replace today's ground package delivery.[43] Although there are state laws, paparazzi laws, and limited court rulings, federal legislation does not yet address the privacy concerns associated with

35. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

36. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2 (2004).

37. Stein, *supra* note 34.

38. *Id.*

39. *See id.*; *see also infra* Part IV.

40. SOLOVE, *supra* note 36, at 1.

41. Stein, *supra* note 34.

42. *See The Future of Drones: Technology vs. Privacy*, 60 MINUTES (Mar. 14, 2014), http://www.cbsnews.com/news/the-future-of-drones-technology-vs-privacy/.

43. *Id.*

this technology.[44]

> In not so many years from now many of our homes will be run on the "internet of things." Your refrigerator, HVAC Unit, washer and dryer, lighting, TV and almost every other appliance in your home will be run by machines connected to the internet. Your car will drive itself and will be connected to the internet, if it isn't already. All of your information will [] be stored in the cloud including your medical information, bank information and multimedia. Every piece of information about you will technically be provided to a third party to run your everyday life.[45]

In the digital age, technology changes so rapidly that it is difficult to imagine what will come out tomorrow, next year, or in the next decade.[46] And once we have access to these new technologies, it is difficult to remember how we ever lived without them.

B. *The Cons: Giving Up Privacy*

"You know how everything has seemed free for the past few years? It wasn't. It's just that no one told you that instead of using money, you were paying with your personal information."[47] Access to free websites and mobile applications can feel unlimited, but users often do not consider what they are giving up in exchange for that access.[48] Mobile applications often have access to location information, photos, contacts, messages, and other personal information.[49] In a concurring opinion written by Justice Sotomayor, the U.S. Supreme Court acknowledged that Americans have "no reasonable expectation of privacy in information voluntarily disclosed to third parties."[50] The disclosure of this information enables third parties to

---

44. Michael Frank, *Drone Privacy: Is Anyone in Charge?*, CONSUMER REP. (Feb. 10, 2016), http://www.consumerreports.org/electronics/drone-privacy-is-anyone-in-charge/.

45. Bradley Henry, *Third-Party Doctrine: What Is It and Why Does It Matter?*, HENRY L. (June 21, 2016), http://www.henrylawny.com/third-party-doctrine-matter/.

46. Rengel, *supra* note 4, at 184 ("The last generation has seen technological change on a scale matching or exceeding that of the industrial revolution.").

47. Stein, *supra* note 34.

48. *See id.*

49. Suzanne Choney, *'Apps Act' Would Make Privacy Disclosures Mandatory*, NBC NEWS (May 10, 2013), http://www.nbcnews.com/technology/apps-act-would-make-privacy-disclosures-mandatory-1C9870952.

50. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers;

ascertain personal information about Americans such as political beliefs, religious beliefs, sexual habits, and much more.[51]

More specifically, the privacy invasion from location-based data collected from mobile devices should not be taken lightly. In 2014, half of top mobile applications were found to be collecting or sharing users' location information without their affirmative consent.[52] The aggregation of location data from mobile applications can easily reveal a user's home address, place of employment, place of worship, the school the user's children attend, and other sensitive information.[53] The frightening part is, under the ECPA, the companies that collect this information have almost no restrictions on who they can give or sell it to.[54]

Younger generations that have grown up with these technologies have a much different perception of privacy than older generations.[55] They expect that everything they do online can be seen by the government, schools, employers, and more.[56] The expectation is that there is no privacy, and the assumption is that they are always being observed.[57] This is a very different mindset than older generations where people expected that they were "private by default and public by effort," as opposed to today's world where we are "public by default and private by effort."[58] The expectation we once had for privacy is disappearing quickly—91 percent of U.S. adults surveyed in a study on privacy perceptions say "that consumers have lost control over how personal information is collected and used by companies."[59]

---

the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.").

51. *See id.* at 416.

52. Al Franken, *The Location Privacy Protection Act of 2014—Summary*, CONGRESS.GOV, https://www.congress.gov/bill/113th-congress/senate-bill/2171 (last visited Feb. 26, 2018).

53. *Id.*

54. *Id.* (arguing that this legal loophole is "misused by popular companies" and "abused by stalkers").

55. *See* Stein, *supra* note 34.

56. *See id.*

57. *Id.* (statement of Sherry Turkle) (finding that although young people do not have an expectation for privacy, they "live with this underlying anxiety of not knowing the rules of who can look at their information on the Internet.").

58. *Id.*

59. *Privacy Perceptions*, PEW RES. CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/privacy-perceptions/.

C. *The Effectiveness of Current Privacy Laws*

"Silicon Valley races every day to create flashy new products and anticipate the next wave of consumer demand. But when it comes to technology laws, Washington is stuck in the days of dial-up."[60] The virtually free exchange of our personal information between third parties is a clear indication that the ECPA is not effective at regulating newer technologies.[61] In today's rapidly changing digital world, the legislature is the best place to successfully balance the technological and privacy interests at stake.[62] Public attitudes towards technology and privacy are changing, and detailed lines must be drawn in order for the courts to consistently and predictably rule on privacy issues.[63] The difficulty in applying 30-year-old legislation to technologies that were not in existence when the legislation was drafted has led to conflict among lower courts.[64] The federal government has yet to resolve this issue, although states have enacted their own laws related to personal location privacy.[65]

In an effort to address the privacy issues, the Federal Trade Commission (FTC) has brought charges against application developers that use deceptive or unfair practices to intrude on consumer privacy.[66] Though the FTC does not specifically cover protection of consumer privacy, it has the power to bring actions for unfair or deceptive practices.[67] For example, in 2014, the FTC brought a claim against Snapchat, Inc., for its popular

60. Alex Byers, *Disconnect: Old Laws vs. New Tech*, POLITICO (Oct. 21, 2014), http://www.politico.com/story/2014/10/washington-dc-technology-112091.

61. *See* Franken, *supra* note 52.

62. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring) ("A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."); *see also* Rengel, *supra* note 4, at 180 (arguing that legislators need to be knowledgeable about the technology they are legislating in order for laws to be effective).

63. *See Jones*, 565 U.S. at 429–30.

64. *See GPS Location Privacy*, GPS.GOV, http://www.gps.gov/policy/privacy/ (last visited Feb. 23, 2017).

65. *Id.*; *see, e.g.*, CALIF. BUS. & PROF. CODE §§ 22575–22579 (West 2017); MINN. STAT. ANN. §§ 325M.01–325M.09 (West 2017); *see also State Laws Related to Internet Privacy*, NAT'L CONF. ST. LEGISLATURES (June 20, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

66. FTC, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 4 (2013), http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

67. *Id.*

mobile application, Snapchat.[68] In its complaint, the FTC alleged that Snapchat marketed its application for sending disappearing picture and video messages, claiming there was no way to view an image after the time expired.[69] In reality, there existed several methods for saving the messages using tools outside of the application.[70] Snapchat also tracked location information contrary to its privacy policy, collected information from users' contacts, and did not reasonably secure personal information.[71] The FTC subsequently brought six claims for false and misleading representation.[72] As a result of the action, Snapchat entered into a consent decree to reform its privacy practices in the future.[73]

In addition to bringing charges against application developers, in May 2012, the FTC held a public workshop relating to privacy issues with digital devices and in February 2013 released a follow-up report focused on mobile privacy disclosures.[74] The information released is not law, but it provides guidelines where law is lacking.[75] The 2013 report emphasizes transparency in what data is collected and how it is used, and it provides recommendations for platforms, app developers, advertising networks and other third parties, and app trade associations.[76] The FTC recommends that companies collecting consumer data provide clear disclosures and receive affirmative consent prior to collection of data, include a "Do Not Track" mechanism to allow consumers to opt out, and work to educate consumers about how collected data is used.[77]

IV. WHAT IS THE IMPACT ON AMERICANS?

With all of this personal information being freely exchanged between third parties, the question remains whether there is an actual harm to the

68. *In re* Snapchat, Inc., No. 132-3078, 2014 WL 1993567, at *1 (F.T.C. May 8, 2014).

69. *Id.*

70. *Id.* at *2.

71. *Id.* at *3–6.

72. *Id.*

73. *See id.* at *9–14 (requiring Snapchat, Inc. to comply with the order for a period of 20 years).

74. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

75. *Id.* at 29.

76. *See Id.* at 1.

77. Lesley Fair, *5 Top-Level Takeaways from the FTC Staff Report on Mobile Privacy Disclosures*, FTC (Feb. 6, 2013), https://www.ftc.gov/news-events/blogs/business-blog/2013/02/5-top-level-takeaways-ftc-staff-report-mobile-privacy.

American people. Though some would argue that the actual impact is very low and regulation on technology development would be burdensome and discourage innovation,[78] some startling statistics suggest otherwise.[79] In a study of 20 social networking sites by AT&T, all but one were found to be sharing information with third parties that would allow these parties to associate the information shared with individual identities.[80] In 2014, at least 25,000 people were victims of GPS stalking—a result of the many stalking-related mobile apps that are easily available online.[81] GPS and cyberstalking provide astonishingly easy access for abusers to locate victims and contribute to domestic violence being the number one cause of injury to women between ages 15 and 44.[82]

A. *Is There Actually Harm?*

We know mobile applications and online companies have access to sensitive personal information, and data mining companies aggregate this information and sell it to third parties. But should we care? Chairman of U.S. tech firm Rethink Robotics discussed Google Maps' ability to guess, usually correctly, where an individual wants to go.[83] He said, "At first, I found that spooky and kind of scary. Then I realised, actually, it's kind of useful."[84] The fact that this type of information can then be sold to data mining companies can be frightening. However, after considering what these companies generally do with the data, it is a little less worrisome.

Russell Glass, CEO of Bizo, a data mining company, said, "People are afraid of what they really don't understand. They don't understand that companies like us have no idea who they are. And we really don't give a s—-. I just want a little information that will help me sell you an ad."[85] In reality, most people are not even aware when and what data is being collected from

78. *See* Stein, *supra* note 34.

79. *See* Franken, *supra* note 52.

80. Balachander Krishnamurthy & Craig E. Wills, *Privacy Leakage in Mobile Online Social Networks*, http://web.cs.wpi.edu/~cew/papers/wosn10.pdf (last visited Feb. 23, 2017) (finding all mobile online social networks studied exhibited "some leakage of private information to third parties").

81. Franken, *supra* note 52.

82. Alexis A. Moore, *Cyberstalking and Women – Facts and Statistics*, THOUGHTCO. (June 12, 2014), http://womensissues.about.com/od/violenceagainstwomen/a/CyberstalkingFS.htm.

83. Agence France-Presse, *Privacy Is Dead, Invasive Technology Is Here to Stay*, INDUSTRY WK. (Jan. 22, 2015), http://www.industryweek.com/technology/privacy-dead-invasive-technology-here-stay?page=2.

84. *Id.*

85. Stein, *supra* note 34.

their mobile applications or that it is being shared with third parties.[86] If people do not even know that the data collection is occurring, some may argue there is no harm done. Additionally, there are options to block or opt out of data-mining activities via web browsers such as Google Chrome or Firefox.[87]

Another perspective is that technology does not diminish privacy, but enhances it.[88] For example, the ability to encrypt data allows people to keep sensitive information private, and computer software allows citizens in repressed countries to browse the Internet anonymously in order to access uncensored information.[89] Rather than viewing technology as an inevitable diminution to our privacy, people should expect privacy to be built into our technology.[90]

Though the collection of personal information may sound harmless when applied to a data-mining company selling advertisements, the reality is that data collection is occurring in far more ways than just that. The potential for misuse of personal information comes with extreme risks.[91] These risks include being located by someone you do not want to find you, being stalked, or having personal information revealed through a data breach.[92]

B. *Hidden Spyware Apps*

One of the most alarming invasions of privacy via new technology is the creation and use of hidden spyware apps. Spyware apps can be installed and hidden on a person's phone in such a way that it is unlikely the victim would ever be aware of their presence.[93] The amount of information these apps collect is disturbing. Spyware apps, such as FlexiSPY, have the capability to turn on a phone's microphone and listen to the surroundings, listen to phone calls, view text messages, track location, take pictures through the phone's camera, capture passwords, view web history, receive

86. *See* Gnadinger, *supra* note 12, at 436.

87. Stein, *supra* note 34.

88. *See* Hanni M. Fakhoury, *Privacy and Technology Can, and Should, Co-Exist*, N.Y. TIMES (Dec. 12, 2012), http://www.nytimes.com/roomfordebate/2012/12/11/privacy-and-the-apps-you-download/privacy-and-technology-can-and-should-co-exist.

89. *Id.*

90. *Id.*

91. *See* Daniel Pieringer, Note, *There's No App for That: Protecting Users from Mobile Service Providers and Developers of Location-Based Applications*, 2012 U. ILL. J.L. TECH. & POL'Y 559, 564 (2012).

92. *See id.*

93. *See* Gross, *supra* note 8.

location alerts, and far more.[94] Naturally, installation of these apps has led to an increase in stalking and domestic abuse.[95] Though there are criminal laws that can be used to prosecute stalkers,[96] privacy laws have not caught up with the technology, and development and sale of these apps is not clearly illegal.[97] App developers protect themselves from liability by using a disclaimer that states, "use of the apps for 'illegal purposes' is prohibited."[98] Thus, companies making money by enabling cyberstalking continue to walk free without criminal or civil liability.[99]

Spyware apps and cyberstalking are so prevalent that they are now a standard tool used by domestic abusers in our country.[100] In turn, the personal information that can be obtained through GPS features in smartphones has had a profound effect on domestic violence shelters.[101] Often when victims are admitted into a shelter, there is a "digital detox" at the door: they must shut off GPS and Wi-Fi on their phones and avoid Facebook, which can provide pinpoint locations.[102] Out of 70 domestic violence shelters surveyed by National Public Radio (a news organization) an astonishing 85 percent said they were working with victims who had been tracked by their abusers using GPS, and 75 percent were working with victims who had been cyberstalked via hidden mobile apps.[103] Surveillance through spyware apps gives abusers a new level of control over their victims.[104] The invasion of privacy is so extreme that stalkers may even listen in on a victim's private conversation with a therapist or trusted friend.[105]

---

94. *Spy on Any Android Phone with Our Unique Android Monitoring App*, FLEXISPY, http://www.flexispy.com/en/android-spy-app-flexispy.htm (last Feb. 26, 2018) (advertising FlexiSPY as an application that "take[s] total control of an Android mobile phone or tablet and sp[ies] on all its communications and activities from any computer with a web browser").

95. Gross, *supra* note 8.

96. *See, e.g.*, IOWA CODE ANN. § 708.11 (West 2017).

97. *See* Gross, *supra* note 8.

98. Jeremy Seth Davis, *Franken Re-Introduces Bill to Ban "Cyber-Stalking Apps"*, SC MEDIA (Nov. 12, 2015), http://www.scmagazine.com/franken-re-introduces-bill-to-ban-cyber-stalking-apps/article/453624/.

99. *See* Gross, *supra* note 8.

100. Aarti Shahani, *Smartphones are Used to Stalk, Control Domestic Abuse Victims*, NPR (Sept. 15, 2014), http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

101. *Id.*

102. *Id.*

103. *Id.*

104. *See id.*

105. *See id.* ("'The strategy of offenders is to have complete and utter domination and control of their victims,' [Cindy Southworth, an advocate with the National Network

Of course, these mobile spyware apps are not being marketed as tools to enable cyberstalking and domestic abuse.[106] Creators market their apps as a means for parents to monitor children who are "sexting," bullying, or for employers to monitor their employees.[107] They advertise the apps as a legal way to watch children or employees when they have full knowledge of the app's existence.[108]

C. *Cybersecurity and Data Breaches: The Ashley Madison Scandal*

Essentially every business collects and stores customers' information, whether it be credit card information, home addresses, or other personal information. When this information is compromised, there can be devastating results for those whose information is breached. This was true for 32 million members of the adultery website Ashley Madison,[109] which resulted in at least two suicides and numerous lawsuits.[110]

Ashley Madison is a website offering married individuals the opportunity to have an affair through an "anonymous" membership.[111] The company retained private customer information including: "first and last names, email addresses, street addresses . . . , GPS location, login information, and partial credit card payment information[,]" which was compromised in a major data hack in August of 2015.[112] Naturally, members whose personal information was released may experience potentially serious impacts on their personal, professional, and financial lives.[113] Though email addresses are not confirmed, the hack has revealed potential affairs by

---

to End Domestic Violence,] says. 'And so it's not enough that they just monitor the victim. They will then taunt them or challenge them and say, "Why were you telling your therapist this? Or why did you tell your sister that? Or why did you go to the mall today when I told you couldn't leave the house?"'").

106. *Id.*

107. *Id.*

108. *Id.*

109. *See* Girard Kelly, *Ashley Madison's Data Breach Notification Exposed*, GIRARD KELLY (Aug. 25, 2015), https://web.archive.org/web/20161203010011/http://www.girardkellylaw.com/privacy-and-cybersecurity/ashley-madisons-data-breach-notification-exposed/.

110. Assoc. Press, *Two Suicides Linked to Ashley Madison Leak*, N.Y. POST (Aug. 24, 2015), http://nypost.com/2015/08/24/two-suicides-linked-to-ashley-madison-leak/ (reporting not only two unconfirmed suicides, but also rumors of hate crimes connected with the leak).

111. Kelly, *supra* note 109.

112. *Id.*

113. John Herrman, *Early Notes on the Ashley Madison Hack*, THE AWL (Aug. 18, 2015), https://www.theawl.com/2015/08/early-notes-on-the-ashley-madison-hack/.

politicians, teachers, government workers, and more.[114]

Time will tell what impact this data hack—one that received massive amounts of media attention—will have on cybersecurity and privacy laws, but one Washington Post writer has already called it the "Pandora's box" of Internet privacy cases.[115] Another author observed the impact on Internet privacy with the tagline, "Welcome to the first day of the rest of your internet."[116] To many, this hack revealed much more than millions of people cheating on their spouses—it revealed that privacy online should never be taken for granted.[117]

V. RECOMMENDATION FOR LEGISLATIVE CHANGE

Unlike mobile applications, privacy law does not auto-update. The governing federal law should not be older than the Internet, and Americans should be able to enjoy both new technology and protection of their privacy.[118] States have begun enacting their own legislation, but this can be counterproductive given that online privacy is a national or international issue.[119] Though there have been a number of proposed bills, nothing has yet passed through Congress, and each of the four bills addressed in this Note has not made it past committee.[120] A number of the proposed bills have an

114. *See id.*

115. *See* Michael E. Miller, *Don't Gloat About the Ashley Madison Leak. It's About Way More than Infidelity.*, WASH. POST (Aug. 19, 2015), https://www.washingtonpost.com/news/morning-mix/wp/2015/08/19/dont-gloat-about-the-ashley-madison-leak-its-about-way-more-than-infidelity/.

116. *See* Herrman, *supra* note 113 (concluding his notes on the hack with, "Welcome to the future, I guess!").

117. Miller, *supra* note 115 ("The Ashley Madison leak is about a lot more than the public shaming of philanderers. Above all, it's about Internet privacy.").

118. *See* Jasmine McNealy & Angelyn Flowers, *Privacy Law and Regulation: Technologies, Implications, and Solutions*, *in* PRIVACY IN A DIGITAL, NETWORKED WORLD: TECHNOLOGIES, IMPLICATIONS AND SOLUTIONS 189, 203 (Sheraldi Zeadally & Mohamed Badra eds., 2015) ("It may be inevitable that as technology expands so too does its insidious creep into the private spaces of our lives. But there has to be an approach to maintaining some semblance of personal privacy without opting out of the benefits of the digital world.").

119. Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, N.Y. TIMES (Oct. 30, 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html?_r=0.

120. *See* Geolocation Privacy and Surveillance Act, H.R. 491, 114th Cong. (2015); Location Privacy Protection Act of 2015, S. 2270, 114th Cong. (2015); Application Privacy, Protection, and Security Act of 2013, H.R. 1913, 113th Cong. (2013); Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013). Once a bill is introduced in committee, it must pass in both the House and the Senate and be signed by the President before it becomes law. *See generally* CONGRESS.GOV,

impact on the government, and one reason they have not pushed forward is a fear the legislation will hamper law enforcement and threaten public safety.[121] Additionally, the bills regulating private parties have received pushback from industry due to the stifling impact on innovation.[122]

A. *Location Privacy Protection Act*

The first bill this Note will discuss is Senator Al Franken's Location Privacy Protection Act, reintroduced in November 2015.[123] This bill was drafted in a response to mobile stalking apps as an attempt to help victims of cyberstalking and domestic abuse.[124] Franken, author of the bill, said: "I believe that Americans have the right to control who can collect their location, and whether or not it can be given to third parties. But right now, companies—some legitimate, some not—are collecting your location and giving it to whomever they want."[125] The key aspects of this bill would "[b]an the development, operation, and sale of GPS stalking apps[;]" require affirmative consent before a company collects location data or shares it with others; and allow for private lawsuits against app makers.[126]

Although the bill has received praise, it has not come without criticism

https://www.congress.gov/search?q={"source":"legislation"} (last visited Feb. 23, 2017) (noting a "tracker" under each proposed bill, which shows the bill must pass the House, Senate, and President before becoming law).

121. *See* Brendan Sasso, *Most House Members Want to End Email Spying. Why Hasn't Their Bill Moved?*, GOV'T EXECUTIVE (Dec. 2, 2015), http://www.govexec.com/oversight/2015/12/most-house-members-want-end-email-spying-why-hasnt-their-bill-moved/124118/.

122. *See* Gross, *supra* note 8.

123. Location Privacy Protection Act of 2015, S. 2270, 114th Cong. (2015); *Sen. Franken Reignites Efforts to End Stalking Apps Once and for All,* AL FRANKEN U.S. SENATOR FOR MINN. (Mar. 27, 2014), https://web.archive.org/web/20140327235609/http://www.franken.senate.gov/?p=press_release&id=2755 [hereinafter, *Sen. Franken Reignites Efforts*].

124. Sam Brodey, *Your Apps Know Where You Are, But Do You Know Who They're Sharing That Information With?*, MINNPOST (Nov. 13, 2015), https://www.minnpost.com/dc-dispatches/2015/11/your-apps-know-where-you-are-do-you-know-who-they-re-sharing-information ("Franken, who is the top Democrat on the Senate Judiciary Subcommittee for Privacy, Technology, and the Law, said the genesis of his law was testimony from the Minnesota Coalition for Battered Women, which told the story of a St. Louis County woman whose abusive partner used stalking software to discover she was seeking a restraining order."); *Sen. Franken Reignites Efforts*, *supra* note 123.

125. *Sen. Franken Reignites Efforts*, *supra* note 123.

126. Location Privacy Protection Act; *Sen. Franken Reignites Efforts*, *supra* note 123.

as well.[127] One critique the bill has received is its breadth.[128] Critics argue the Location Privacy Protection Act is overbroad and it should be more focused on cyberstalking, not limiting commercial use of geolocation data.[129] A serious issue with the bill, some believe, is its interference with legitimate tracking applications, which would potentially require changes in mobile operating systems.[130] The bill has received clear opposition from the U.S. Chamber of Commerce, which argues that "existing self-regulatory programs and user-friendly technological solutions" are sufficient, and legislation is not necessary.[131] Consumers today enjoy many free digital services due to the sale of their personal information and resulting advertisements—this bill may greatly impact this process and could put access to this free technology in jeopardy.[132] Additionally, app developers have a disincentive to innovate due to the risk of private lawsuits.[133]

B. *Online Communications and Geolocation Protection Act*

A second bill that proposed to modernize the ECPA of 1986 and strengthen privacy protections is the Online Communications and Geolocation Protection Act introduced by California Congresswoman Zoe Lofgren, Texas Congressman Ted Poe, and Washington Congresswoman Suzan DelBene.[134] The bill is broader in scope than the Location Privacy Protection Act in that it attempts to reform the ECPA and federal privacy law in general, rather than focus on location tracking technology and mobile stalking apps.[135] It also differs from Senator Franken's bill in that it focuses

127. *See* Gross, *supra* note 8.

128. *Id.*

129. *Id.*

130. *See* Ernie Smith, *Ad Group: Privacy Bill Could Target More than 'Stalker Apps'*, ASSOCIATIONS NOW (June 9, 2014), http://associationsnow.com/2014/06/ad-group-privacy-bill-target-stalker-apps/.

131. *Hill Letter Opposing S. 2171, The Location Privacy Protection Act*, U.S. CHAMBER COM. (June 11, 2014), https://www.uschamber.com/letter/hill-letter-opposing-s-2171-location-privacy-protection-act.

132. *See* Smith, *supra* note 130.

133. Gross, *supra* note 8 (statement of Robert Atkinson) ("Many small app developers, 'if they were faced with the potential of a $1 million fine for making a small coding mistake, or putting something inaccurate on a website, I believe would think twice about developing a mobile app.'").

134. Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013); *Reps. Zoe Lofgren Introduces Bipartisan ECPA Reform Bill*, CONGRESSWOMAN ZOE LOFGREN (Mar. 6, 2013), https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=365633.

135. *See Reps. Zoe Lofgren Introduces Bipartisan ECPA Reform Bill*, *supra* note 134.

on protection from government access, rather than private parties.[136] In introducing the bill, Congresswoman DelBene said:

> In the past decade, advances in technology and the Internet have dramatically changed the way we communicate, live and work. In this constantly evolving world, Congress must be a good steward of policy to ensure our laws keep up. When current law affords more protections for a letter in a filing cabinet than an email on a server, it's clear our policies are outdated.[137]

As the ECPA exists today, a warrant is not clearly required in order for law enforcement to access online communication.[138] Instead, online content more than 180 days old can be seized with a mere subpoena.[139] The focus of this bill is to apply the Fourth Amendment's constitutional privacy guarantees to location data and digital communications.[140] To do this, the bill would require issuance of a warrant before the government can obtain location data or intercept or seize digital communications.[141]

Among those who oppose the bill are the U.S. Department of Justice and law enforcement agencies.[142] Government agencies fear the requirement of a warrant will be burdensome on law enforcement and will make it more difficult to prosecute criminals.[143]

C. *Geolocation Privacy and Surveillance Act*

The third bill this Note will analyze is the Geolocation Privacy and Surveillance Act (the GPS Act).[144] Like the Online Communications and

136. *See id.*

137. *Lawmakers Introduce Bipartisan Privacy Reform Legislation*, CONGRESSWOMAN ZOE LOFGREN (Feb. 2, 2015), https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=365633.

138. *Id.*

139. *Id.*

140. Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2014); *Reps. Zoe Lofgren Introduces Bipartisan ECPA Reform Bill*, *supra* note 134.

141. *See* sources cited *supra* note 134.

142. Ronald Bailey, *Warrants for Emails and Cell Phone Locations: Online Communications and Geolocation Protection Act*, REASON.COM (Feb. 2, 2015), http://reason.com/blog/2015/02/02/warrants-for-emails-and-cell-phone-locat; Zack Whittaker, *Justice Dept. to Congress: We Want Greater Email, Facebook, Twitter Snooping Powers*, ZD NET (Mar. 19, 2013), http://www.zdnet.com/article/justice-dept-to-congress-we-want-greater-email-facebook-twitter-snooping-powers/.

143. Whittaker, *supra* note 142.

144. Geolocation Privacy and Surveillance Act, H.R. 491, 114th Cong. (2015).

Geolocation Protection Act, this bill is the result of bipartisan efforts to establish "clear rules governing how law enforcement, commercial entities and private citizens can access, use and sell [location] data."[145] However, the Acts differ in that the GPS Act regulates both law enforcement and private parties, rather than just the government.[146] The GPS Act is modeled after the federal wiretapping statutes and establishes both a process where government agencies can get a warrant for location information, as well as "guidelines for when and how geolocation information can be accessed and used."[147] In regards to the regulation of private parties, businesses are prohibited from disclosing geographical tracking data about its customers to third parties without the customer's permission.[148]

This bill has similar drawbacks to the Location Privacy and Protection Act and the Online Communications and Geolocation Protection Act as it encompasses parts of each of them. Additionally, there is fear that the Act would encourage a flood of class action lawsuits due to the unclear scope of geolocation information, which arguably includes IP addresses, as well as the unspecific degree of consent required from consumers.[149] The bill was reintroduced in Congress on July 27, 2017 and with the increased public scrutiny on personal privacy, the bill is likely to receive attention from many.[150]

D. *Application Privacy, Protection, and Security Act*

Finally, a bill cleverly called the APPS Act (Application Privacy, Protection and Security Act) was drafted in order to specifically regulate mobile applications, an area that has yet to receive direct regulation from the federal government.[151] This bill was written in an effort to balance the protection of consumer privacy and the functionality of mobile

145. *See GPS Act*, RON WYDEN SENATOR FOR OR., https://www.wyden.senate.gov/priorities/gps-act (last visited Feb. 23, 2017).

146. *See id.*

147. *Id.*

148. *Id.*

149. *The Next Privacy Frontier: Geolocation*, IAPP (June 3, 2013), https://iapp.org/news/a/the-next-privacy-frontier-geolocation ("[T]he bill defines 'geolocation information' as information derived from a device that is not the content of a communication and 'could be used to determine or infer information regarding the location of the person.'").

150. *See* Morgan, Lewis & Bockius LLP, *Geolocation Privacy and Surveillance Act Introduced in US Congress*, NAT'L L. REV. (Feb. 23, 2017), http://www.natlawreview.com/article/geolocation-privacy-and-surveillance-act-introduced-us-congress.

151. Application Privacy, Protection, and Security Act of 2013, H.R. 1913, 113th Cong. (2013); *see also* Gnadinger, *supra* note 12, at 417.

applications.[152] The essence of the APPS Act is the requirement of a notice to consumers that private information is being collected about them.[153] After being informed of the information collected, consumers are given the right to withdraw consent and disallow collection of this information.[154]

With nearly two-thirds of the U.S. population owning smartphones, mobile applications are extremely prevalent,[155] and some sort of federal regulation is necessary. However, the APPS Act is not without its criticisms. The Act encompasses mobile applications, platforms, advertisers, and third parties, and it is difficult to draft a bill that effectively regulates every party that is impacted.[156] Additionally, although a consumer privacy notice is a nice idea in theory, in reality, few consumers actually read these notices, and even fewer comprehend them.[157]

E. *Legislation Recommendation*

The four legislative solutions proposed above all address important privacy concerns for Americans today and range in their breadth. Though the Online Communications and Geolocation Protection Act tackles an important issue of modernizing the ECPA, it focuses on raising the standard for the government to access geolocation data and online communications.[158] It does not directly address private parties,[159] and thus does not solve the issues discussed in this Note.

Additionally, the APPS Act is advantageous in that it is focused on mobile applications, but the notice to consumers is not likely to be an effective solution to the privacy concerns addressed in this Note.[160] It seems almost everything we do contains some sort of disclosure filled with legalese that few outside of the legal profession would understand. The APPS Act's

152. *See* Application Privacy, Protection, and Security Act; *see also* Gnadinger, *supra* note 12, at 418.

153. *See* Application Privacy, Protection, and Security Act; *see also* Gnadinger, *supra* note 12, at 425.

154. *See* Application Privacy, Protection, and Security Act; *see also* Gnadinger, *supra* note 12, at 437.

155. Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

156. *See* Gnadinger, *supra* note 12, at 438.

157. *Id.*

158. *See* Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013); *Reps. Zoe Lofgren Introduces Bipartisan ECPA Reform Bill*, *supra* note 134.

159. *See* Online Communications and Geolocation Protection Act.

160. *See* Application Privacy, Protection, and Security Act of 2013, H.R. 1913, 113th Cong. (2013); Gnadinger, *supra* note 12, at 418.

requirement for notice of the scope of data collection is unlikely to have a profound impact on how consumers share personal information because consumers are unlikely to read a notice and take affirmative steps to withdraw consent.[161]

The Location Privacy Protection Act and the GPS Act both focus on the collection and sharing of location information, with the GPS Act being the broader of the two, encompassing government activity in addition to that of private parties.[162] Because the Location Privacy Protection Act is more specific, it is likely to receive less opposition than the GPS Act. The Location Privacy Protection Act focuses on private parties and does not include government regulation like the GPS Act, which encompasses both and therefore has opponents both in the technology industry and law enforcement.[163] The Location Privacy Protection Act therefore will be more likely to pass through Congress and will also best address the issues raised in this Note for several reasons.[164]

First, the Location Privacy Protection Act ensures that any company that collects and discloses location information cannot do so without the user's consent, aside from defined exceptions such as emergency services and law enforcement.[165] Second, it specifically addresses mobile spyware apps and clearly prohibits their development and distribution.[166] Though there are certainly many other privacy concerns, location information is very sensitive and the prohibition of apps that lead to increased cyberstalking and domestic abuse should be a priority with enacted legislation. Moreover, this bill's specific target on technology that assists violent criminals may give it a better chance of passing than other privacy bills.[167] Then-Senator Al Franken has introduced different versions of the bill to the 112th, 113th, and 114th Congress.[168]

---

161. *See* Gnadinger, *supra* note 12, at 438.

162. *See* Geolocation Privacy and Surveillance Act, H.R. 491, 114th Cong. (2015); Location Privacy Protection Act of 2015, S. 2270, 114th Cong. (2015); *GPS Act*, *supra* note 145; *Sen. Franken Reignites Efforts*, *supra* note 123.

163. *See* Geolocation Privacy and Surveillance Act.

164. *See* Location Privacy Protection Act.

165. *See id.*

166. *See id.*

167. Kate Kaye, *Location Privacy Bill Gets Another Push*, ADVERT. AGE (June 4, 2014), http://adage.com/article/datadriven-marketing/location-privacy-bill-push/293556/.

168. *See* Wendy Davis, *Franken Presses for Location Privacy Bill*, MEDIAPOST (Nov. 12, 2015), http://www.mediapost.com/publications/article/262474/franken-presses-for-location-privacy-bill.html; *Geolocation Privacy Legislation*, GPS.GOV, http://www.gps.gov/policy/legislation/gps-act/ (last visited Aug. 6, 2017).

VI. CONCLUSION

Though people may debate what the best solution is, one thing is clear: federal privacy law regulating digital communications is necessary. Research shows that the majority of Americans believe the government should be doing more to regulate private parties' use of their personal information.[169] The balance between protecting privacy and encouraging innovation is certainly a difficult one to achieve, but the nature of drafting legislation in any area always requires balancing competing interests. Cellphones, mobile applications, and location-tracking technology are undoubtedly a part of everyday life, and privacy laws should address the concerns that come with these technologies. The place for this update is the legislature, and the time is now.

*Olivia Kilgore**

169. *Privacy Perceptions*, *supra* note 59 ("Sixty-four [percent of consumers] believe the government should do more to regulate what advertisers do with customers' personal information . . . .").

* B.S., Iowa State University, 2012; J.D., Drake University Law School, 2017. Ms. Kilgore is the 2017 Recipient of the H.G. Cartwright Law Review Award. She currently is an Associate at Fredrikson & Byron, P.A.