Loyola of Los Angeles Law Review

Volume 50 | Number 4 Article 5

2017

Counteracting Diminished Privacy in an Augmented Reality: Protecting Geolocation Privacy

Diana Martinez
Loyola Law School, Los Angeles

Counteracting Diminished Privacy in an Augmented Reality: Protecting Geolocation Privacy

Cover Page Footnote

J.D. Candidate, May 2018, Loyola Law School, Los Angeles; B.A., Psychology, Neuroscience and Behavior (Music Cognition Specialization), McMaster University. I would like to thank Professor John Nockleby for his guidance, patience, and encouragement throughout the law review process. Most importantly, I would like to thank my parents, Don and Clemencia, for their unwavering love and support.

COUNTERACTING DIMINISHED PRIVACY IN AN AUGMENTED REALITY: PROTECTING GEOLOCATION PRIVACY

*Diana Martinez**

I. INTRODUCTION

Imagine you own a house on a quiet street in Maryland. Upon driving home from work one day, you notice a large group of strangers—children, teenagers, and adults alike—congregated at the park across the street. Upon further investigation, you notice a common pattern in behavior: each stranger walks around the park holding his or her smartphone and swipes upwards on the screen. Rather than ask the strangers about their motives, you leave them to their devices in hopes that this occurrence is an anomaly. This occurrence, however, becomes universal overnight. The next day, you see crowds of seemingly antisocial strangers exhibiting the same pattern of behavior everywhere: the grocery store, the fountain placed outside the museum, and even your neighbor's lawn. This unusual yet ubiquitous behavior is attributed to the mobile application game known as Pokémon Go.

Developed and created by Niantic, Inc., the object of the game is to collect virtual creatures by visiting locations in the real world, training creatures, and battling other players' creatures. By tracking the player's geolocation, the application provides a geographic view of nearby locations that are fertile for collecting and battling creatures.

The technology underlying Pokémon Go is augmented reality ("AR") and operates in three steps. An individual end user collects information about the physical world through an application on his or her device, such as a smartphone or tablet. Next, the application sends

* J.D. Candidate, May 2018, Loyola Law School, Los Angeles; B.A., Psychology, Neuroscience and Behavior (Music Cognition Specialization), McMaster University. I would like to thank Professor John Nockleby for his guidance, patience, and encouragement throughout the law review process. Most importantly, I would like to thank my parents, Don and Clemencia, for their unwavering love and support.

the information to a computer linked to the application's network, which modifies the information. The computer sends the modified information back to the end user and superimposes this information on the device as though it is inherently part of the physical world.[1]

Applying these steps to the first phase of Pokémon Go, first, a player enables the application to collect the smartphone's geolocation information from the physical world. The application then sends the geolocation information to a computer in Niantic, Inc.'s network to determine which virtual creatures are available for collection at nearby locations. Lastly, the computer sends this information back to the application and superimposes an image of the virtual creature on the user's screen as though it were part of the real world. Because gameplay is entirely based on the geolocation of the player's device, Niantic, Inc. necessarily collects, stores, and may disclose this information to third parties.[2] Therefore, the main privacy concern with Pokémon Go is Niantic, Inc.'s unregulated practices involving the player's geolocation information.[3]

In the United States, individuals are clearly protected from privacy intrusions by the government.[4] In contrast, end users may seek redress from non-government entities, such as technology corporations and mobile application developers, only under certain circumstances.[5] Currently, there is no federal or state legislation that expressly protects an end user's geolocation privacy from non-government entities. Because of this legislative gap, Niantic, Inc. may freely collect, store, and disclose a player's geolocation information for unspecified purposes without the end user's consent.

The Location Privacy Protection Act ("LPPA") is a federal bill that proposes to bridge this gap by prohibiting a non-government entity from collecting or disclosing an end user's geolocation information without consent. This Note critiques the proposed bill on

1. *See infra* Part II.A.

2. *Pokémon GO Privacy Policy*, NIANTIC, INC. 4–5, https://www.nianticlabs.com/privacy/pokemongo/en (last visited Dec. 21, 2016).

3. *See infra* Part II.B.2.

4. *See* United States v. Jones, 556 U.S. 400 (2012).

5. *See, e.g.*, CAL. BUS. & PROF. CODE §§ 22575–79 (2008) (privacy violations arise where non-government entities do not notify California residents that they collect or disclose information such as social security numbers, but not the resident's geolocation information); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 287–89 (3d Cir. 2016) (holding that there was no privacy violation under the Video Privacy Protection Act because an IP address does not personally identify the end user).

the basis that it fails to regulate non-government entities' storage practices, and recommends legislative amendments. Part II describes augmented reality, its application to Pokémon Go, and the surrounding data privacy concerns. Part III introduces the framework of data privacy law in the U.S. and highlights the difference in privacy actions against the government and non-government entities. Part IV focuses on the privacy issues associated with geolocation information and the governing federal statute. Part V interprets the relevant provisions from the proposed LPPA, identifies legislative gaps, and recommends appropriate amendments in light of privacy and policy concerns. Lastly, Part VI recapitulates the privacy issue posed by Pokémon Go, and the importance of the proposed Act and the recommended legislative amendments.

II. OVERVIEW OF THE PROBLEM

A. Augmented Reality

In today's world, completing mundane tasks often involves using a device, such as a computer or smartphone. For example, obtaining driving directions from the Google Maps website involves turning on the computer, logging in, opening the web browser, entering the Google Maps website, and typing in the respective address fields. Similarly, using the Google Maps smartphone application involves unlocking the smartphone, tapping the Google Maps icon, and typing in the address fields. In both scenarios, the device—the computer or the smartphone—acts as an intermediary between the end user and the information.

Augmented reality ("AR") eliminates the need for an intermediary device by merging information from the digital world with the user's device from the physical world.[6] For example, through the camera of the user's device, the IKEA application catalogue allows the user to view a potential piece of furniture (*e.g.*, a couch) superimposed in a desired room (*e.g.*, a living room),[7] thereby merging the furniture from the digital world with the actual room from the

6. *See* Andreas Kotsios, *Privacy in an Augmented Reality*, 23 INT'L J.L. & INFO. TECH. 157, 157–58 (2015).

7. Paul Ridden, *IKEA Catalog Uses Augmented Reality to Give a Virtual Preview of Furniture in a Room*, NEW ATLAS (Aug. 14, 2013), http://newatlas.com/ikea-augmented-reality-catalog-app/28703.

physical world. The ability to directly superimpose digital information on the physical world literally augments reality.[8]

The technology underlying AR is relatively simple. AR requires an application on a particular device[9] to gather information about the physical world.[10] This information is then relayed to a computer linked to the application's network, which then modifies the information and sends back to the application.[11] Using the modified information, the application projects the information on the device's camera as if it was "overlaid onto the real world."[12]

Because AR merges digital and physical information, this technology conveys information to the user much faster than an intermediary device, and is used subtly in a variety of contexts, including sports,[13] interior design,[14] and education.[15] AR has also been adopted in wearable head devices, such as Google Glass, which integrates information about a person or object viewed through the glasses themselves.[16] Most recently, AR has been applied to mobile applications.[17]

B. Pokémon Go

Perhaps AR's most controversial recent application is the mobile application game developed by Niantic, Inc. ("Niantic") known as Pokémon Go.[18] Before beginning gameplay, Niantic requires the player to take a number of steps.[19] Prospective players must sign up using a Gmail, Facebook, or Pokémon Trainer Club account.[20] After signing up, the player must agree to Niantic's Terms and Services,

8. Brian D. Wassom, *IP in an Augmented Reality*, 6 LANDSLIDE 8, 10 (2014).

9. Olivia Whitcroft, *Augmented Reality—a Leap into a New World*, 14 PRIVACY & DATA PROTECTION 7 (2013).

10. *Id.*

11. *Id.*

12. *Id.*

13. Piazza v. Kirkbride, 785 S.E.2d 695, 699 (N.C. Ct. App. 2016) ("the yellow first-down line that appears on screen during a televised football game.").

14. *See* Ridden, *supra* note 7.

15. *Anatomy Education Tools*, SOFT INTERACTION LAB (July 10, 2016), http://softinteraction.com/archives/1165.

16. *See* Kotsios, *supra* note 6.

17. *See, e.g.*, Brandon Widder, *The Twenty Best Augmented-Reality Apps*, DIGITAL TRENDS (Aug. 6, 2016, 10:00 AM), http://www.digitaltrends.com/mobile/best-augmented-reality-apps.

18. NIANTIC, INC., *supra* note 2, at 1.

19. *Id.* at 2.

20. *Id.* at 1–2.

including its privacy policy.[21] The relevant provision of the policy addresses Niantic's data collection, storage, and disclosure practices: Niantic collects geolocation information of the player's smartphone through "cell/mobile tower triangulation, wifi triangulation, and/or GPS."[22] Additionally, Niantic reserves the right in perpetuity to store[23] and disclose this information to third parties.[24]

A player can begin playing after signing up and accepting Niantic's Terms and Services. Gameplay occurs in three phases: (1) collect virtual creatures from locations in the real-world environment, (2) train creatures, and (3) battle another player's creatures.[25] As described below, AR technology permeates each stage of the game.

1. Gameplay

First, a player must collect or catch a virtual creature, known as a Pokémon.[26] To collect Pokémon, the player must visit locations in the real world environment, known as Pokéstops,[27] which are fertile for collecting Pokémon.[28] As the player navigates the real world, the underlying AR technology tracks the player's device and provides a map of nearby Pokéstops.[29] Alternatively, the player can view the physical world through the camera of the device ("camera mode").

Once the player arrives at a Pokéstop, the application, through AR technology, notifies the player that a Pokémon is available for collection.[30] Using camera mode, the player locates the Pokémon by holding the device upwards and moving around the Pokéstop until the three-dimensional creature appears on the screen of the device, superimposed on the real world environment as though it were a physical, tangible object.[31] The player then captures the Pokémon by swiping upwards on the screen to throw a Pokéball at the creature.[32]

---

21. *See id.* at 1.
22. *Id.* at 4.
23. *Id.*
24. *Id.* at 4–5.
25. Sam Haysom, *A Beginner's Guide: How to Play 'Pokémon Go'*, MASHABLE (July 22, 2016), http://mashable.com/2016/07/22/pokemon-go-beginners-guide/#irtcvbSGzmqE.
26. Serenity Caldwell et al., *Beginner's Guide: How to Play Pokémon Go!*, IMORE (Nov. 19, 2016, 7:00 AM), http://www.imore.com/pokemon-go-beginners-guide.
27. *Id.*
28. *See id.*
29. *Id.*
30. *Id*.
31. *Id*.
32. *Id*.

After collecting the Pokémon, the player must prepare the Pokémon for battle.[33] This requires catching the same type of Pokémon by navigating the real world as described above. Collecting the same type of Pokémon enables the creature to evolve in its strength and abilities.[34]

The final step of gameplay involves using the evolved Pokémon to battle other players' Pokémon at designated areas, known as Gyms.[35] Similar to locating Pokéstops, the application, through AR technology, provides a geographic view of nearby Gyms based on the location of the player's device.[36]

2. Reactions

Pokémon Go has generated a variety of reactions from players, third parties, politicians, and interest groups. Overall, players have embraced Pokémon Go. In the United States, Pokémon Go was released on July 6, 2016 and became the top grossing application within thirteen hours.[37] As of August 2016, the application attracted twenty-one million users and four to five million downloads each day.[38] Touchtone Research attributed Pokémon Go's instant success to nostalgia among older players, the opportunity for player interaction at Gyms, and the fact that the underlying AR technology requires the player to navigate the real world.[39]

Private entities, however, have not been as receptive to the game. Entities have complained that Niantic's placement of Pokéstops and Gyms on their properties has been disrespectful and disruptive.[40] For

33. *Id*.

34. *Pokémon Video Games*, POKÉMON, http://www.pokemon.com/us/pokemon-video-games/pokemon-go (last visited Nov. 8, 2016).

35. *See* Caldwell, *supra* note 26.

36. *Id*.

37. Jacob Siegal, *All the Crazy Stats About Pokémon Go Collected on a Single Infographic*, BGR (Aug. 4, 2016, 8:00 PM), http://bgr.com/2016/08/04/all-the-crazy-stats-about-pokemon-go-collected-on-a-single-infographic.

38. *Id*.

39. Rich Foreman, *Four Reasons Behind Pokémon Go's Wild Success*, STARTUP GRIND (Jul. 2016), https://www.startupgrind.com/blog/4-reasons-behind-pokemon-gos-wild-success/; Caroline Praderio, *The Simple Reason Pokémon Go is so Insanely Successful*, INSIDER (Jul. 11, 2016, 10:25 AM), http://www.thisisinsider.com/the-simple-reason-pokemon-go-is-so-successful-2016-7.

40. Tim Mulkerin, *You Officially Can't Play Pokémon Go at the Hiroshima Memorial or the Holocaust Museum*, BUS. INSIDER (Aug. 9, 2016, 11:33 AM), http://www.businessinsider.com/pokemon-go-pokestops-removed-from-hiroshima-memorial-and-holocaust-museum-2016-8. Private homeowners have also complained about Niantic's placement

instance, Niantic placed Pokéstops and Gyms at both the U.S. Holocaust Memorial Museum and the Hiroshima Peace Memorial Museum.[41] Upon request from the Museums' respective officials, however, Niantic removed these Pokémon hotspots.

Politicians and interest groups alike have expressed data privacy concerns about the game. Because each phase of gameplay involves the geolocation of the end user's device, Niantic may use the underlying AR technology to collect and disclose this information to third parties. Approximately one week after Pokémon Go was released, Minnesota Senator Al Franken expressed his concerns about Niantic's uninhibited access to all players' Gmail accounts, along with its collection and disclosure practices.[42] Similarly, the Electronic Privacy Information Center urged the Federal Trade Commission ("FTC")[43] to investigate Niantic's practices and ensure that Niantic complied with legislation carved out for children under the age of thirteen.[44] While remaining silent on its geolocation information collection and disclosure practices, Niantic assured Senator Franken that it remedied the issue of accessing players' Gmail accounts.[45] Pokémon Go, and more generally AR, demonstrate the growing concerns regarding a non-government entity's ability to collect, store, and disclose an end user's information. These concerns are governed by data privacy law.

---

of Pokéstops. In an ongoing class action suit against Niantic, plaintiffs alleged that Niantic caused a nuisance by placing Pokémon hotspots on their private properties without consent, which attracted crowds of Pokémon Go players. *See* Complaint at 1, Marder v. Niantic, Inc., 2016 WL 4073537 (N.D. Cal. 2016) (No. 3:16-cv-04300); Complaint at 8–9, Dodich v. Niantic, Inc., No. 3:16-cv-04556 (N.D. Cal. *Filed* Aug. 10, 2016).

41. Mulkerin, *supra* note 40.

42. Letter from Al Franken, Senator, Dist. of Minn., to John Hancke, Chief Exec. Officer, Niantic, Inc. (July 12, 2016), http://www.franken.senate.gov/files/letter/160712_PokemonGO.pdf. Mirroring Senator Al Franken's data security concerns along with other "social risks," China has banned Pokémon Go in part because it has also banned Google Maps, which is an integral component of the smartphone game. David Jagneux, *China Cites National Security as It Bans Pokémon Go and Other AR Games*, VENTURE BEAT (Jan. 15, 2017, 12:10 PM), http://venturebeat.com/2017/01/15/china-cites-national-security-as-it-bans-pokemon-go-and-other-ar-games.

43. The FTC is the primary federal agency that regulates non-government entities' data collection and sharing practices. *See infra* Part III.A.

44. Letter from Marc Rotenberg, President and Exec. Dir., Elec. Privacy Info. Ctr. et al. to Edith Ramirez, Chairwoman, Fed. Trade Comm'n (July 22, 2016), https://epic.org/privacy/ftc/FTC-letter-Pokemon-GO-07-22-2016.pdf.

45. Letter from Courtney Greene Power, Gen. Couns., Niantic, Inc., to Al Franken, Senator, Dist. of Minn. (Aug. 26, 2016), https://www.franken.senate.gov/files/documents/160826NianticResponse.pdf.

III. DATA PRIVACY LAW IN THE UNITED STATES

As announced by Boston attorneys Samuel D. Warren and Louis D. Brandeis in 1890, the touchstone of privacy law is "[t]hat the individual shall have the full protection in person and in property. . . [and has] the right to be let alone."[46] Over a century after Warren and Brandeis imparted their wisdom, the legal system struggles to adapt to novel notions of privacy, particularly in light of today's digital landscape. In the United States, data privacy law exclusively protects the end user's data, known as personally identifiable information ("PII").[47] PII generally refers to information that may personally identify the end user, such as social security numbers, passport numbers, and first and last names.[48] As a caveat, there is no universally adopted definition of PII.[49] Consequently, information may qualify as PII only for certain statutes, in certain jurisdictions.[50] The inconsistency of what qualifies as PII is attributed to the fragmented structure of data privacy law.

A. Structure of Data Privacy Law

In the United States, data privacy law is regulated at both the federal and the state level.[51] At the federal level, data is not uniformly regulated, but instead, varies depending on the industry.[52] Aside from these industry-specific bodies, the Federal Trade Commission ("FTC") is the main regulatory body.[53] The FTC is primarily responsible for protecting consumers from "[u]nfair methods of

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

47. 1 RAYMOND T. NIMMER & HOLLY K. TOWLE, DATA PRIVACY, PROTECTION, AND SECURITY LAW § 2.01, at 8 (2017).

48. *Id.*

49. *Id.* at 4.

50. *Compare* Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016) (holding the end user's GPS coordinates are PII in the context of the Video Privacy Protection Act of 1988), *with In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) (holding the end user's automatically generated geolocation information is not PII in the context of the Wiretap Act).

51. Lisa J. Sotto & Aaron P. Simpson, *United States*, *in* DATA PROTECTION & PRIVACY 2015 208, 208 (Rosemary P. Jay ed., 2015), https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf.

52. *Id.* For example, the Department of Health and Human Services regulates healthcare entities pursuant to the Health Insurance Portability and Accountability Act. *HIPAA Enforcement*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement (last visited Nov. 8, 2016).

53. Sotto & Simpson, *supra* note 51, at 208.

competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[54] In the context of data privacy law, the FTC protects consumers by "enforcing companies' privacy policies."[55] Thus, it is clear that the FTC's responsibilities are limited to consumers, or end users, rather than the general public.[56]

Data privacy law is also regulated at the state level and varies from state to state. At this level, the Attorney General has the authority to enforce privacy laws.[57] This discussion will focus on California, as it is considered the model state for data privacy laws.[58] California's recently enacted Electronic Communications Privacy Act limits the government's ability to collect and use a California resident's electronic communications for law enforcement purposes.[59] The Online Privacy Protection Act protects individuals' privacy against non-government entities by requiring website owners or operators to give end users notice regarding the types of information they intend to collect and/or disclose to third parties.[60] Considering the FTC's purpose along with these California laws, data privacy law protects an end user against both government and non-government entities.[61] Furthermore, California's laws naturally reveal two dichotomies: (1) users and non-users, and (2) government and non-government entities.

B. The Government/Non-Government Dichotomy

To simplify privacy law, privacy actions can be divided into two categories:(1) actions against the government, and (2) actions against a non-government entity ("NGE").[62] This distinction is important because it dictates the legal framework courts apply in resolving

54. 15 U.S.C. § 45(a) (2012).

55. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

56. *Id.* (noting the dominant role the FTC plays in protecting an individual's PII).

57. Sotto & Simpson, *supra* note 51, at 208.

58. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law.

59. David Navetta et al., *Five New Privacy Laws on Tap in California*, NORTON ROSE FULBRIGHT: DATA PROTECTION REP. (Oct. 23, 2015), http://www.dataprotectionreport.com /2015/10/five-new-privacy-laws-on-tap-in-california/. *See* CAL. PENAL CODE § 1546 (2016).

60. CAL. BUS. & PROF. CODE §§ 22575–79 (2008).

61. Sotto & Simpson, *supra* note, 51 at 209–10.

62. Victoria Schwartz, *Overcoming the Public-Private Divide in Privacy Analogies*, 67 HASTINGS L.J. 143, 146 (2015). *But see*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095 (2002) ("The government is increasingly contracting with private sector entities to acquire databases of personal information.").

privacy actions.[63] Courts apply the Fourth Amendment[64] reasonable expectation of privacy test[65] for actions against the government.[66] Courts do not apply the Fourth Amendment for privacy actions against NGEs,[67] but instead, rely on a variety of sources of law,[68] including federal statutes,[69] state constitutions,[70] state laws,[71] and FTC regulations.[72]

Professor Schwartz of Pepperdine University School of Law offers four justifications for this dichotomy. First, the government is traditionally more powerful than NGEs because of "a combination of coercion, state power, and . . . monopoly features of government."[73] This coercive power is rooted in the government's ability to deprive the individual of life and liberty.[74] Second, the government's surveillance abilities may instill fear in an individual, deter the individual from making decisions that develop his or her identity, and ultimately chill participation in the democratic system.[75] Third, the

63. Schwartz, *supra* note 62, at 150; Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 298 (1983).

64. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

65. Katz v. United States, 389 U.S. 347, 359 (1967) (holding the government conducted an unreasonable search by wiretapping a telephone booth because the defendant had a reasonable expectation of privacy); *see also id.* at 361 (Harlan, J., concurring) (outlining a two-part expectation of privacy test); Minnesota v. Carter, 525 U.S. 83, 97 (1998) (stating that the reasonable expectation of privacy test "has come to mean the test enunciated by Justice Harlan's separate concurrence in *Katz*.").

66. Schwartz, *supra* note 62, at 150.

67. Chandler v. Miller, 520 U.S. 305, 323 (1997) ("[T]he private sector [is] a domain unguarded by Fourth Amendment constraints."); United States v. Jacobsen, 466 U.S. 109, 113 (1984).

68. Schwartz, *supra* note 62, at 151.

69. *See*, *e.g.*, Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–05 (2012).

70. *See, e.g.*, Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 644 (Cal. 1994) (holding the California constitution protects an individual's right to privacy against both government and non-government entities).

71. *See*, *e.g.*, CAL. LAB. CODE § 435 (2011) ("No [public or private] employer [except the federal government] may cause an audio or video recording to be made of an employee in a restroom, locker room, or room designated by an employer for changing clothes . . ."); CAL. PENAL CODE § 637.7 (2016) ("No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.").

72. Solove & Hartzog, *supra* note 55, at 588 ("The FTC can bring an action against a company for breaching a promise in its privacy policy—and, even more broadly, for any deceptive or unfair act or practice.").

73. Schwartz, *supra* note 62, at 174.

74. *Id*.

75. *Id*. at 176. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1657 (1999) ("[L]imitless surveillance of expression in cyberspace . . . can corrupt individual decision-making about the elements of one's identity.").

government traditionally has better access to superior technology than NGEs.[76] Finally, the government faces bureaucratic pressures to produce favorable results in the short-term without considering the long-term effects.[77] This is particularly salient for law enforcement, where police forces are constantly pressured to protect the public by arresting suspects in a short amount of time.[78]

Noting that courts often analogize between government and non-government cases without any basis,[79] Professor Schwartz developed a framework for courts to use in deciding whether such analogies are appropriate.[80] The framework requires balancing the four justifications that explain the government/NGE dichotomy.[81] Thus, a court resolving a privacy action against an NGE may analogize to Fourth Amendment cases if the NGE exhibited coercive power,[82] had the ability to instill fear in an individual that amounts to potentially chilling democratic participation,[83] had better access to superior technology,[84] and faced similar bureaucratic pressures.[85]

---

76. Schwartz, *supra* note 62, at 178. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) ("[I]t may well be, as the Government concedes, that surveillance of personal property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.").

77. Schwartz, *supra* note 62, at 180. *See* Adam Shinar, *Public Employee Speech and the Privatization of the First Amendment*, 46 CONN. L. REV. 1, 40 (2013) (noting that bureaucracy in government entities is intentional and "intrinsic to government work").

78. Solove, *supra* note 62, at 1104 (Asserting that bureaucratic pressure results in "decisions without adequate accountability, dangerous pockets of unfettered discretion, and choices based on short-term goals without consideration of the long-term consequences or the larger social effects.").

79. Schwartz, *supra* note 62, at 147–48. *Compare Dow Chem. Co.*, 476 U.S. at 231–32 (the Court preserved the public-private distinction by stating "[w]hether they may be employed by competitors to penetrate trade secrets is not a question presented in this case. Governments do not generally seek to appropriate trade secrets of the private-sector, and the right to be free of appropriation of trade secrets is protected by law."), *with* City of Ontario v. Quon, 560 U.S. 746, 759 (2010) (the Court did not explicitly reject the public-private analogy in the context of a government workplace case, but noted that some states require employers, i.e., non-government entities, to disclose surveillance of electronic communications).

80. Schwartz, *supra* note 62, at 180.

81. *Id*. at 187.

82. For example, security guards are non-government entities that have the ability to deprive individuals of liberty. Elizabeth E. Joh, *The Paradox of Private Policing*, 95 J. CRIM. L. & CRIMINOLOGY 49, 50 (2004).

83. For example, when financial institutions call to find out if a loan applicant has a terminal illness, "privacy is violated in a manner about as consequential as if the same violations had been carried out by a government agency." Amitai Etzioni, *The Privacy Merchants: What Is to Be Done?*, 14 U. PA. J. CONST. L. 929, 934 (2012).

84. For example, Google Maps readily provides the public with access to satellite photos. Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2344 (2007).

85. Schwartz, *supra* note 62, at 187. *See* Gerald Frug, *The Ideology of Bureaucracy in American Law*, 97 HARV. L. REV. 1277, 1306 (2005) ("[C]orporate bureaucratic power, as it has

Although Schwartz's normative framework has the potential to guide courts in deciding whether analogizing is appropriate, the framework has its drawbacks. While Professor Schwartz provided examples, courts must ultimately exercise heavy judicial discretion in applying each factor. Because the factors are based on tradition rather than distinctions drawn from legislation or precedent,[86] courts lack guidance in defining these factors, which results in a lack of predictability for courts and NGEs.[87] This is particularly salient for the first factor, which is arguably the most prominent distinction between government and NGEs. Although Schwartz defined the first factor as "a combination of coercion, state power, and the monopoly features of government,"[88] a number of questions arise: What is meant by coercion? What are specific monopolistic features of the government? Moreover, Professor Schwartz noted that the most extreme form of coercive power is the government's ability to deprive the individual of life or liberty,[89] suggesting that coercive power operates on a spectrum. This proves problematic if a court is faced with an NGE that falls in the middle of the spectrum.

Because courts must exercise heavy judicial discretion in defining and applying the four factors, the framework as a whole is unpredictable and may aggravate the inconsistencies in data privacy law. This is particularly relevant for NGEs. As stated above, courts do not apply the Fourth Amendment to privacy cases against NGEs, but instead rely on a variety of sources of law, including federal law, state constitutions, state law, and FTC regulations—some of which do not incorporate the Fourth Amendment's reasonable expectation of privacy test.[90] If the court determined that analogizing was

---

emerged, has imposed a forceful objective restraint on the shareholders' ability to govern the corporation.").

86. By way of analogy, Congress codified four factors in the fair use doctrine from copyright law. *See* 17 U.S.C. § 107 (2012). These factors guide courts in deciding whether a defendant's use of a plaintiff's copyrightable work is authorized. Barton Beebe, *An Empirical Study of U.S. Copyright Fair Use Opinions, 1978–2005*, 156 U. PA. L. REV. 549, 551 (2008). Scholars note that, notwithstanding this legislation and a rich body of precedent, courts define each factor inconsistently. *See* Michael J. Madison, *Rewriting Fair Use and the Future of Copyright Reform*, 23 CARDOZO ARTS & ENT. L.J. 391 (2005).

87. Predictability in the rule of law is one of the highest priorities in the judicial system. Kem Thompson Frost, *Predictability in the Law, Prized Yet Not Promoted: A Study in Judicial Priorities*, 67 BAYLOR L. REV. 48, 51 (2015).

88. Schwartz, *supra* note 62, at 174.

89. *Id*.

90. *Id*. at 151.

appropriate, then NGEs may be subject to the Fourth Amendment reasonable expectation of privacy test, which may be different from the applicable laws that govern NGEs. This unpredictability may discourage NGEs from developing and manufacturing products that could affect the end user's privacy, such as applications that integrate the user's geolocation information.

IV. GEOLOCATION INFORMATION

As a preliminary matter, geolocation information ("GI") refers to the specific locations of an electronic communications device, such as a smartphone or a tablet.[91] While GI may be generated in a few different ways,[92] the most relevant is the Global Positioning System ("GPS"), which utilizes a system of satellites to accurately pinpoint the location of a device.[93] The U.S. Department of Defense initially developed the GPS for military purposes in order to bolster national security.[94] This purpose became one of the four underlying policies of the GPS, along with "effectively contribut[ing] to . . . public safety, scientific, and economic interests of the U.S. . . ."[95] Since its inception, the GPS has been adopted in contexts outside the military, such as driving navigation[96] and agriculture.[97] Furthermore, mobile application developers have increasingly incorporated the GPS into their applications to generate GI[98] and unsurprisingly, a recent study

91. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011).

92. *See In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 137 (E.D.N.Y. 2013) (noting that GI is generated through cell-site towers, the Global Positioning System, and wireless routers).

93. *See* Renee McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 414 (2007).

94. Aaron Renenger, Note, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L.J. 549, 550 (2002).

95. 51 U.S.C. § 50112 (2012).

96. *Roads & Highways*, GPS.GOV, http://www.gps.gov/applications/roads (last visited Mar. 18, 2017).

97. *Agriculture*, GPS.GOV, http://www.gps.gov/applications/agriculture (last visited Mar. 18, 2017).

98. Will Fulton, *Five Great Location-Based Games That Aren't Pokémon Go*, DIG. TRENDS (July 18, 2016, 11:27 AM), http://www.digitaltrends.com/gaming/best-location-based-gps-games/. In February 2012, the FTC reported that many mobile applications that target children automatically collect geolocation information. FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DIS*APP*OINTING (Feb. 2012), https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

revealed that 90% of Americans use their smartphone for geolocation-related purposes.[99]

A. The Government/Non-Government Dichotomy

Geolocation information is one example of the dichotomy between the government and NGEs in data privacy law. Consequently, the Fourth Amendment ensures protection against government privacy intrusions. The Supreme Court recently confirmed this principle in a case involving GI. In *United States v. Jones*, the government placed a GPS device on defendant Jones' vehicle and tracked his geolocation for four weeks.[100] The Supreme Court resolved the issue of whether Jones' Fourth Amendment right had been violated and held that tracking Jones' location via the GPS constituted a search within the meaning of the Fourth Amendment.[101] Therefore, *Jones* corroborates that the Fourth Amendment indeed protects an individual's GI against government intrusions.

Because GI exemplifies this dichotomy, presumably an end user's GI is protected against NGE's, such as technology companies and mobile application developers. In *Yershov v. Gannett Satellite Info. Network, Inc.*, the defendant media company developed and distributed a news and entertainment mobile app.[102] Each time the plaintiff end user watched a video on the app, the defendant shared the plaintiff's GI with third party companies.[103] The First Circuit held that GI qualified as PII under the Video Privacy Protection Act of 1988, and the Act prohibits disclosing GI to third parties.[104] Therefore, the First Circuit confirmed that, at least under the Video Privacy Protection Act, an end user's GI is protected against NGEs, such as mobile application developers.

B. The FTC's Geolocation Privacy Concerns

The marriage between mobile applications and the GPS presents an interesting paradox: While Google Maps efficiently delivers

99. Monica Anderson, *More Americans Using Smartphones for Getting Directions, Streaming TV*, PEW RES. CTR. (Jan. 29, 2016), http://www.pewresearch.org/fact-tank/2016/01/29/us-smartphone-use.

100. 132 S. Ct. 945, 948 (2012).

101. *Id.* at 949.

102. 820 F.3d 482, 484 (1st Cir. 2016).

103. *Id.* at 485.

104. *Id.* at 489; *see* 18 U.S.C. § 2710(b)(1) (2012).

driving directions and Pokémon Go encourages social and physical activity in the real world, this marriage allows an NGE to freely collect and disclose GI virtually unopposed. An NGE's freedom, according to the FTC, raises four privacy concerns: (1) targeted advertising, (2) stalking or physically harming the end user, (3) lack of end user's consent, and (4) hackers committing cybercrimes.

Underlying the first concern is the possibility that an NGE may collect or disclose an end user's GI for targeted advertising.[105] By collecting an end user's aggregate GI, the NGE can build the end user's profile of recently visited locations.[106] The NGE may use this profile to target advertising to the end user through his or her device.[107] The FTC also expressed the concern that an NGE may collect or disclose this information to the end user's detriment.[108] Specifically, a criminal may identify the end user's current or future GI and use this information to stalk or physically harm the end user.[109] Moreover, there is also the possibility that an NGE collects and discloses this information without the end user's express consent.[110] This is particularly troublesome if NGEs use or disclose the GI for unspecified purposes, e.g., selling the information to the government.[111] Lastly, an NGE's ability to collect and disclose an end user's GI may increase the possibility of a privacy breach.[112] Specifically, a hacker may access the NGEs GI database to commit a cybercrime, such as identity theft.[113]

C. The Stored Communications Act

Notwithstanding the FTC's enumerated privacy concerns, currently there is no federal legislation that expressly protects an end

105. *The Location Privacy Protection Act of 2014: Hearing on S.2171 Before the Subcomm. for Privacy, Tech. & the Law of the U.S. S. Comm. on the Judiciary*, at 2–3 (June 4, 2014) [hereinafter *Senate Hearing*] (prepared statement of the Federal Trade Commission), https://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf; *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 138 (E.D.N.Y. 2013).

106. *Senate Hearing*, *supra* note 105, at 2.

107. *In re Smartphone*, 977 F. Supp. 2d at 138.

108. *Senate Hearing*, *supra* note 105, at 2.

109. ISACA, GEOLOCATION: RISKS, ISSUES AND STRATEGIES, 8 (2011), http://www.isaca.org/groups/professional-english/wireless/groupdocuments/geolocation_wp.pdf.

110. *Senate Hearing*, *supra* note 105, at 3.

111. *See* Solove, *supra* note 62, at 1095.

112. *Senate Hearing*, *supra* note 105, at 2.

113. ISACA, *supra* note 109.

user's GI.[114] Instead, the Electronic Communications Privacy Act of 1986 presumably governs.[115] While this Act consists of three titles, the most relevant is Title II, known as the Stored Communications Act ("SCA"). The SCA protects an end user's stored electronic communications ("SEC")[116] against a provider's (NGE's) compelled[117] and voluntary[118] disclosure to the government. While the SCA unambiguously regulates an NGE's disclosure practices, it is unclear whether the SCA protects GI generated from mobile applications, such as Pokémon Go.

To qualify for SCA protection, as a threshold matter, GI must qualify as an SEC. To qualify as an SEC, GI must be "temporar[ily and] intermediate[ly]" stored by either: (1) an electronic communication service ("ECS"), or (2) a remote computing service ("RCS").[119] An ECS must allow end users to communicate.[120] An example is WhatsApp: a mobile application that allows end users to communicate through a text message platform and share their respective locations.[121] If the end user chooses to share his or her location, WhatsApp temporarily stores the user's GI.[122] An RCS, in contrast, is an NGE that offers "computer storage or processing services."[123] For example, Dropbox provides cloud storage for files, such as documents and photos. If an end user opts to automatically upload files from a smartphone, Dropbox tracks the smartphone's GI and restarts the upload when it detects a significant change in the location.[124] Therefore, Dropbox collects GI in order to process and

114. Jennifer Ann Urban, *Has GPS Made the Adequate Enforcement of Privacy Laws in the United States a Luxury of the Past?*, 16 WAKE FOREST J. BUS. & INTELL. PROP. L. 401, 414 (2016).

115. Christian Levis, Note, *Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 191, 204 (2011).

116. Storage Communications Act, 18 U.S.C. §§ 2701–12 (2012).

117. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1218 (2004); *See* 18 U.S.C. § 2703 (2012).

118. Kerr, *supra* note 117; *See* 18 U.S.C. § 2702 (2012).

119. 18 U.S.C. § 2510(17)(a) (2012).

120. 18 U.S.C. § 2510(15) (2012).

121. *FAQ*, WHATSAPP, https://www.whatsapp.com/faq/en/iphone/20964587 (last visited Feb. 8, 2017).

122. *WhatsApp Legal Info*, WHATSAPP, https://www.whatsapp.com/legal/#terms-of-service (last visited Feb. 8, 2017).

123. 18 U.S.C.§ 2711(2) (2012).

124. *Background Uploading—Why the Dropbox iOS App Needs Location Data*, DROPBOX, https://www.dropbox.com/en/help/209 (last visited Feb. 8, 2017).

upload files.[125] Because WhatsApp and Dropbox qualify as an ECS and RCS, respectively, the SCA governs their disclosure practices.

The SCA, however, does not protect Pokémon Go players. Assuming that a Pokémon Go player's GI is "temporar[ily and] intermediate[ly]"[126] stored, Niantic is not an ECS because Pokémon Go players cannot directly communicate with each other through the application itself. Nor does Niantic qualify as an RCS because it does not collect and store a player's GI merely for storage or processing services. Consequently, the SCA does not protect Pokémon Go players and end users of other mobile applications that integrate GI in a similar manner. Rather, these end users are only entitled to Fourth Amendment protection against the government.[127]

V. THE PROPOSED LOCATION PRIVACY PROTECTION ACT

As stated in Part I, Pokémon Go, and more generally AR, demonstrate an NGE's uninhibited ability to collect, store, and disclose an end user's GI to third parties without consent.

While current federal legislation does not regulate this ability,[128] the Location Privacy Protection Act ("LPPA") proposes to bridge this gap by prohibiting NGEs from collecting or disclosing end users' GI without consent, absent an exception.[129]

This Note identifies legislative gaps in the LPPA and recommends appropriate amendments (collectively "amended LPPA") in hopes of accomplishing three goals. First, this Note ensures that the amended LPPA protects an end user's geolocation privacy in light of the FTC's concerns. Today, technology companies, like mobile application developers, capitalize on new technologies, such as AR. Without much thought, end users give in to these technologies for convenience or mere entertainment. These users, however, may not realize that these companies may freely collect, store, and disclose their GI to undisclosed third parties for undisclosed purposes. This creates an information asymmetry between companies and end users that, according to the FTC, raises four privacy concerns: specifically

125. *Id.*
126. 18 U.S.C. § 2510(17)(a) (2012).
127. Kerr, *supra* note 117, at 1213.
128. Urban, *supra* note 114, at 414.
129. Location Privacy Protection Act, S. 2270, 114th Cong. § 2713 (2015).

targeting advertisements at end users;[130] physically harming end users;[131] collecting end users' GI without consent,[132] and; hackers committing cybercrimes against end users.[133]

This Note also ensures that the amended LPPA remains consistent with the policies underlying the GPS. The LPPA's first and foremost concern is protecting an end user's privacy over GI. Although this right is important, it must be balanced against the policies of national security, public safety, scientific interests, and economic interests[134] that underlie the system that generates GI.

While the ultimate goal of the amended LPPA is to protect an end user's GI in light of privacy and policy concerns, the amended LPPA also promotes predictability for courts and NGEs alike by prescribing bright line rules. Professor Schwartz noted that courts arbitrarily decide when to analogize between government and non-government privacy violations,[135] and proposed a four-factor framework to determine whether such analogies are appropriate.[136] This framework, however, requires heavy judicial discretion in defining and applying each factor. The solution must be legislative. The amended LPPA reduces the judicial discretion that Professor Schwartz's framework sought to counteract by expressly identifying what NGEs can and cannot do with an end user's GI.

A. Interpretation

Minnesota Senator Al Franken introduced the LPPA to amend the Electronics Communications Privacy Act. This Note focuses on five provisions of the LPPA: (1) the general prohibition, (2) exceptions, (3) the stalking and domestic violence provision, (4) the publication requirement, and (5) enforcement.

First, the LPPA generally prohibits a non-government individual or entity ("covered entity") from knowingly collecting or disclosing an end user's GI without express consent.[137] In isolation, this provision

130. Fed. Trade Comm'n, *supra* note 105; *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 138 (E.D.N.Y. 2013).
131. Fed. Trade Comm'n, *supra* note 105.
132. *Id.*
133. *Id.*
134. 51 U.S.C. § 50112 (2012).
135. Schwartz, *supra* note 62, at 147–48.
136. Schwartz, *supra* note 62, at 187.
137. Location Privacy Protection Act, S. 2270, 114th Cong. § 2713(b)(1) (2015).

undoubtedly protects the end user's geolocation privacy. Notably, this provision is silent on a covered entity's ability to store an end user's GI. This ability, however, is implied because the LPPA does not require a covered entity to disclose the information within a specified period of time after initially collecting the information. Because a covered entity may store the information in perpetuity, this ability can be read into the statute. Therefore, the LPPA requires consent to collect, *store*, and disclose the end user's GI.

The LPPA also enumerates nine exceptions that allow a covered entity to collect and disclose an end user's GI *without* consent. The relevant exceptions may be classified into the following categories: (1) disclosure to a parent or guardian locating a minor, a ward, or a legally incompetent person; (2) disclosure for other emergency purposes; (3) disclosure pursuant to a court order or for law enforcement purposes; (4) disclosure to operate a network; (5) necessary disclosure to another person for any of the previously mentioned exceptions; (6) disclosure to protect the NGE's property, its customers, or another entity from unlawful conduct, and; (7) disclosure to any other covered entity that did not initially collect information from the end user's device.[138]

Moreover, the LPPA's stalking and domestic violence provision prohibits the knowing and willful disclosure of an end user's GI to another covered entity for these purposes.[139] The LPPA also imposes a fine, imprisonment for a maximum of two years, or both, regardless of the end user's consent.[140]

Additionally, the LPPA requires a covered entity to publish its privacy policy on a website. This policy must include the purpose of collection and disclosure, the specific non-governmental recipients of disclosure, and the end user's ability to revoke consent.[141] This provision, however, only governs a covered entity that collects GI from at least 1,000 devices in a year.[142]

Lastly, the LPPA provides the means of enforcing its provisions. The enforcement provision requires the Attorney General to work with

138. *Id.* § 2713(b)(2).
139. *Id.* § 2266(a).
140. *Id.* § 2266(b).
141. *Id.* § 2713(b)(4).
142. *Id.*

the FTC to "issue regulations to implement the requirements of this regulation."[143]

B. Legislative Gaps and Recommendations

1. The LPPA's Silence on Storage

The LPPA undoubtedly regulates a covered entity's ability to collect and disclose an end user's GI. Consequently, the LPPA does not explicitly address an NGE's ability to store an end user's GI, but this ability is implied. Since the LPPA does not regulate storage practices, an NGE can store an end user's GI in perpetuity.

Perhaps the LPPA drafters intended to defer to the Stored Communications Act. This is plausible considering that the SCA immediately precedes the proposed LPPA. It is unlikely, however, that the drafters intended to defer to the SCA because the LPPA only modifies Section 2702(c) of the SCA, which regulates a provider's (NGE's) ability to voluntarily disclose a subscriber's information.[144] Therefore, the LPPA's modification only applies to a provider's disclosure practices, which does not address the provider's storage practices.

Even if the drafters intended to defer to the SCA, the SCA does not adequately address an NGE's ability to store an end user's GI. As stated above, the SCA only protects a "temporar[ily and] "intermediate[ly]" stored electronic communication.[145] Assuming that GI qualifies as an SEC, the next and more important issue is whether the SCA limits an NGE's ability to store an end user's GI. The SCA only regulates a provider's (NGE's) compelled[146] and voluntary[147] disclosure to the government. The SCA, therefore, only regulates an NGE's disclosure practices and is virtually silent on storage practices. Because of this silence, the only viable solution is to amend the proposed LPPA.

143. *Id.* § 2713(c)(1).
144. *Id.*
145. 18 U.S.C. § 2510(17)(a) (2012).
146. Kerr, *supra* note 117, at 1218. 18 U.S.C. § 2703 (2012).
147. Kerr, *supra* note 117, at 1218. 18 U.S.C. § 2702 (2012).

2. Recommended Amendments

The recommended solution is three-fold: (1) amend the general prohibition; (2) add the storage limit provision,[148] and; (3) amend the publication provision.

First, the general prohibition should be amended to reflect a covered entity's ability to store the end user's GI. Accordingly, this provision should read: "Except as provided in paragraph (2), a covered entity may not knowingly collect, store, or disclose to another covered entity the geolocation information from an electronic communications device without the consent of the individual that is using the electronic communications device."[149]

Next, the LPPA should include a provision that imposes a time limit on storing an end user's GI. This storage limit provision should read: "A covered entity who collects the geolocation information from an electronic communications device may store such information for X amount of time."

The publication provision should be amended to better inform the end user of the covered entity's storage practices. This provision should read: "A covered entity that collects the geolocation information . . . shall maintain a publicly accessible Internet website that includes . . . the amount of time it intends to store the end user's geolocation information pursuant to the time limit imposed in [the second recommended amendment]."

Unlike the preceding provisions, the enforcement provision should not be amended because it clearly and unambiguously delegates enforcement to the Attorney General and the FTC. Even in the absence of this provision or other federal legislation, the FTC publicly supported the LPPA's initiatives and vowed to continue to enforce privacy violations against NGEs.[150] Because the enforcement provision simply formalizes what the FTC has vowed to do, this provision should remain status quo.

148. The drafters of the LPPA did not hesitate to draw bright line rules. For example, Section 2713(b)(4) only requires publication if the covered entity collects GI from at least 1,000 electronic communications devices.

149. Location Privacy Protection Act, S. 2270, 114th Cong. § 2713(b)(1) (2015).

150. *Senate Hearing*, *supra* note 105, at 12.

C. Justifications

The amended LPPA first and foremost seeks to protect an end user's geolocation privacy. This section demonstrates that the amended LPPA accomplishes this goal in light of the FTC's enumerated privacy concerns and the policies underlying the GPS, with the added benefit of promoting predictability in data privacy law.

1. The FTC's Privacy Concerns

The FTC articulated four concerns associated with GI: (1) targeted advertising, (2) stalking or physical harm, (3) lack of an end user's consent, and (4) hackers committing cybercrimes. This section determines whether the amended LPPA addresses these concerns.

First, the FTC articulated a concern regarding an NGE's use of an end user's GI for targeted advertising without consent.[151] None of the LPPA's exceptions allow collection or disclosure for targeted advertising. This purpose is unnecessary for locating a minor or incompetent person, other emergencies, for law enforcement purposes, or out of necessity. Nor is disclosure required to protect the NGE, its customers, or other NGEs. Notably, the last exception allows a third party's collection or disclosure if the third party did not conduct the initial collection. Thus, the third party must lawfully acquire this information from a covered entity under one of the previous exceptions. Because these exceptions apply to a targeted end user in limited circumstances, it is very unlikely that the covered entity will disclose a significant proportion of user GI to a third party. Consequently, the ambitious third party must rely on collecting an end user's GI individually. Requiring collection on an individual basis imposes high transactional costs that are likely to deter the third party. Therefore, the proposed LPPA addresses the targeted advertising concern.

The FTC also noted the possibility that an NGE may collect an end user's GI to locate and/or harm the user.[152] Two of the LPPA's provisions directly address this concern. The necessity exception allows an NGE to collect or disclose GI if it is necessary to protect the end user from unlawful conduct. This provision affirmatively protects the end user from physical harm. The stalking and domestic violence

151. *Senate Hearing*, *supra* note 105; *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 138 (E.D.N.Y. 2013).

152. *Senate Hearing*, *supra* note 105.

provision prohibits an NGE's disclosure to stalk or commit domestic violence against the end user.[153] This provision also imposes criminal penalties to deter such conduct.[154] Because the LPPA allows disclosure to prevent harm and criminalizes such use for stalking or domestic violence purposes, the LPPA addresses the FTC's second concern.

The FTC also recognized that an NGE may collect an end user's GI without the end user knowing.[155] The policies underlying this concern are transparency, allowing the end user to make better-informed decisions, and preventing unfair or deceptive practices.[156] A few of the LPPA's provisions address this concern. The LPPA's general prohibition requires the end user's consent for collection. Coupled with the publication requirement, the end user has ample access to the covered entity's GI collection practices. These requirements may provide the end user with actual knowledge of—or at least make it more likely that the end user has knowledge of—the covered entity's data practices.[157] The LPPA's exceptions allow collection or disclosure without the end user's express consent in very limited circumstances. The underlying policies for these exceptions outweigh the end user's geolocation privacy. For instance, the first category of exceptions exhibits a strong policy of protecting minors and legally incapacitated persons. The legal purposes exception promotes the policy of assisting law enforcement to protect the general public. The necessity exception, as described above, protects the end user from harm. It is clear that the LPPA does not afford the individual the absolute right to privacy, but rather, balances this right with strong public policies. Notwithstanding these exceptions, the LPPA addresses the FTC's third concern.

Lastly, the FTC articulated the possibility of hackers accessing an end user's GI to commit a cybercrime, such as identity theft.[158] At the

153. Location Privacy Protection Act, S. 2270, 114th Cong. § 2266(a) (2015).

154. *Id.* § 2266(b).

155. *Senate Hearing*, *supra* note 105.

156. 15 U.S.C. § 45(a) (2012).

157. This assumption breaks down considering that most end users consent to privacy policies without reading them. Amanda Grannis, Note, *You Didn't Even Notice! Elements of Effective Online Privacy Policies*, 42 FORDHAM URB. L.J. 1109, 1154 (2015); *see* Sarah Gordon, *Privacy: A Study of Attitudes and Behaviors in U.S., U.K. and E.U. Information Security Professionals*, SYMANTEC SECURITY RESPONSE WHITE PAPER 12 (2003), https://www.symantec.com/avcenter/reference/privacy.attitudes.behaviors.pdf.

158. *Senate Hearing*, *supra* note 105.

heart of this concern are an NGE's storage practices. If an NGE did not store an end user's GI, there would be absolutely no risk of a privacy breach because there would be nowhere to steal the information from. While the NGE's ability to store an end user's GI may be implied from the general prohibition provision, none of the LPPA's provisions regulate this practice. The recommended storage limit provision bridges this gap and prevents NGEs from perpetually storing an end user's GI. A defined time limit restricts the amount of time for hackers to unlawfully access this information, and thus, reduces the opportunity for a privacy breach.[159] Therefore, in reducing this opportunity, the LPPA and the recommended amendments address the FTC's final concern.

Although the preceding provisions address the FTC's enumerated privacy concerns, these provisions are meaningless without enforcement. The LPPA's enforcement provision unambiguously delegates the role of enforcement to the Attorney General and the FTC. Therefore, the amended LPPA addresses the FTC's privacy concerns associated with GI.

2. GPS Policies

As stated above, the amended LPPA intends to protect the end user's right to privacy over his or her GI. This right, however, must be balanced against the policies underlying the very system that generates GI: the Global Positioning System. These policies include: (1) national security, (2) public safety, (3) scientific interests, and (4) economic interests.[160]

The U.S. Department of Defense originally developed the GPS for military purposes to bolster national security.[161] In its current state, the LPPA does not directly address national security concerns, such as the potential that databases consisting of end user information will be hacked.[162] By requiring covered entities to obtain consent before collection and disclosure, the end user ultimately decides whether to

159. Notably, it may not be feasible to completely eliminate the possibility of a privacy breach because the only solution is to prevent NGEs from collecting and storing an end user's GI. The LPPA's exceptions, however, underscore important countervailing policies that weigh in favor of collection and storage.

160. 51 U.S.C. § 50112 (2012).

161. Renenger, *supra* note 94, at 550.

162. *See* Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor?*, 18 N.C. J. L. & TECH. 233 (2016).

contribute his or her GI to this database. The end user's decision directly impacts national security by influencing the size of the database or the potential hacking target. The recommended storage limit provision directly promotes national security because a time limit minimizes the time frame for an entity—whether foreign or local—to hack into a covered entity's database of GI. Therefore, the amended LPPA promotes the policy of national security.

The amended LPPA must also be considered in light of the public safety policy. The most relevant LPPA portions are the necessity exception and the stalking and domestic violence provision. The necessity exception allows an NGE to collect or disclose GI if it is necessary to protect the end user from unlawful conduct. The LPPA allows such use to protect the end user or his or her property from harm. Moreover, the stalking and domestic violence provision explicitly prohibits disclosure to stalk or commit domestic violence against an end user. This provision also imposes criminal penalties. On a superficial level, these provisions only protect the end user. But considering that most individuals use mobile applications that require collecting GI, the LPPA protects a significant portion of the population.[163] Therefore, the LPPA promotes the policy of public safety.

The amended LPPA must also be balanced against the scientific interests of the U.S. In the geolocation context, this refers to researching and developing GPS technology.[164] While the amended LPPA does not directly address this policy, it limits covered entities' collection, storage, and disclosure practices. Broadly, these limitations exhibit Congress's power to restrict how covered entities use the information the GPS generates. Because these limitations may discourage technology companies from developing GPS technology, the amended LPPA has the potential to impede scientific progress. These limitations, however, may promote efficiency in scientific progress by providing clear rules for technology companies to follow. Therefore, while the amended LPPA does not directly address scientific interests, it may obstruct or promote this policy.

The final policy to consider is the economic interests of the U.S. The underlying concern is that the amended LPPA chills researching

163. Anderson, *supra* note 99.

164. *See* 10 U.S.C. § 2281(b) (2012) (expanding how GPS may be applied for transportation and other civilian purposes).

and developing GI because it unduly burdens covered entities. This is a distinct possibility, particularly if covered entities have a financial stake in the GI itself. On the contrary, the amended LPPA could be framed as bright line rules that promote competition. By requiring all covered entities to abide by the same rules, covered entities may be incentivized to think outside the box and invest in other creative and productive ventures that place goods on the market for public consumption. This consumption will contribute to the economy and, therefore, the LPPA and the recommended amendments promote the policy of economic interests. Taken together, the amended LPPA promotes each policy underlying the GPS.

3. Predictability

One of the greatest criticisms of U.S. data privacy jurisprudence is its unpredictable nature, which arises from the fragmented enforcement structure. The LPPA represents a shift in remedying this structure in two ways. First, as a federal bill, the LPPA casts a wide net in regulating an NGE's GI collection, storage, and disclosure practices at both the federal and state level.

Second, the amended LPPA effectively eliminates the current heavy judicial discretion[165] by providing courts with bright line rules. The amended general prohibition provision and recommended amendment explicitly require an NGE to obtain consent before collecting, storing, and disclosing an end user's GI. The LPPA's enumerated exceptions allow these practices without an end user's consent in limited, unambiguous circumstances. The storage limit provision specifies the maximum amount of time a non-government entity may store the information. The amended publication requirement lists the types of information the NGE must include in its privacy policy. The enforcement provision delegates the enforcement to the Attorney General and the FTC. In tandem, these provisions provide bright line rules, leaving minimal room for interpretation, and therefore, promote predictability for courts and NGEs alike.

D. Caveats

While this Note narrowly focuses on the amended LPPA and an NGE's storage practices in light of numerous privacy and policy

165. Schwartz, *supra* note 62, at 147–48.

considerations, it leaves a several areas unexplored. First, this Note only focuses on select provisions of the LPPA. These provisions, however, are most relevant for the narrow purpose of this Note, which is to address an NGE's storage practices. Notably, this omission does not undermine the importance of the other provisions.

This Note does not address *how* an NGE may store an end user's GI. The *how* refers to the mechanics surrounding the NGE's storage practices, including its ability to contract third parties. This *how* issue concerns the NGE's direct relationship with third parties. While this indirectly affects the end user, this only focuses on the direct relationship between the NGE and the end user. Notwithstanding that the *how* issue is beyond the scope of this Note, it may be an important area for future legislation to regulate.

VI. CONCLUSION

Today's digital landscape presents novel technologies that pose practical difficulties for protecting an individual's right to privacy. In part, this is due to the subtle complexities of such technologies. An example is augmented reality. AR is convenient because it eliminates the need for an intermediary device by providing information directly to the user. In the context of Pokémon Go, however, the application developer requires players' consent to collect, store, and disclose their GI to undisclosed third parties. Although a lawsuit has not yet been filed, policy makers and interest groups alike have expressed concerns over the privacy implications arising from Pokémon Go. Therefore, the underlying issue is whether the law adequately protects an end user's GI against non-government entities, such as mobile application developers.

As the law stands, the answer is an emphatic no. The law clearly protects an individual's right to privacy against the government. An end user's privacy from a non-government entity, however, is limited. Currently, non-government entities may freely collect, store, and disclose an end user's geolocation information without consent. Although the Location Privacy Protection Act proposes to bridge this gap, it is unclear if the Act imposes a time limit on storing this information. This Note recommends legislative amendments to the federal bill to address storage practices in light of privacy and policy concerns. Additionally, these amendments serve to guide lawmakers

in enacting bright line rules of law to promote predictability, of which privacy law has been sorely lacking.

That technology develops more quickly than the law adapts is one of the realities that policymakers, judges, and lawyers alike face in today's world. But, reality and technology aside, this should not diminish an individual's right to privacy in the real or digital world.