Vanderbilt Journal of Entertainment & Technology Law

Volume 15
Issue 3 *Issue 3 - Spring 2013*

Article 6

2013

Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection

Timothy J. Van Hal

Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection

ABSTRACT

With the implementation of new geolocation technologies, the boundaries between private versus commercial and secret versus easily ascertainable have vanished. Consumer information that was once very difficult and prohibitively expensive to ascertain, catalogue, and recall is available to companies at the click of a button. Not only that, but the collecting company can share consumer information with other companies even more easily than it can initially collect the information. Today, with the widespread use of smartphone and location-enabled tablet devices, it is possible for location services to determine and plot the location and travel of the device and thereby the travel and habits of the owner. Companies can use the collected customer information to sell products, and they can sell the information to third parties for a variety of both benign and malicious purposes. Meanwhile, skilled hackers can steal consumer information.

After analyzing the current legal landscape of consumer privacy law as it relates to geolocation services, this Note argues that US and global consumers need the United States to act. In order to foster trust in corporations and the market, Congress should enact a framework that assures consumers of sufficient protection of those details that consumers hold intrinsically private, such as their personal locations. This Note concludes by examining the bills currently under consideration by Congress and their respective deficiencies.

TABLE OF CONTENTS

The reality of our modern, wireless world is that the sharing of information, particularly that of your geographical location (geolocation) data, occurs every day.[1] In other words, like it or not, if you have not opted out of being tracked by your smartphone or tablet on every single app that uses geolocation, and to a certain extent even if you have, your device is tracking you.[2] Every time you make a location request or run many popular apps, your device records where you are.[3] There are no current laws that restrict the possible uses of

1. *See infra* Part I.C.
2. *See infra* Part I.A–C.
3. *See* Daniel Ionescu, *Geolocation 101: How It Works, the Apps, and Your Privacy*, PC WORLD (Mar. 29, 2010, 7:45 PM), http://www.pcworld.com/article/192803/geolo.html.

this information, so the corporations that acquire such information are at liberty to use it as they see fit.[4]

This Note argues that Congress should enact a statutory landscape that would preempt both state and tort regulation in favor of a uniform protection regime. That regime should inform consumers of the information being collected, provide consumers the option to specifically and conveniently opt out of the data collection, and enable consumers to monitor and delete their geolocation data whenever they choose. Additionally, this Note suggests that if a company violates its statutory obligations, it should be subject to civil damages through class action suits brought by private citizens against infringers. To support this conclusion, Part I provides a brief introduction to the mechanics of geolocation tracking and the overarching legal concepts of privacy. Part II explains why a lack of regulation is concerning and introduces the two sets of privacy principles that are most prevalent in the area of consumer privacy law: those of the Federal Trade Commission and those of the American Institution of Certified Public Accountants. Part III supplies the elements of a solution built upon openness to consumers and a strong enforcement mechanism provided by private class actions. Part IV concludes with an analysis of current bills under consideration by Congress and a discussion of their relative strengths and deficiencies.

I. BACKGROUND

Not so long ago, wireless mobile devices simply made and received phone calls.[5] Those simple devices have been replaced by the modern smartphone,[6] as well as the location-enabled tablet,[7] which

4. *See In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865, at *9, *46 (N.D. Cal. Sept. 20, 2011) (holding that plaintiffs lacked standing to sue Apple for collecting and using customers' personal data without the customers' consent or knowledge).

5. Dana B. Rosenfeld & Matthew P. Sullivan, *Legal Growing Pains in the Mobile App Market*, METROPOLITAN CORP. COUNS., 13 (Sept. 1, 2011), http://www.metrocorpcounsel.com/pdf/2011/September/13.pdf.

6. *See Smartphone*, PCMAG.COM ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia (search "smartphone") (last visited Feb. 19, 2013) ("[A smartphone is a] cellular telephone with built-in applications and Internet access. In addition to digital voice service, modern smartphones provide text messaging, e-mail, Web browsing, still and video cameras, MP3 player, and video playback and calling. . . . [S]martphones run myriad free and paid applications, turning the once single-minded cellphone into a mobile personal computer."); *see also* Joe McKendrick, *Milestone: More Smartphones than PCs Sold in 2011*, SMARTPLANET.COM (Feb. 4, 2012, 5:00 AM), http://www.smartplanet.com/blog/business-brains/milestone-more-smartphones-than-pcs-sold-in-2011/21828.

7. As the technology that supports the services grows less intrusive and requires less power from the battery of a device, geolocation services are being integrated into a wide variety of devices in which they have not previously been seen. *See* Matthew Schwartz, *Anonymous Hacker Girlfriend Pictures Revealed Much, Police Say*, INFORMATIONWEEK SECURITY (Apr. 16,

today comprise the backbone of a wholly new market based on mobile applications (apps).[8] Many of these apps, as well as the devices on which they operate, track the user.[9]

A. Apps and Geolocation-Tracking Utilities

Using mobile apps, consumers can make full use of the combination of mobile broadband and Web-based content, and mobile apps represent an area of high growth for the wireless-telecommunications industry.[10] More recently, however, mobile apps have attracted scrutiny from legislators, regulators, and the consumer-protection bar due to privacy concerns and claims of undisclosed charges.[11]

It is possible to ascertain the precise geolocation of individual devices, and thereby the location of the users to whom the devices belong, through several technological methods.[12] First, all modern smartphones contain a global positioning system (GPS) chip that permits the user, on a relatively clear day, to ascertain his location.[13] Second, it is possible for network carriers and geolocation apps to triangulate the location of a mobile device using time-stamped information broadcast from known cell towers.[14] This type of geolocation system, however, is usually only accurate to 200–1000 meters; thus it serves as a contingency option to the other geolocation systems.[15] The Federal Communications Commission (FCC) requires all telecommunication carriers to provide this service in order to locate users in the event of an emergency.[16] This

---

2012, 10:50 AM), www.informationweek.com/security/government/anonymous-hacker-girlfriend-pictures-rev/232900329. These devices now include tablets and cameras and are rapidly expanding. *Id.*

8. Rosenfeld & Sullivan, *supra* note 5.

9. *See infra* Part I.A–C.

10. Rosenfeld & Sullivan, *supra* note 5.

11. *See, e.g.*, Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); ANN CAVOUKIAN & KIM CAMERON, INFO. & PRIVACY COMM'R OF CANADA, WI-FI POSITIONING SYSTEMS: BEWARE OF UNINTENDED CONSEQUENCES: ISSUES INVOLVING THE UNFORESEEN USES OF PRE-EXISTING ARCHITECTURE 8 (2011), http://privacybydesign.ca/content/ uploads/2011/06/wi-fi.pdf.

12. Ionescu, *supra* note 3.

13. *See In re* United States *ex rel.* Historical Cell Site Data, 747 F. Supp. 2d 827, 831–33 (S.D. Tex. 2010); Ionescu, *supra* note 3.

14. *Historical Cell Site Data*, 747 F. Supp. 2d at 831–33; Ionescu, *supra* note 3.

15. *How It Works*, SKYHOOK, http://www.skyhookwireless.com/howitworks (last visited Oct. 20, 2011).

16. *See* FTC, PUBLIC WORKSHOP: THE MOBILE WIRELESS WEB, DATA SERVICES AND BEYOND: EMERGING TECHNOLOGIES AND CONSUMER ISSUES 9 (2002), http://www.ftc.gov/bcp/reports/wirelesssummary.pdf; Geoffrey D. Smith, Note, *Private Eyes Are Watching You: With the*

technology is growing ever more accurate with the implementation of microcell base stations and "Location Measurement Units," which more precisely triangulate a user's geolocation,[17] but it remains under the control of telecommunication carriers.[18] A third, newer, and far more discreet method, however, is that used in the apps created by Google, Apple, and Skyhook for use in the Android and iPhone systems,[19] the two reigning systems in the smartphone market.[20] This method is called WiFi Positioning System (WPS).[21]

B. WiFi Positioning System

WPS offers many advantages to mobile devices, leading to a sharp increase in its implementation in the past few years.[22] In urban areas, satellite-based GPS is much weaker, meaning both that location finding is more difficult[23] and that GPS places a much heavier strain on the battery of a mobile device.[24] WiFi networks, on the other hand, tend to be more concentrated and reliable in urban areas, requiring less battery power to run the system;[25] hence, WPS is an attractive substitute for GPS.[26] Additionally, using WPS permits companies such as Apple and Google, who do not have telecommunication networks of their own, to geolocate.[27] Armed with

---

Implementation of the E-911 Mandate, Who Will Watch Every Move You Make?, 58 FED. COMM. L.J. 705, 706 (2006).

17. *Historical Cell Site Data*, 747 F. Supp. at 833–34.

18. *Id.* at 834.

19. *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J. (Apr. 22, 2011), http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

20. Rosenfeld & Sullivan, *supra* note 5.

21. CAVOUKIAN & CAMERON, *supra* note 11, at 5. Alohar Mobile is currently developing a fourth method of geolocation that is even more precise than WPS. This new method builds on the advances of WPS—using GPS systems, WiFi network catalogues, and a device's hardware (accelerometers, cameras)—in conjunction with an advanced algorithm that deduces a device's likely location (e.g., if travelling at a walking speed, then the sidewalk; if travelling at a driving speed, on the roadway). *See* Rafe Needleman, *Cool or Creepy? Alohar Tracks Your Location, Always*, CNET.COM (June 2, 2012, 6:00 AM), http://news.cnet.com/8301-32973_3-57445927-296.

22. *See* Rosenfeld & Sullivan, *supra* note 5.

23. *See* Skyhook Wireless, Inc. v. Google, Inc., No. SUCV2010-03652-BLS2, 2010 Mass. Super. LEXIS 362, at *2–3 (Super. Ct. Dec. 2, 2010); CAVOUKIAN & CAMERON, *supra* note 11, at 5.

24. CAVOUKIAN & CAMERON, *supra* note 11, at 5.

25. *See How It Works*, *supra* note 15.

26. *Id.*

27. CAVOUKIAN & CAMERON, *supra* note 11, at 5.

information about the habits and lifestyles of smartphone users, these companies can more effectively market their products.[28]

The operation of WPS has two stages.[29] First, a company must index the Media Access Control (MAC) address assigned to the real physical equipment that emits the WiFi network, along with the associated location of the address.[30] Some systems also collect the Service Set Identifier (SSID) of the router,[31] but the SSID is only sometimes indexed, as a network manager may disable it.[32] Second, the mobile device seeking to identify its location sends out a signal, receives signals containing MAC addresses from all networks in range, compiles the information, and sends everything to the WPS database of the parent company.[33] Finally, the WPS database returns the location of the WiFi networks and, using the known location of the WiFi networks and their relative signal strengths, the mobile device calculates its geolocation.[34]

To make the system work, any geolocation provider must first compile an index of MAC addresses (and SSIDs) through a process called "wardriving."[35] This process consists of sending a computer, usually by car, throughout an area in order to probe for WiFi networks, index the addresses, associate the MAC and SSID with the specific geographical location, record the signal strength, and finally upload the information to a central database.[36] Google's "street cars"

---

28. John Terauds, *Why Some Traffic Apps Are a Two-Way Street*, TORONTO STAR (Sept. 2, 2011), http://www.thestar.com/wheels/article/1048298.

29. Skyhook's system is the prototypical WPS, in part because Skyhook was the first major company to start wardriving and WPS services, but also because Apple implemented Skyhook's system in connection with iPhone apps until Apple developed its own system in July 2010. *See Who We Are: Company Overview*, SKYHOOK, http://www.skyhookwireless.com/whoweare (last visited Nov. 5, 2011). This Note details Skyhook's processes, but Google and Apple's systems vary inconsequentially from Skyhook's system. *See* Spencer E. Ante, *Skyhook Loses a Big Fish—Apple*, WALL ST. J. BLOG (July 30, 2010, 9:44 PM), http://blogs.wsj.com/digits/2010/07/30.

30. CAVOUKIAN & CAMERON, *supra* note 11, at 6.

31. The SSID is a unique ID given to a wireless network. *SSID*, TECHTERMS.COM, http://www.techterms.com/definition/ssid (last visited Jan. 8, 2012). It consists of thirty-two characters and is used to ensure, where multiple wireless devices overlap in a given location, that data is sent to the correct location. *Id.*

32. *See id.*

33. Nils Ole Tippenhauer et al., *Attacks on Public WLAN-Based Positioning Systems*, SYS. SECURITY GROUP, 2 (2009), http://www.syssec.ethz.ch/research/tippenhauer08attacks. pdf.

34. *Id.*; *see supra* note 21 (describing the Alohar system's algorithmic improvement on WPS).

35. CAVOUKIAN & CAMERON, *supra* note 11, at 6. Alternatively, a company can simply buy the database from another company that has already undertaken the "wardriving" process. *See* Ante, *supra* note 29. Prior to creating its own database, Apple purchased technology and indexes from Skyhook and Google. *Id.*

36. CAVOUKIAN & CAMERON, *supra* note 11, at 6.

were on just such a mission in 2010 when they "inadvertently" intercepted and recorded information transmitted over unencrypted networks.[37] The information, which Google claims was collected due to a programming error, included personal information and sensitive data, such as email addresses and passwords.[38]

At first glance, Apple and Google's utilization of the WPS geolocation-tracking system seems harmless.[39] The companies are simply supplying individuals with their locations when they so desire.[40] Recent revelations, however, strongly suggest that Apple's and Google's systems do not merely provide mobile-device users with their locations; rather, both operating systems are set to save the geolocation data of the mobile devices and to transmit the data back to the respective company's database.[41] In other words, both of these companies have a log of the precise geolocation of a particular device every time its users make a WPS geolocation request.[42]

Additionally, a large percentage of the apps running on both Android and iOS mobile platforms transmit geolocation information to Google or Apple and to app companies without the customer's knowledge or consent.[43] Even more perturbing, some apps transmit geolocation information to third-party companies.[44] In 2010, the *Wall Street Journal* completed a study regarding how frequently such transmission to third-party companies occurs.[45] From a cross section of 101 apps, including such popular apps as Angry Birds and Pandora, the *Journal* discovered that some fifty-six had, without the user's awareness, transmitted a mobile device's unique ID to other

37. Harry McCracken, *Google: The Accidental Spy*, PC WORLD (May 14, 2010, 5:35 PM), http://www.pcworld.com/article/196379; *see also* Angwin & Valentino-Devries, *supra* note 19.

38. *See* Angwin & Valentino-Devries, *supra* note 19.

39. *See* Rosenfeld & Sullivan, *supra* note 5.

40. *Id.*

41. *See* Skyhook Wireless, Inc. v. Google, Inc., No. SUCV2010-03652-BLS2, 2010 Mass. Super. LEXIS 362, at *2-4 (Super. Ct. Dec. 2, 2010); Angwin & Valentino-Devries, *supra* note 19. Android phones determine "location every few seconds and transmit[] the data to Google at least several times an hour," while the iPhone saves the information in a file that is transmitted to Apple's servers every twelve hours. Angwin & Valentino-Devries, *supra* note 19.

42. *See* Angwin & Valentino-Devries, *supra* note 19; Andrew Munchbach, *Apple Stealthily Recording, Storing GPS Position of iPhone, 3G iPad Users [Video]*, BGR.COM (Apr. 20, 2011), http://www.bgr.com/2011/04/20/apple-recording-storing-gps-position-of-iphone-3g-ipad-users-video.

43. Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J. (Dec. 18, 2010), http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

44. *See id.*; *see also* Eric Smith, *iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)*, PSKL BLOG (Sept. 30, 2010), http://www.pskl.us/wp/?p=476.

45. Thurm & Kane, *supra* note 43.

companies.[46] Additionally, the report found that "[f]orty-seven apps transmitted the phone's location in some way," and "[f]ive sent age, gender and other personal details to outsiders."[47] Additionally, a program called Clueful, recently developed by Bitdefender,[48] compiled a cross section of all mobile apps by conducting an audit of applications running in the memory of iPhones.[49] Of the devices that downloaded the program, Clueful determined that 41 percent of the apps studied could track users' locations, while 18.6 percent of apps could access all contact information in the address books of the user devices.[50] It seems obvious that, while WPS has many advantages, with so many apps collecting personal data, the potential for abuse is considerable.[51]

C. Geolocation Data Uses

Once a company has collected geolocation data, there are two primary uses for the data, each with its own privacy concerns.[52] First, the collecting company may use the data in-house.[53] In-house usage of private consumer data in order to improve consumer services or products is a technique already implemented by major players in today's consumer markets.[54] An excellent example is Netflix's website, which uses the data submitted by the consumer and information from numerous other consumers, in the form of ratings, to make recommendations to viewers for future rentals or purchases.[55]

---

46. *Id.*

47. *Id.*

48. Clueful was available from the Appstore from May 2012 to July 2012, when Apple blocked it. Bitdefender relaunched Clueful on August 27, 2012, with new features, this time at no cost to users. *Bitdefender Relaunches Clueful as Free Social Web-Guide on iOS App Behavior*, BITDEFENDER (Aug. 27, 2012), http://www.bitdefender.com/news/bitdefender-relaunches-clueful-as-free-social-web-guide-on-ios-app-behavior-2568.html.

49. Dan Rowinski, *Apple Won't Let You See What iPhone Apps Do with Your Data*, READWRITE (July 20, 2012), http://www.readwriteweb.com/mobile/2012/07/apple-wont-let-you-see-what-iphone-apps-do-with-your-data.php.

50. *Id.*

51. *See id.*

52. *See* discussion *infra* Part I.C.

53. Amazon, iTunes, Bloglines, NYTimes, and Netflix all utilize customer information to recommend additional products or services that may be of interest to the customer. Joshua Porter, *Which Movie to Watch? An Overview of Recommendation Systems*, BOKARDO BLOG, http://bokardo.com/archives/quick-overview-of-recommendation-systems (last visited Dec. 20, 2012).

54. *Id.*

55. Laurie J. Flynn, *Like This? You'll Hate That. (Not All Web Recommendations Are Welcome.)*, N.Y. TIMES (Jan. 23, 2006), http://www.nytimes.com/2006/01/23/technology/23recommend.html; Todd Yellin, *More Accurate Star Predictions*, NETFLIX U.S. & CANADA BLOG (May 7, 2009, 2:51 PM), http://blog.netflix.com/2009/05/more-accurate-star-predictions.html.

The Netflix website recommends roughly two-thirds of all Netflix rentals.[56]

Megacorporations, such as Google and Apple, also collect and use data derived from WPS.[57] Indeed, Google announced on January 24, 2012, that it would begin to track users even more closely and would be combining the information from across its websites and services in order to compile a more complete in-house profile of Google users.[58] The changes, complete with changes to Google's privacy policy for its users, took effect on March 1, 2012.[59] Consumers cannot opt out of these changes.[60]

Second, and even more of a red flag to privacy advocates and wary consumers,[61] companies sell geolocation data to third-party companies and individuals.[62] These third parties include employers, banks, marketers, and potentially even law enforcement.[63] The consumer often has no relationship to the third party that purchases the information, the collecting company never alerts the consumer that it distributed personal geolocation data to the third party, and the consumer is unable to determine which company initially ascertained and sold his personal information to the third party.[64] The third party anonymously and surreptitiously purchases what may be a surprisingly vast amount of information about the consumer.[65] The collected information of any one company may be aggregated with private information possessed by other companies to create a digital profile of individuals, one that is particularly powerful if it contains geolocation data.[66] For example, in *Pineda v. Williams-Sonoma Stores, Inc.*, the defendant store used a customer's zip code to perform

---

56. Flynn, *supra* note 55.

57. *See* Cecilia Kang, *Google Announces Privacy Changes Across Products; Users Can't Opt Out*, WASH. POST. (Jan. 24, 2012), http://articles.washingtonpost.com/2012-01-24/business/35440035_1_google-web-sites-privacy-policies.

58. *Id.*

59. *Id.*

60. *Id.*

61. Bob Sullivan, *Online Privacy Fears Are Real: More People Are Tracking You than You Think*, MSNBC.COM (Dec. 6, 2011), http://www.msnbc.msn.com/id/3078835.

62. *See* FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 45–47 (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter SELF-REGULATORY PRINCIPLES].

63. FED. TRADE COMM'N, PERSONAL DATA ECOSYSTEM, http://www.ftc.gov/bcp/workshops/privacyroundtables/personalDataEcosystem.pdf (last visited Feb. 2, 2012).

64. *See* Sullivan, *supra* note 61.

65. *See id.*

66. *See* Miguel Helft & Tanzina Vega, *Seeing That Ad on Every Site? You're Right. It's Tracking You.*, N.Y. TIMES, Aug. 30, 2010, at B2; *see also* Kang, *supra* note 57. The collection of geolocation data is particularly concerning because it often contains a detailed history about travel and behavioral patterns. Sullivan, *supra* note 61.

a reverse search in an attempt to match her name with her previously undisclosed addresses.[67] The store saved the matched information in its databases for future use and potential sale to third parties.[68] The California Supreme Court determined that recording customer zip codes violated the 1971 California Credit Card Act as it constituted the storing of "personal information."[69]

A company's ability to aggregate data obtained from multiple sources can be detrimental to consumers. It is possible, for example, to combine geolocation data with sales receipts to determine a consumer's preferences, especially when choosing between different sales outlets, or even between items within a particular store.[70] Indeed, the market's push for such a compilation of personal data has increased dramatically over the past decade due to the vacuum left by the gradual decline of mass advertising.[71] Media companies are under increasing pressure to attract and target more specific audiences.[72] As there are fewer and fewer "views" or "listens" to particular advertisements, marketers remaining in the advertising market must increasingly personalize their advertisements to remain lucrative.[73] The use of geolocation data comprises a substantial part of the push of media companies and app makers to improve their bottom line.[74]

II. LEGAL BACKGROUND

While this Note will not argue that privacy law should protect consumers from geolocation data misappropriation, it is imperative to undertake a brief examination of the history of privacy law in order to determine why the current privacy-law-based scheme does not adequately protect consumers.

---

67. Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612, 615 (Cal. 2011).

68. *Id.*

69. *Id.* at 614–15. The California Credit Card Act prohibits such collection of "personal information," a category the *Pineda* court declared included zip codes. CAL. CIV. CODE § 1798.82 (West 2012); *Pineda*, 246 P.3d at 615.

70. It is theoretically possible to track this information, but there is no evidence any company has done so. This Note merely suggests this as a hypothetical future use for geolocation data, as more accurate systems are developed. *See* Needleman, *supra* note 21.

71. Louise Story, *The Higher Value of Eyeballs*, N.Y. TIMES (Nov. 5, 2007), http://www.nytimes.com/2007/11/05/technology/05bits.html.

72. *Id.*

73. *Id.*

74. *See* CAVOUKIAN & CAMERON, *supra* note 11, at 5.

A. Warren and Brandeis's "Right to Privacy"

US privacy law traces its origin to the landmark law journal article by Samuel Warren and Louis Brandeis, entitled "The Right to Privacy," published in the *Harvard Law Review*.[75] Warren and Brandeis lamented the fact that the instant photograph had the potential to allow the press to transgress "in every direction the obvious bounds of propriety and of decency,"[76] allowing an individual's private life to be on display for all (or at least the highest bidder).[77] They defined the right to privacy as the "right to be let alone,"[78] establishing two foundational rights of privacy: the right of private individuals to be protected from harmful uses of their private information and the right of private citizens to be free from government invasion of privacy.[79] The modern framework of privacy protection derives from these two rights, particularly as relates to the conceptions of solitude, independence, and personal autonomy.[80]

B. Tort Regulation of Privacy

Even after Warren and Brandeis's formative work, the individual is responsible for protecting his privacy,[81] either by preventing others from intruding into his private life or by bringing a tort claim against an offender.[82] The primary framework of legal sanction, protection, and remedy developed in tort law.[83] Three private torts emerged in the courts[84]: "(1) the tort of unreasonable intrusion into the seclusion of another, (2) the tort of unreasonable publicity given to the other's private life, and (3) the tort of publicity that unreasonably places the other in a false light before the public."[85]

The torts add little protection and are not an effective manner of protecting consumer privacy in the digital age. The first tort

---

75. Smith, *supra* note 16.

76. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

77. *See id.* at 195.

78. *Id.* at 193.

79. Smith, *supra* note 16, at 708.

80. *Id.*

81. ANN CAVOUKIAN, PRIVACY BY DESIGN IN LAW, POLICY AND PRACTICE: A WHITE PAPER FOR REGULATORS, DECISION-MAKERS AND POLICY-MAKERS 7 (2011), *available at* http://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf.

82. *Id.*

83. Smith, *supra* note 16, at 708.

84. RESTATEMENT (SECOND) OF TORTS § 652A (1977); *see also* Phillips v. Smalley Maint. Servs., Inc., 435 So. 2d 705, 706 (Ala. 1983).

85. Smith, *supra* note 16, at 708.

requires the plaintiff to prove an intrusion of his solitude,[86] meaning that an individual must first have a reasonable expectation of privacy given the setting and circumstances and that the intrusion must be highly offensive to a reasonable person.[87] But, if an individual is in a public place where public observation is possible, on a public highway for example, courts in most cases find no liability.[88] The second tort—that of true statements receiving a level of publicity that would be highly offensive to a reasonable person and are not of legitimate public concern—has never been fully resolved with the free-speech and free-press provisions of the First Amendment.[89] The US Supreme Court has clearly held that information about events that occur within an individual's home, such as his intimate relations, is actionable if publicized.[90] The problem is that the information must be *publicized*, something that rarely, if ever, occurs with geolocation data. The third tort is, in essence, a stronger version of a defamation claim.[91] Defamation is rarely an issue for geolocation data, as there is no untruth nor is there normally widespread distribution of the information contained in the data.

C. Protection from Intrusion by the Government

In addition to the right to be protected from harmful uses of their private information, individuals have the right to be free from government intrusions.[92] Although courts have developed many factors in determining whether the tracking of citizens is an intrusion, there are two primary tests formulated by the Supreme Court in *Katz v. United States*.[93] First, the majority in *Katz* established an objective test considering whether the individual had a reasonable expectation of privacy, given his actions.[94] Second, Justice Harlan, in his concurrence, posited that a better test would include a subjective element in addition to the objective, asking whether the defendant exhibited an actual and reasonable expectation of privacy.[95] These

86. *See* RESTATEMENT (SECOND) OF TORTS § 652B.

87. *See id.* § 652B cmt. a.

88. *See id.* § 652B cmt. c.

89. U.S. CONST. amend. I; RESTATEMENT (SECOND) OF TORTS § 652D.

90. RESTATEMENT (SECOND) OF TORTS § 652D cmt. c.

91. *See id.* § 652E cmt. b.

92. Fred H. Cate, *The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It*, 4 FIRST REP. 1, 4 (Mar. 2003), http://www.thefreepress.net/PDF/FirstReport.privacyproblem.pdf; Stephen A. Josey, Note, *Along for the Ride: GPS and the Fourth Amendment*, 14 VAND. J. ENT. & TECH. L. 161, 164 (2011).

93. Katz v. United States, 389 U.S. 347 (1967).

94. *Id.* at 351.

95. *Id.* at 361 (Harlan, J., concurring).

two tests, selectively used by subsequent courts, eventually spawned the Open Fields Doctrine and the limitation on the use of technological aids in surveilling an individual.[96]

The Open Fields Doctrine suggests that an individual may not demand privacy from the government for actions conducted out of doors (or in the "open fields"), with the exception of conduct in and around the area of the home.[97] In order to receive protection, an individual must withdraw from the public view into an area where he has a reasonable expectation of privacy, such as his home.[98]

The limitation on the use of certain technological aids creates an intrusion of privacy if the government utilizes technology to glean information that it could not have obtained through other legitimate means.[99] For example, in *United States v. Karo*, the Supreme Court held that a radio beeper hidden on property "withdrawn from the public view" would be an intrusion of the privacy interests of the home too great to be sustained under the Fourth Amendment.[100] In effect, the technology would enable the state to enter a realm that it otherwise could not.[101]

Despite the considerable jurisprudence on government use of geolocation data, none of those cases extend to the private sphere, as the Fourth Amendment provides protection only against government actors. As companies are not government actors, Congress must enact a regulatory scheme that will protect individuals from not only governmental entities, but also private entities.

III. LEGAL ANALYSIS

The modern wired world has changed the way we behave and interact considerably, particularly with the advent of geolocation technologies, as the private sphere has become capable of tracking individuals in new and novel ways.[102] Private companies can now silently and effortlessly acquire information electronically that previously only the government could have obtained through a

96. *See, e.g.*, United States v. Karo, 468 U.S. 705, 706 (1984) (discussing the two relevant tests); Josey, *supra* note 92, at 164–66.

97. *See* Oliver v. United States, 466 U.S. 170, 178 (1984) (discussing and implementing the Open Fields Doctrine).

98. *See id.*

99. *Karo*, 468 U.S. at 716; *see also* United States v. Jones, 132 S. Ct. 945, 946–47 (2012).

100. *Karo*, 468 U.S. at 716; *see* Josey, *supra* note 92, at 169.

101. Josey, *supra* note 92, at 169.

102. Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35, 61 (2002).

government investigator persistently tailing an individual.[103] The private sector now has the monitoring capabilities of the government yet without concomitant Fourth Amendment safeguards.[104]

A. Consumer Concern Regarding Tracking through Geolocation Systems

There seems to be a common question voiced by some young consumers, who are most active on the Internet and therefore most affected by any abuses[105]: Why does it matter that companies are collecting the geolocation data of their customers, particularly when consumers benefit from technological advances that geolocation systems bring? The answer: money, power, and misuse.[106]

Geolocation information reveals the mobile-device user's work habits, travel patterns, and precise physical location at any given moment.[107] Over time, market actors can aggregate a comprehensive profile of a person, and with such information, the market actors gain great advantage through both use and misuse. One need not be too creative to imagine the blackmail potential a company with access to such a profile would hold over the average citizen, much less a board member for a Fortune-500 company, a judge presiding over a shareholder suit against a major market actor, or a politician.

Companies such as Google and Apple that acquire geolocation information could also sell or license the information to third parties.[108] The third party could employ the geolocation data to advertise directly to the owner of a mobile device based upon the owner's daily route to work or apparent recreational patterns; however, the third party's use could also be far less benign.[109] For example, a sales company could buy the geolocation records for a salesman of a competing company and then use that information to recreate the competing company's customer list,[110] something that

103. ANDREW L. SHAPIRO, THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 158 (1999).

104. *Id.*

105. Press Release, Harris Interactive, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles (Apr. 10, 2008), http://www.harris interactive.com/vault/Harris-Interactive-Poll-Research-Majority-Uncomfortable-with-Websites-Customizing-C-2008-04.pdf [hereinafter Harris Interactive Press Release].

106. *See infra* notes 108–133 and accompanying text.

107. *See supra* Part I.A–C.

108. Rosenfeld & Sullivan, *supra* note 5.

109. *See* Smith, *supra* note 16, at 713–14.

110. *Id.* at 714.

could be protected as a trade secret.[111] Alternatively, an employer could deny an employment applicant because the employer discovered through purchased geolocation data that the applicant frequented an AIDS clinic or perhaps a childcare center in the past few months.[112] The amount of private information that would literally be up for sale to the highest bidder could be considerable.[113]

Another concern is security of the data.[114] Although Google and Apple may claim to take the greatest precautions in securing their data, two recent breaches of security of the Sony PlayStation 3 system, in which unknown sources obtained considerable online-subscriber information,[115] should give consumers pause. The first hack occurred in April 2011.[116] Criminal hackers accessed sensitive information, including the credit card numbers, of seventy-seven million customers.[117] Next, in October 2011, hackers infiltrated over ninety-three thousand accounts.[118] Despite heightened security, once hacked, even a megacorporation like Sony may not be able to keep sensitive information safe.[119] Furthermore, although Google and Apple would not likely misuse the information, the same may not be the case for a blackmailer, an individual seeking to quiet minority political viewpoints, or a stalker.[120] Finally, the Sony hack belies the assumption that information collected but maintained with anonymity is of little value to a hacker.[121]

Despite the great risk and potential for abuse, an increasing number of major companies are offering services or programs that

111. *See* Stampede Tool Warehouse, Inc. v. May, 651 N.E.2d 209, 215–16 (Ill. App. Ct. 1995) (holding that a customer list was a trade secret under an Illinois statute modeled closely after the common-law factors).

112. Smith, *supra* note 16, at 714.

113. *See id.*

114. Press Release, KPMG, KPMG Survey: U.S. Consumers Believe Mobile Banking Is Important but Security, Privacy, and Cost Cited as Major Barriers to Mass Adoption (Apr. 8, 2009), http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Press-Releases/Documents/mobile-banking.pdf [hereinafter KPMG Press Release].

115. Philip Reitinger, *An Important Message from Sony's Chief Information Security Officer*, PLAYSTATION.BLOG (Oct. 11, 2011), http://blog.us.playstation.com/2011/10/11.

116. Charles Arthur & Keith Stuart, *PlayStation Network Users Fear Identity Theft after Major Data Leak*, GUARDIAN (Apr. 27, 2011, 3:59 PM), http://www.guardian.co.uk/technology/2011/apr/27/playstation-users-identity-theft-data-leak.

117. *Id.*

118. Reitinger, *supra* note 115.

119. *See id.*

120. This is not intended as a critique of Google's, Apple's, or Sony's security measures but rather to highlight the concern that once data is created, it is at risk of misuse, even when protected by highly sophisticated companies.

121. *See* Reitinger, *supra* note 115.

utilize geolocation data.[122] As these services have become more prolific, consumers have grown increasingly concerned.[123] In one study undertaken jointly by the University of Pennsylvania and the University of California-Berkeley, the majority of the participants wrongly believed that current laws restrict companies from selling general information about them.[124] When asked if there should be a law requiring websites and advertising companies to delete all stored information about an individual, if requested to do so, 92 percent of participants responded affirmatively.[125] A majority (66 percent) opposed the use of the information to tailor advertisements to them, even when told that tracking would occur anonymously.[126]

Additionally, Americans exhibit a lack of trust regarding privacy and their mobile devices.[127] In a study of more than four thousand smartphone and mobile-device users, KPMG found that more than 87 percent of US users surveyed harbor concerns about privacy and security regarding banking on their phones.[128] Also, in a 2010 study conducted by Webroot, which surveyed one-thousand-five-hundred social-network users owning geolocation-ready devices, 55 percent of the participants expressed fear regarding a loss of privacy through geolocation apps on their mobile devices.[129] Forty-six percent of the women surveyed were "highly concerned" about stalkers getting the information,[130] and some 45 percent of participants were "highly concerned" about letting a

122. In 2010, Facebook, Twitter, and Google all launched their own "Places" services and products with features to allow individuals to "check" themselves into a restaurant and discover content. Janet Jaiswal & Saira Nayak, *Location-Aware Mobile Applications: Privacy Concerns & Best Practices*, TRUSTE (2010), http://www.truste.com/pdf/Location_Aware_Mobile_Applications.pdf. Other popular location-based social-networking services include BrightKite, Foursquare, Gowalla, Loopt, Whrrl, and Yelp!. *Location, Location, Location: A Primer on Location-Based Social Network Marketing*, 4IMPRINT.COM (2011), http://info.4imprint.com/wp-content/uploads/1P-02-0111-Jan-2011-Blue-Paper-Geolocation.pdf.

123. *See* Joseph Turow et al., *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* 3 (2009), http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

124. *Id.* at 4.

125. *Id.* at 3.

126. *Id.*

127. KPMG Press Release, *supra* note 114.

128. *Id.*

129. Press Release, Webroot, Webroot Survey Finds Geolocation Apps Prevalent amongst Mobile Device Users, but 55% Concerned about Loss of Privacy (July 13, 2010), http://www.webroot.com/En_US/pr/threat-research/cons/social-networks-mobile-security-071310.html [hereinafter Webroot Press Release].

130. Josh Halliday, *People Worry About Over-Sharing Location from Mobiles, Study Finds*, GUARDIAN TECH. BLOG (July 12, 2010, 2:00 PM), http://www.guardian.co.uk/technology/blog/2010/jul/12/geolocation-foursquare-gowalla-privacy-concerns.

potential burglar know when they are away from home.[131] The high level of consumer concern likely translates into a loss of sales and a hesitancy to engage fully and efficiently in market interactions,[132] particularly among women and older generations.[133]

B. Absence of Legal Protection and the Winds of Change

Contrary to popular consumer belief,[134] current federal law permits companies, such as Skyhook, Google, Apple, and other app makers, to collect geolocation data and share it with third parties without obtaining prior consent from, or even notifying, their customers.[135] This collection and sale are probably not subject to tort liability[136] because the typical collection and sale of geolocation data is accomplished without unreasonably intruding on the seclusion of a customer, without ever publicizing anything, and without the false portrayal of any information.[137]

Fortunately, the winds of consumer protection in the United States are beginning to shift, if only for Google customers.[138] The change is not the result of US political pressure or threatened litigation, although such pressure is growing,[139] but rather originates from foreign sources—the German and French governments and an EU data-protection directive.[140] These European governmental actors

---

131. Webroot Press Release, *supra* note 129.

132. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 2 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter FED. TRADE COMM'N 2000].

133. According to the AARP, "24% of computer users age 45 and over who have never purchased online cite privacy as the key reason." *Id.* at 41 n.15 (citation omitted).

134. *See* Turow et al, *supra* note 123, at 4.

135. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. § 2702 (2006).

136. *See, e.g.*, *In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865, at *46 (N.D. Cal. Sept. 20, 2011).

137. WPS and GPS tracking do not necessarily intrude on an individual's seclusion, as the information concerns a person's movements, which often occur on public roads where there is no reasonable expectation of seclusion. *See supra* Part II.B. If this information is true and not put in the public sphere, it may be sold to a third-party advertiser without implicating any common-law tort. *See supra* Part II.B.

138. *See* Cyrus Farivar, *Google Bends to European Privacy Worries with WiFi Opt-Out Plan*, DEUTSCHE WELLE (Sept. 14, 2011), http://www.dw.de/google-bends-to-european-privacy-worries-with-wifi-opt-out-plan/a-15387075; Kevin J. O'Brien, *Google Offers More Privacy to Avert Clash with E.U.*, INT'L HERALD TRIB. (Sept. 14, 2011), http://www.highbeam.com/doc/1P1-197631044.html (discussing Google's efforts to avoid potential liability for privacy intrusion within the European Union).

139. *See supra* Part II.A.

140. *See* Farivar, *supra* note 138; *see also* Council Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and

have determined that participation in the collection of consumer geolocation data must be voluntary.[141] In response, largely due to the importance of the European market to Google's Android sales, which is now the most popular operating system on new cell phone shipments,[142] Google has announced it will create an opt-out option of geolocation services for WiFi providers worldwide.[143] Once a wireless network host has opted out, Google will not utilize the access point to determine user locations.[144] Apple and other app makers have yet to make any similar opt-out allowances.

As believed by some privacy advocates, however, Google's modest changes, even if adopted industry-wide, are insufficient,[145] especially given recent statements from Google announcing more consumer data collection and less consumer choice.[146] Although WiFi providers may deny Google the privilege of using their access point to geolocate mobile devices, consumers still cannot opt out of geolocation or data sharing with third parties.[147] The United States, the world's technology leader and home to both Google and Apple, should do more to strike a balance between fostering technological advancement and mitigating unwanted commercial intrusion into the lives of consumers.

C. Self-Regulation Disclosure Frameworks

A potential solution to the disclosure deficit is an effective and broad self-regulatory framework. Two such frameworks have been proposed: the Federal Trade Commission's (FTC) Fair Information Practice Principles (FTC Principles) and the Generally Accepted Privacy Principles, as formulated by the American Institute of Certified Public Accountants.

1. FTC Self-Regulation–Disclosure Framework

The FTC has been very active in its attempts to promote consumer privacy by issuing a series of guidelines for private

---

Electronic Communications), art. 9, 2002 O.J. (L 201) 37, 45, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF.

141. Farivar, *supra* note 138.

142. Alexis Santos, *IDC: Android Claims 75 Percent of Smartphone Shipments in Q3, 136 Million Handsets Sold*, ENGADGET (Nov. 1, 2012, 10:30 PM), http://www.engadget.com/2012/11/01/android-75-percent-marketshare-136-million-shipped.

143. Farivar, *supra* note 138.

144. *Id.*

145. *See* CAVOUKIAN, *supra* note 81, at 21 n.60.

146. *See* Kang, *supra* note 57.

147. *See* Farivar, *supra* note 138.

companies.[148] Some consider § 5 of the Federal Trade Commission Act to be the best framework in current legislation for addressing privacy issues.[149] The Act itself empowers the FTC to prohibit "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[150] Under this aegis and seemingly drawing from a number of domestic and international privacy laws,[151] the FTC has formulated the Fair Information Practice Principles.[152] Within those principles, the FTC has stressed heightened protection for "personally identifiable information" (PII),[153] which includes "information that can be linked to a specific individual"[154] and encompasses "financial data, data about children, health information, *precise geographic location information*, and Social Security numbers."[155] These advisory principles, if followed, promote congruity with international laws while fostering consumer confidence.

The FTC Principles set forth five main doctrines. The first is "Notice/Awareness."[156] As mentioned above in the discussion of tort-regulation effectiveness, consumers cannot make informed decisions about their consumption practices without notice of the

148. *See* FED. TRADE COMM'N, PRELIMINARY FTC STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 39–78 (2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf [hereinafter PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE].

149. *See, e.g.*, Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 115 (2011).

150. 15 U.S.C. § 45(a)(1) (2006).

151. *See* FED. TRADE COMM'N 2000, *supra* note 132; FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), http://www.ftc.gov/reports/privacy3/priv-23a.pdf [hereinafter FED. TRADE COMM'N 1998]; THE CANADIAN STANDARDS ASS'N, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION: A NATIONAL STANDARD OF CANADA (1996); INFO. INFRASTRUCTURE TASK FORCE, INFO. POLICY COMM., PRIVACY WORKING GRP., PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (1995); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281); U.S. DEPT. OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995); ORG. FOR ECON. CO-OPERATION AND DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980); THE PRIVACY PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977).

152. PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 148, at 6–7.

153. SELF-REGULATORY PRINCIPLES, *supra* note 62, at 20.

154. *Id.* at 20 n.47.

155. *Id.* at 44 (emphasis added).

156. PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 148, at 6–7, 45–47.

disclosure of their personal information.[157] The other four principles are meaningful only to the extent consumers know of the disclosure.[158] Indeed, studies have repeatedly shown[159] that consumers want to be informed that companies are collecting their personal data, what kind of data the companies are collecting (sensitive, anonymized, etc.), how the companies are collecting it, and what the companies intend to do with it.[160]

Second is "Choice/Consent," which, according to the FTC, means, "giving consumers options as to how any personal information collected from them may be used."[161] This element of Choice/Consent most often is related to the use of information beyond that necessary to complete the transaction and typically takes the form of opt-in or opt-out.[162] The FTC does not specify the extent of the option, that is, whether it would be granular[163] as to each element of privacy or black-and-white like consumer choice in the market.[164]

Third is "Access/Participation." This principle suggests that collectors of data should grant individuals access to all of their information, so that each individual can check for completeness and accuracy.[165] The consumers should then be able to augment, correct, delete, or contest the compiled information.[166]

Fourth is "Integrity/Security," meaning that collectors of personal data should take reasonable steps to prevent its misappropriation.[167] Preventative measures include managerial and

---

157. *See supra* Part II.B.

158. PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 148, at 6–7, 45–47.

159. Julia B. Earp et al., *Examining Internet Privacy Policies Within the Context of User Privacy Values*, 52 IEEE TRANSACTIONS ON ENGINEERING MGMT. 227, 227–37 (2005), *available at* http://www4.ncsu.edu/~jbearp/IEEE_TEM_Privacy_Values.pdf.

160. Efrim Boritz et al., *Do Companies' Online Privacy Policy Disclosures Match Customer Needs?* 3 (Canadian Academic Accounting Assoc. Conference Paper, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1082961.

161. *Fair Information Practice Principles*, FED. TRADE COMM'N, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified Nov. 23, 2012).

162. *Id.*

163. As used in this note, the term "granular" is intended to refer to the most basic complete element of a system. A granular opt-out would not provide one blanket option approving or denying the collection and sharing of consumer information, but would rather require presentation of the option to opt out of tracking in certain instances. Some examples of the opt-out options on a granular level would be an opt out at each moment the service is significantly changed, any time an app begins requesting geolocation information not previously approved by the consumer, and each and every occasion of sharing geolocation information with a specified third party.

164. *See* FED. TRADE COMM'N 2000, *supra* note 132.

165. *Id.* at 29–31

166. *Id.*

167. *Id.* at 32–33.

technical procedures, organizational form, technological security systems, and fail-safes.[168] Security should adequately protect data against breaches, such as those that occurred at Sony.[169]

The fifth and final principle is "Enforcement/Redress."[170] Enforcement is the key to a successful consumer privacy regime and has traditionally been the weak link in the privacy chain.[171] Self regulation has been the most common method of enforcement, but to be meaningful it must be more concrete than mere broad policies.[172] Additional civil and criminal penalties are nonexistent.

A congressional statute based upon these five principles that establishes a cause of action that could be litigated in a class action suit would constitute the ideal method to protect consumer privacy and promote consumer confidence. Although admittedly abstract, the FTC Principles encompass all the crucial elements of an effective consumer privacy regime. If properly combined in a statutory landscape with an adequate civil remedy[173] and a focus on the provision of notice to consumers, the guidelines would provide the necessary structure to foster consumer confidence in geolocation-data collection and sharing.

2. AICPA Self-Regulation Framework

The current self-regulatory framework upheld and voluntarily followed by many companies is the Generally Accepted Privacy Principles (GAPP), as formulated by the American Institute of Certified Public Accountants (AICPA).[174] GAPP follows the five FTC Principles closely,[175] but it does not directly state them; it instead lists ten principles that companies must follow in order to protect the privacy of their customers.[176] Although fairly well articulated and structured, the regime has a problem at the point where it is most

168. *Fair Information Practice Principles*, *supra* note 161.

169. *See supra* notes 114–121 and accompanying text.

170. *Fair Information Practice Principles*, *supra* note 161.

171. *See id.*

172. NAT'L TELECOMMS. & INFO. ADMIN., ELEMENTS OF EFFECTIVE SELF-REGULATION FOR PROTECTION OF PRIVACY—DISCUSSION DRAFT (1998), *available at* http://www.ntia.doc.gov/report/1998/elements-effective-self-regulation-protection-privacy-discussion-draft.

173. *See infra* Part IV.C.

174. *Generally Accepted Privacy Principles*, AM. INST. OF CERTIFIED PUB. ACCOUNTANTS (2009), *available at* http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples (follow "Practitioner Version of GAPP" hyperlink) [hereinafter *GAPP*].

175. *See id.*; *see also Fair Information Practice Principles*, *supra* note 161.

176. *See GAPP*, *supra* note 174, at 7.

needed: enforcement.[177] Principle ten, "Monitoring and Enforcement Criteria," requires a company to enact various monitoring and enforcement mechanisms so that the company may ensure that it is properly enforcing its privacy policy,[178] but the AICPA has no means of forcing companies to comply with its standard.[179] For example, GAPP requires member companies to have "inquiry, complaint, and dispute" processes, but GAPP lists no means of punishing a company if it should choose not to comply or to only partially comply with the requirements.[180]

Recently, critics of GAPP and of self-regulation have become more outspoken. Indeed, *Wired* magazine has observed that self-regulation by the advertising industry has "conspicuously failed to make the industry more transparent about when, how, and why it collects data about internet users."[181] Several studies lend support to these statements,[182] such as one undertaken by the Berkeley School of Information.[183] In its study, Berkeley found that of twenty-two major websites[184] requesting and collecting geolocation data, none informed their users upfront that they were doing so,[185] and only three mentioned it in their privacy policies.[186] Self-regulation or not, it seems that more must be done to address geolocation-data-privacy issues.

D. Opt-in Impossibility

One potential solution is to allow consumers to opt-in rather than opt-out of data collection. If properly formulated, such a change would flip the default, making consumer privacy the norm while forcing companies to request permission to collect geolocation information in every instance they desire it. The FCC proposed a

177. *See id.* at 60–65.

178. *Id.*

179. *See id.* at iii.

180. *Id.* at 60–61.

181. Ryan Singel, *You Deleted Your Cookies? Think Again*, WIRED (Aug. 10, 2009, 7:39 PM), http://www.wired.com/business/2009/08/you-deleted-your-cookies-think-again.

182. PAM DIXON, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND AT SELF-REGULATION 39 (2007), *available at* http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf; Nick Doty et al., *Privacy Issues of the W3C Geolocation API*, UC BERKELEY SCH. OF INFO., 8–10 (Feb. 2010), http://escholarship.org/uc/item/0rp834wf.

183. *See* Doty et al., *supra* note 182, at 8–10.

184. *See id.* at 10 (providing chart of twenty-two sites, including Google Maps and Flikr).

185. *Id.*

186. *Id.*

similar opt-in solution[187] under the authority granted to it by the Telecommunications Act.[188] The Act sought to prevent telecommunications carriers from distributing customer proprietary network information (CPNI)[189] to third parties, "except as required by law or with approval of the customer."[190] As a preliminary matter, the Telecommunications Act offers no protection for consumer geolocation data, as none of the companies concerned are telecommunications carriers governed by the Act.[191]

The US Court of Appeals for the Tenth Circuit, hearing a challenge to the FCC opt-in rule,[192] found the opt-in requirement to be an unconstitutional restriction on the carrier's free-speech right to communicate with their customers,[193] asserting that rules could not be broader than is necessary to prevent "specific and significant harm" to individuals.[194] The Supreme Court denied certiorari on the decision,[195] and in response the FCC reversed course by adopting an opt-out procedure.[196] Neither Congress nor regulatory agencies have adopted an opt-in measure since. Although an opt-in technically remains a possibility, it stands on shaky constitutional grounds.[197]

IV. WORKING TOWARD A SOLUTION

Congress should bolster self regulation regarding geolocation data by enacting a statute that codifies self-regulation principles.[198]

---

187. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1230 (10th Cir. 1999).

188. 47 U.S.C. § 222 (2006).

189. *Id.* § 222(h)(1) (defining "customer proprietary network information" as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information").

190. *Id.* § 222(c)(1).

191. *See id.* § 253. The Act does not cover geolocation data as CPNI because it is other companies' programs running on a device that ascertain the data, not the carriers. Peter Schaar, *Smart Phones Always Under Control?*, FED. COMMISSIONER OF DATA PROTECTION BLOG (July 9, 2010), http://www.bfdi.bund.de/EN/PublicRelations/SpeechesAndInterviews/blog/SmartPhonesUnterKontrolle20100709.html.

192. *U.S. West*, 182 F.3d at 1230.

193. *Id.* at 1237–38.

194. *Id.* at 1235.

195. Competition Policy Inst. v. U.S. West, Inc., 530 U.S. 1213, 1213 (2000).

196. *See* Implementation of the Telecomms. Act of 1996: Telecomms. Carriers' Use of Customer Proprietary Network Info. & Other Customer Info., 17 FCC Rcd. 14860 (2002).

197. *See Competition Policy Inst.*, 530 U.S. at 1213.

198. *See supra* Part III.C–D.

Congress should also create a civil remedy for failure to comply, permitting private individuals to file class action suits for privacy intrusion. This solution, as explained below, is the best means to both foster consumer confidence in security of their personal information[199] and to allow growth in the communications sector. It is critical to protect consumer privacy and assuage consumer concern[200] while allowing creative companies such as Google and Apple to continue to innovate in the way that has enabled them to rise to the top as industry and global leaders.[201] In other words, it is imperative not to kill the golden goose, but it is also imperative that private citizens not be forced under its wing.

A. Openness Is the Key to Consumer Confidence

Openness and free disclosure of information is the best solution to the current geolocation privacy problem and exactly the solution which both the FTC Principles and most privacy advocates espouse.[202] Open and honest disclosure would permit consumers to make their own decisions on what is the proper level of privacy for them and whether a service is worth forgoing their personal privacy. In order for consumers to make an informed decision regarding the level of privacy proper for them, companies must present consumers with clear, understandable information.[203]

---

199. *See supra* notes 115–127 and accompanying text.

200. *Id.*

201. As of market close on February 23, 2012, Google had a market cap of $197.07 billion. *Google Inc.*, GOOGLE FIN. (Feb. 23, 2012, 7:23 PM), http://www.google.com/finance?q=google. As of market close on February, 23, 2012, Apple had a market cap of $481.47 billion. *Apple Inc.*, GOOGLE FIN. (Feb. 23, 2012, 7:23 PM), http://www.google.com/finance?q=apple&hl=en.

202. *See* SELF-REGULATORY PRINCIPLES, *supra* note 62, at 46–47.

203. It is ironic that one of the biggest offenders, Google, has historically placed a priority on disclosure. JEFF JARVIS, WHAT WOULD GOOGLE DO?: REVERSE-ENGINEERING THE FASTEST GROWING COMPANY IN THE HISTORY OF THE WORLD 95–98 (2009). Indeed many in the industry would describe two of the most important themes of Google's success as "Be Honest" and "Be Open." *Id.* To be fair, at the time this Note went to press, Google was undertaking some measures and making some concessions that most of its competitors were unwilling to make, an example being the aforementioned implementation of an opt-out. *See* O'Brien, *supra* note 138 (noting the efforts of Google to avoid potential liability for privacy intrusion within the European Union); *see also* Farivar, *supra* note 138. Google has a willingness to frankly admit imperfection, and a culture that promotes openness and disclosure. Matt Cutts, *Google Search and Search Engine Spam*, OFFICIAL GOOGLE BLOG (Jan 21, 2011, 9:00 AM), http://googleblog.blogspot.com/2011/01/google-search-and-search-engine-spam.html ("We take pride in Google search and strive to make each and every search perfect. *The fact is that we're not perfect*, and combined with users' skyrocketing expectations of Google, these imperfections get magnified in perception. However, we can and should do better."(emphasis added)). Google's open model has not only worked well, it has propelled Google to the top of almost every niche it has chosen to enter. To be fair to Google's efforts, Google has created a program entitled "Dashboard" that permits a user to

B. Adding Incentive to the Self-Regulatory Regime

Self-regulation, as currently implemented, is insufficient; a system that implements the principles of the AICPA and FTC and punishes noncompliant companies via a civil penalty is the best solution.[204] Congress should create a privacy floor—a level of privacy that consumers cannot unwittingly give away. Additionally, Congress should require companies to attain informed consent at the granular level, and Congress should place strict limits on companies that seek geolocation data.[205] Such a system would bolster consumer confidence in the privacy of geolocation data while also requiring companies to protect consumer privacy or face penalties. In order to reach this goal, Congress should establish a precise set of guidelines for consumer privacy, add more specifics to the principles formulated by the FTC[206] or by the AICPA,[207] and create a private cause of action that would foster a class action enforcement regime.

Indeed, the FTC Principles, if properly enforced, would sufficiently increase consumer confidence in their right to privacy. In a study conducted in 2008 by Dr. Alan Westin in collaboration with Harris Interactive, Westin found that 59 percent of participants were uncomfortable with "websites us[ing] information about [their] online activity to tailor advertisements or content to [their] hobbies and interests."[208] But when Westin described to participants actions by the websites that would comply with the first four FTC principles, Westin found that most people, apart from the over-sixty-three age bracket, were comfortable with such actions, particularly with companies using online activities to customize advertisements.[209] Although the survey related to online information in general and not solely geolocation information,[210] physical location is just as personal

---

see and, to an extent, manage the data associated with a user account. *Privacy Tools*, GOOGLE.COM, http://www.google.com/privacy/tools.html (last visited Feb. 4, 2012). To log into your Dashboard account and view your personal data, visit https://www.google.com/dashboard. Apple typically takes the opposite approach, providing fewer options and less openness in the majority of its products. Still, despite the obvious success of its openness approach in other areas, Google has made only small steps toward implementing broad policies of openness regarding geolocation data. *See supra* Part I.

204. *See supra* Part III.C–D.

205. *See* SHAPIRO, *supra* note 103, at 220 (stating the necessity of a privacy safety net that protects consumers from their own impulses to trade away too much information on a competitive private market for consumer privacy).

206. *See Fair Information Practice Principles*, *supra* note 161.

207. *See GAPP*, *supra* note 174, at 7.

208. Harris Interactive Press Release, *supra* note 105, at 3.

209. *Id.*

210. *See id.*

and deserving of privacy, if not more so, than an individual's digital profile.

Ultimately, companies must notify consumers of data collection before it occurs.[211] Consumers must receive information regarding who is doing the collecting, for what purpose, what security measures the collector is taking, and with or to whom the collector may or may not share or sell the data.[212] Also, consumers must be able to opt-out of specific data elements on the granular level, not simply affirm or deny a request for data to be collected generally, meaning that consumers should be able to prohibit the sharing of information with all third-party companies.[213] Consumers must be able to access their information, correct any incorrect data, or delete any and all information, meaning that each company must have an app or website comprehensively structured so as to permit the average consumer to be able to delete any information stored by the company. For this to be possible, once the consumer deletes the information, the collecting company must also permanently delete the data, as must any of the affiliates with whom the collecting company has shared the data.

C. Civil Award

In order to properly strike the balance between sufficiently incentivizing business and unduly burdening the burgeoning geolocation industry, this Note recommends Congress create a civil award[214] to accompany the statutory enactment of the FTC Principles.[215] The award should be substantial enough that companies as large as Google will have a strong disincentive to violate consumer privacy but small enough that it should not bankrupt a small apps company. The proper balance would be a fine of between $15,000 and $40,000 per consumer who falls victim to geolocation data misappropriation.[216] To prevail, the plaintiff must show: (1) the collecting company appropriated his geolocation information without his knowledge or consent, (2) the company stored the geolocation

211. *See Fair Information Practice Principles*, *supra* note 161.

212. These suggestions closely follow the first four categories of the FTC Principles. *See* SELF-REGULATORY PRINCIPLES, *supra* note 62.

213. *See Fair Information Practice Principles*, *supra* note 161.

214. A criminal remedy would be necessary in order to address stalking and extortion concerns related to geolocation information, but a full inspection of a criminal remedy—its scope, magnitude, and prospects for effectiveness—are outside the scope of this Note. *See* Location Privacy Protection Act of 2011, S. 1223, 112th Cong. § 2266 (2011) (addressing the use of geological information in instances of stalking and domestic violence).

215. *See Fair Information Practice Principles*, *supra* note 161.

216. *Cf.* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 404 (2011) (establishing a maximum remedy of $16,500 per day of infraction).

information, and (3) the collecting company either employed the geolocation information to sell its goods or the collecting company sold the geolocation information to a third-party company. The congressional statute should establish a specific award amount, so as to avoid complicated lawsuits and extensive jury findings regarding statutory, compensatory, and punitive damages.[217]

It is imperative that Congress construct the statute in such a fashion so as to easily permit class certification, thereby allowing private citizens to serve as the primary enforcement mechanism. Fifteen thousand dollars in remedy may be enough to motivate some individuals to bring suit apart from a class, but it would not likely be worth the challenge of confronting large corporations in what could be an expensive litigation battle, particularly not when others would likely be watching and waiting to bring similar suits. Also, only a few claims of $15,000 each are not enough to serve as a strong deterrent to major companies, particularly companies such as Google and Apple, with market caps of $197.07 billion[218] and $481.47 billion,[219] respectively.

But if each claimant has a claim potentially worth $15,000 and claimants are able to sue as a class, it would force companies, even those as large as Apple, to change their privacy policies. If, for example, there were two million claimants,[220] a defendant would potentially be liable for upwards of $30 billion in damages. Such a sum would unavoidably give app makers and smartphone-operating-system creators the necessary incentive to

---

217. Statutory damages are available in other areas of law dealing with more abstract rights such as trademark and copyright. *See* 17 U.S.C. § 504(c) (2006); 15 U.S.C. § 1117(c). Although statutory damages are not the sole remedy in intellectual property law, this Note posits that making statutory damages the sole remedy for geolocation privacy violations is ideal because privacy violations result in little monetary harm and a factual inquiry into the damages to each victim would prove protracted and unpredictable. For a more comprehensive examination of the effectiveness of statutory damages in copyright law, see R. Collins Kilgore, *Sneering at the Law: An Argument for Punitive Damages in Copyright*, 15 VAND. J. ENT. & TECH. L. 637 (2013).

218. As of market close on February 23, 2012, Google has issued 325.14 million shares with a trading value of $606.11 per share. *Google Inc.*, GOOGLE FIN., http://www.google.com/finance?q=google (last visited Feb. 23, 2012).

219. As of market close on February 23, 2012, Apple has issued 932.37 million shares with a trading value of $516.39 per share. *Apple Inc.*, GOOGLE FIN., http://www.google.com/finance?q=apple&hl=en (last visited Feb. 23, 2012).

220. Two million is only 1 percent of the current number of Gmail accounts, which as of November 2010, was 193 million accounts worldwide. Joshua Norman, *"Gmail Killer" from Facebook on Its Way?*, CBSNEWS.COM (Nov. 15, 2010, 11:15 AM), http://www.cbsnews.com/8301-501465_162-20022793-501465.html. Setting the remedy between $15,000 and $40,000 per consumer seems reasonable given that Apple sold 18.65 million iPhones from January to March 2011 alone. Philip Elmer-DeWitt, *How Many iPhones Did Apple Sell Last Quarter?*, CNNMONEY (July 13, 2011, 5:41 AM), http://tech.fortune.cnn.com/2011/07/13/how-many-iphones-did-apple-sell-last-quarter-2.

respect a consumer-privacy statute. Both major players and minor app producers alike would comply with the federal law. Thus, a class action would be a powerful deterrent.

The bad press and negative image created by a successful suit for geolocation privacy breach against even a large tech company like Google, which relies heavily on stock options for employee motivation,[221] would be a significant deterrent in its own right. A drop in stock price could result in repercussions within a company's labor force, potentially leading to drastic measures similar to 2009, when the huge drop in the market forced Google to reprice its employee stock options.[222]

Lastly, a reward of at least $15,000 is likely to be a large enough sum to give the lead plaintiff a strong incentive to monitor the actions of the plaintiffs' counsel, a relationship upon which other private class-action regimes have placed great emphasis in order to ensure the regime functions properly.[223]

D. Class Action Enforcement

It is not within the scope of this Note to weigh every ancillary element of a class action system of enforcement.[224] Changes in class action rules may bring some level of uncertainty to the class action enforcement regime; however, if Congress were to model the class action regime on Section 10(b) of the Securities Exchange Act,[225] it

---

221. *See* Lewis D. Lowenfels et al., *Attorneys as Gatekeepers: SEC Actions Against Lawyers in the Age of Sarbanes-Oxley*, 37 U. TOL. L. REV. 877, 901–05 (2006); Katie Hafner, *Google Options Make Masseuse a Multimillionaire*, N.Y. TIMES (Nov. 12, 2007), http://www.nytimes.com/2007/11/12/technology/12google.html.

222. In early 2009, Google had seventeen thousand employees holding more than eight million stock options, which it reset to a lower price to benefit and continue to incentivize its employees. *Google Reprices Employee Stock Options*, CBSNEWS.COM (Feb. 11, 2009, 1:43 PM), http://www.cbsnews.com/stories/2009/01/23/business/main4750463.shtml.

223. *See In re* Cendant Corp. Litig., 264 F.3d 201, 222–26 (3d Cir. 2001); STEPHEN J. CHOI & A.C. PRITCHARD, SECURITIES REGULATIONS: CASES AND ANALYSIS 238 (Robert C. Clark et al. eds., 3d ed. 2012) (discussing the lack of incentive for plaintiffs in securities-fraud class actions to adequately monitor plaintiffs' counsel when the lead plaintiff stands to gain only a trivial sum). The intricacies of plaintiffs' counsel theory is beyond the scope of this Note.

224. Nor is it within the scope of this Note to analyze the impact on class actions of *Wal-Mart Stores v. Dukes*, 131 S. Ct. 2541 (2011), a case that potentially changed the rules for certification of a class. *See id. Wal-Mart Stores v. Dukes* involved a class action suit for sexual discrimination based on Wal-Mart's alleged practice of promoting men rather than women to management positions. *Id.* at 2547. The Supreme Court dismissed the case, holding in part that the class could not be certified because it did not satisfy the commonality requirement. *Id.* at 2556–57. The Court's holding arguably tweaked the Rule 23 commonality requirement, but any such change is unlikely to impact a finding of commonality as proposed in the solution of this Note.

225. 15 U.S.C. § 78j(b) (2006).

would likely prove highly effective at protecting consumer privacy regarding geolocation data. While class action enforcement is already available under the current tort model, the current scheme provides little protection to consumers, because the selling of personal geolocation data to third parties generally does not violate any tort. Additionally, any creation of a new tort by a court would likely occur in chaotic and piecemeal fashion, a manner that characterizes court-made common law.

1. Jurisdiction

Class action plaintiffs may bring class action claims in federal court if their claims arise under federal law[226] or if their claims qualify for diversity jurisdiction under the requirements of 28 U.S.C. § 1332(d).[227] Section 1332(d) makes diversity jurisdiction contingent upon the amount in controversy exceeding $5 million[228] and the plaintiffs satisfying any one of the typical diversity jurisdiction requirements.[229] As it would be a far better solution for Congress to create a uniform body of law rather than allowing a patchwork of state legislation,[230] class action plaintiffs under a federal consumer–geolocation-data–privacy bill would qualify for federal question jurisdiction.

2. Class Action Certification

Courts would likely certify a geolocation privacy suit as a class action under Rule 23.[231] The privacy breach would be the primary claim of all of the plaintiffs, particularly if the court sanctioned a remedy of $15,000, thereby satisfying the "predominance" or

---

226. 28 U.S.C. § 1331.

227. *Id.* § 1332(d).

228. *Id.* § 1332(d)(2).

229. Section 1332(d)(2) sets forth grounds for diversity jurisdiction based on citizenship:

> The district courts shall have original jurisdiction of any civil action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which—
>
> (A) any member of a class of plaintiffs is a citizen of a State different from any defendant;
>
> (B) any member of a class of plaintiffs is a foreign state or a citizen or subject of a foreign state and any defendant is a citizen of a State; or
>
> (C) any member of a class of plaintiffs is a citizen of a State and any defendant is a foreign state or a citizen or subject of a foreign state.

Id. § 1332(d)(2)(A)–(C).

230. *See* discussion *infra* Part IV.E.iii.

231. *See* FED. R. CIV. P. 23.

"superiority" requirement.[232] Although it is difficult to definitively state all of the claims that members of a putative class action could raise, as most privacy claims lack standing,[233] it seems reasonable that the privacy claim sanctioned by Congress's newly enacted geolocation-privacy law would predominate the litigation or, indeed, be the only claim not dismissed for lack of standing of the collective plaintiffs. Courts consider efficiency and judicial economy when considering whether to certify a class,[234] and a court would likely find that it is far more economic and efficient to decide one suit alleging the same factual pattern and raising the same predominate claim, rather than thousands or millions of individual suits.[235]

E. Advantages over Other Regimes

A class action–based enforcement regime has advantages over other available regimes. These advantages include avoidance of (1) agency capture, (2) a burdensome and inefficient tort regime, and (3) a state patchwork of regulation.

---

232. *Id.* at 23(b)(3) ("[A class action may be maintained if] questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.").

233. *See, e.g.*, *In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865, at *46 (N.D. Cal. Sept. 20, 2011).

234. 2 HERBERT B. NEWBERG ET AL., NEWBERG ON CLASS ACTIONS § 4.25 (4th ed. 2002) (explaining that the predominance test "asks whether a class suit for the unitary adjudication of common issues is economical and efficient in the context of all of the issues in the suit").

235. A class action suit for breach of disclosure of geolocation information would also be able to satisfy the five requirements of sustaining a class action in federal courts. First, the class would satisfy the ascertainability clause, as having their data acquired, stored, and sold without their consent serves as "objective criteria" allowing a court to identify class members. *See* FED. R. CIV. P. 23(c)(1)(B) ("An order that certifies a class action must define the class . . . ."); *In re* Methyl Tertiary Butyl Ether Prods. Liab. Litig., 209 F.R.D. 323, 337 (S.D.N.Y. 2002) (stating that an "identifiable class exists" if members can be ascertained by reference to "objective criteria" and it is "administratively feasible" for a court to determine). Second, the class would satisfy the numerosity requirement by including enough plaintiffs to make joinder "impracticable." FED. R. CIV. P. 23(a)(1). Courts interpret impracticable to mean making joinder difficult or inconvenient, not impossible. *See* Robidoux v. Celani, 987 F.2d 931, 935 (2d Cir. 1993) ("Impracticable does not mean impossible."). Third, the class would satisfy the commonality requirement by having a "question of law common to the class," FED. R. CIV. P. 23(a)(2), meaning a similar claim centering on a fact or law whose resolution "is central to the validity of each" class member's claim. Wal-Mart Stores, Inc. v. Dukes, 131 S. Ct. 2541, 2557 (2011). Fourth, the class would satisfy the adequacy requirement, given that finding a consumer who fairly and adequately represents the interests of the class would not be difficult. FED. R. CIV. P. 23(a)(4). Fifth, the privacy violation claim would be "typical" of the claims of the class, as each member's claim would arise from the same course of events. *See* FED. R. CIV. P. 23(a)(3); Marisol A. v. Giuliani, 126 F.3d 372, 376 (2d Cir. 1997).

1. Avoidance of Agency Capture

Geolocation touches upon a complex area of the law that is plagued by a rate of technological advancement paralleled in few other fields. While some would argue that a regulatory agency is a better candidate for enforcement,[236] a class action regime avoids many of the drawbacks that would arise with a regulatory regime.

First, a class action enforcement regime eliminates any risk of administrative capture,[237] which refers to interest groups or market actors exerting a "capturing" influence on the staff or commission members of a regulatory agency, typically leading to the implementation of the preferred policy outcomes of special interest groups.[238] Administrative capture is not new to economists and is sometimes the result of the simple fact that highly organized businesses have better information on what is occurring in a particular market than do regulatory agencies.[239] Alternatively, regulated companies also have a much higher incentive to lobby regulators than do citizens, whose interests are quite diffuse in comparison.[240]

Second, a class action regime would prevent the delays and substantial inefficiencies that accompany any regime managed by a regulatory agency.[241] Agencies have little incentive to work quickly and effectively when formulating regulations, and indeed individuals have used class action suits in order to sidestep an ineffective regulatory regime in multiple instances.[242] While there may be some transaction costs to a private-enforcement regime, if judges are active in the pleading process, the aggregate costs associated with dismissing frivolous claims are not likely to be higher than the costs of employing regulators.

---

236. *See* SHAPIRO, *supra* note 103, at 221.

237. The concept described by administrative capture has many names, including agency capture and regulatory capture.

238. *See, e.g.*, George Stigler, *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. SCI. 3 (1971).

239. *Id.*; *see* Reuel E. Schiller, *The Era of Deference: Courts, Expertise, and the Emergence of New Deal Administrative Law*, 106 MICH. L. REV. 399, 417 (2007); Wendy E. Wagner, *Administrative Law, Filter Failure, and Information Capture*, 59 DUKE L.J. 1321, 1334 (2010).

240. *See, e.g.*, Eric Helland & Jonathan Klick, *To Regulate, Litigate, or Both* 5 (RAND Inst. for Civil Justice, Working Paper No. WR-677-ICJ, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450425.

241. For an analysis of environment regulatory agencies' inefficiencies, see STEVEN C. HACKETT, ENVIRONMENTAL AND NATURAL RESOURCES ECONOMICS: THEORY, POLICY, AND THE SUSTAINABLE SOCIETY 105 (3d ed. 1998).

242. *See* Joni Hersch, *Breast Implants: Regulation, Litigation, and Science*, *in* REGULATION THROUGH LITIGATION 144, 176 (W. Kip Viscusi ed., 2002).

The biggest critique against a class action regime is that it creates heavy reactive regulation, rather than preventive regulation.[243] While it is true that a violation of geolocation privacy must predicate a suit, under a strong class action regime with an adequate remedy, companies will have a robust incentive to avoid violations. A successful suit will be very costly, and industries will choose to self-regulate in order to avoid the courtroom.

2. Avoidance of Tort Inadequacies

A class action regime built upon a statute passed by Congress is superior to the adoption of a new common-law tort. Even if established by the courts, a tort regime would place a single individual tracked by WPS software at a huge bargaining disadvantage as compared to a highly centralized corporation tracking the person's whereabouts for profit-making purposes. While a judge-made tort for privacy intrusion using geolocation data could experience success, it would require judges to take a huge step in adopting a new law.

In a tort regime, regulation would be reactive,[244] meaning the law would develop slowly and consumer protection would develop even more slowly. With the amount of time that it sometimes takes for cases to wind their way through the courts,[245] a vast amount of information on consumers could already be generated, collected, utilized, sold to third parties, and even stolen. Thus, private companies could compromise consumer privacy while waiting for the common law to develop.

A tort-based system would result in a hodgepodge of regulation based on court decisions.[246] Although judges would also be deciding class actions, a congressional statute would limit the disagreements that different judges may have over the political or theoretical framework of the tort regime. A congressional statute would create the framework with much of the necessary theory and policy therein, theoretically obviating this responsibility.

Finally, a tort system would fail to resolve the collective-action dilemma, meaning individuals would need to bring suit against Apple

---

243. *See* Elizabeth Chamblee Burch, *Securities Class Actions as Pragmatic Ex Post Regulation*, 43 GA. L. REV. 63, 75–88 (2008) (discussing how securities class actions serve as a check against agency capture and provide important pragmatic benefits to society).

244. *See* Robert V. Percival, *Environmental Law in the Twenty-First Century*, 25 VA. ENVTL. L.J. 1, 10 (2007) (discussing the reactive nature of common-law tort regulation in the area of environmental law).

245. For example, *Wal-Mart Stores v. Dukes*, 131 S. Ct. 2541 (2011), was filed December 3, 2001, and decided after the appeals process on June 20, 2011. *Id.*

246. *See* Somes v. United Airlines, Inc., 33 F. Supp. 2d 78, 82 (D. Mass. 1999) (discussing how state tort law created a patchwork of regulation governing the airline industry).

or Google alone while all others look on, hoping for a verdict they can use in future suits.[247] Class actions, on the other hand, avoid this problem; they permit easy collectivization and are more like business deals than adversarial litigation.[248]

3. Avoidance of a State Patchwork

A final option for enforcement is to leave regulation to the states, and indeed both Utah and California have recently initiated regulation.[249] A state-based regulatory scheme would have many disadvantages as compared to a federal class action solution. A state system would be decentralized, increasing compliance costs for businesses that span multiple jurisdictions. For example, while a company may be able to collect information from a consumer in Arizona, it may be unable to do so if the consumer then drives across the California border.[250] This patchwork would be unnecessarily cumbersome and inefficient for companies.[251] Ultimately, consumer confidence and privacy are necessary, regardless of the state of residence.[252]

F. Limits to a Statutory Solution

The statutory scheme should be narrow in order to delicately balance the needs of multiple areas.[253] For example, a consumer opt-out provision that places consumers in a position to choose whether or not an app can see their location would cause problems for

---

247. *See supra* Part IV.C–D.

248. *See* William B. Rubenstein, *A Transactional Model of Adjudication*, 89 GEO. L.J. 371, 418–32 (2001) (discussing how class actions provide the basis for a new model of US adjudication premised on dealmaking and transactional principles).

249. CAL. CIV. CODE § 1798.83 (West 2010); UTAH CODE ANN. § 13-37-201 (West 2012).

250. *See supra* Part IV.E.2.

251. The right of publicity is an example of a laborious, time-consuming area of regulation that has been left to the states. *See* Kevin L. Vick & Jean-Paul Jassy, *Why a Federal Right of Publicity Statute Is Necessary*, 28 COMM. LAW. 14, 16–17 (2011); *see also* Talor Bearman, Note, *Intercepting Licensing Rights: Why College Athletes Need a Right of Publicity*, 15 VAND J. ENT. & TECH. L. 85, 88 (2012).

252. Another argument against a state regulatory system is that it would incentivize plaintiffs to forum shop, choosing a state or federal jurisdiction depending on which one is more plaintiff-friendly. As there is little evidence that any such proclivity exists, the argument need not be addressed here.

253. *See* King, *supra* note 149, at 115 (discussing how limitation on personal jurisdiction, like those on state action, should consider the "costs associated with an effective geolocation mandate, the relevance of geography to the underlying online conduct, and the burden on protected speech").

apps subject to direct or indirect geolocation mandates.[254] For those apps, the creators must be able to ascertain the geolocation of the user in order to effectively regulate access to sensitive or illegal content.[255] A statute that denies all geolocation information to certain app companies would make it impossible for them to comply with the variances of laws across multiple states in a state-based system.[256] Still, it would be possible to permit websites to geolocate only as necessary to comply with any independent legal obligation or to avoid liability in a jurisdiction.[257]

V. BILLS CURRENTLY UNDER CONGRESSIONAL CONSIDERATION

Due to the pressure of constituents, the outcry of privacy advocates, and the concern of businesses that fear the regulating away of a very profitable and promising market, Congress has begun considering a series of bills that either directly or tangentially deal with the issue of geolocation. This Part briefly discusses the three most promising bills and concludes with a brief overview of the other candidates.

A. Location Privacy Protection Act

In June of 2011, Senators Al Franken (D-MN) and Richard Blumenthal (D-CT)[258] introduced the most promising bill of all currently under consideration, the Location Privacy Protection Act (LPPA).[259] Since referral of the LPPA to the Senate Committee on the Judiciary,[260] six other senators have agreed to cosponsor the bill.[261] Under the LPPA, a nongovernmental agency engaged in interstate or foreign commerce that provides an electronic communication service to "electronic communication devices" would need to receive express authorization from the consumer in order to knowingly collect, receive,

254. Most of these apps are online-gambling websites that are regulated in some jurisdictions but not others. *See id.* at 115, 122.

255. *See id.* at 122.

256. *See id.* at 123.

257. *See id.* at 114.

258. Daren M. Orzechowski et al., *Federal Legislation Introduced Regarding Geolocation Information*, WHITE & CASE (Sept. 2011), http://www.whitecase.com/articles-09162011.

259. Location Privacy Protection Act of 2011, S. 1223, 112th Cong. § 2266 (2011) (stating the purpose of the bill was "[t]o address voluntary location tracking of electronic communications devices, and for other purposes").

260. Location Privacy Protection Act Bill Summary & Status, Library of Congress THOMAS, http://thomas.loc.gov (select "bill number" and search "S. 1223") (last visited Nov. 9, 2012).

261. *Id.*

record, obtain, or disclose to a nongovernmental individual or entity the geolocation information from an electronic communication.[262] Express authorization requires that the device owner give affirmative consent following "clear and prominent notice."[263] The nongovernmental agency must notify the consumer as to what geolocation information the agency will collect and the specific nongovernmental entities that may become privy to the information.[264]

The LPPA definition of "electronic communication device" is broader than necessary for the area of the law this Note considers, as the definition is broad enough to encompass issues of consumer online privacy.[265] The bill sweeps all mobile devices under its strictures, including smartphones, mobile phones, tablets, WiFi-equipped laptops, GPS navigation units, and most other mobile devices that permit geolocation.[266] It also supersedes any noncomplying state or local laws.[267]

One element of the bill that could quash most private-enforcement actions is the bill's empowerment of the US Attorney General and the state attorneys general to bring actions against violators.[268] In order to avoid the common issue of parallel regimes of private enforcement and administrative enforcement,[269] the bill specifies that if the US Attorney General brings suit, citizens may not bring private actions while the litigation is pending.[270] While it is possible the preemption clause would prevent the problems relating to exclusive private enforcement or simultaneous private and government enforcement actions, the Attorney General may not be as zealous in his representation as would private citizens who have actually suffered the harm.[271]

---

262. Location Privacy Protection Act of 2011 § 2713(a)(1)–(2), (b)(1).

263. *Id.* § 2713(a)(3) (defining "clear and prominent notice" as requiring a display "by the electronic communications device, separate and apart from any final end user license agreement, privacy policy, terms of use page, or similar document").

264. *Id.* § 2713(a)(3)(B).

265. *See id.* § 2713(a)(2), (b)(1). Privacy issues concerning geolocation data are distinct from those affecting online consumer data, as geolocation data deals with the concrete physical location of users rather than their virtual reality.

266. *See id.*

267. *Id.* § 2713(e)(1).

268. *Id.* § 2713(d)(1)–(2).

269. *See* Helland & Klick, *supra* note 240, at 68.

270. Location Privacy Protection Act of 2011 § 2713(d)(4)(A).

271. The Attorney General suffers from many of the same capture problems as regulatory agencies. *See supra* Part IV.E.1.

A major deficiency of the statute is the civil damage award of only $2,500 and the allowance of punitive damages.[272] This sum is too low, as it would discourage strong lead-plaintiff participation. Plaintiffs would gain little after a victory, particularly after attorneys' fees reduce the damage award.[273] The possibility of punitive damages[274] creates far less certainty as to the stakes of the claim, adding further inefficiency and expense to the enforcement mechanism. Additionally, $2,500 in damages would require at least two thousand plaintiffs to be able to clear the Rule 23 damages hurdle for class certification, meaning courts will refuse to certify some meritorious suits due to the small number of plaintiffs bringing claims against small infringers.[275]

B. Geolocational Privacy and Surveillance Act

Representative Jason Chaffetz (R-UT) and Senator Ron Wyden (D-OR) introduced the Geolocational Privacy and Surveillance Act[276] (GPS Act) in June of 2011,[277] and it has since been offered as an amendment to the Cybersecurity Act of 2012.[278] The GPS Act, like the LPPA, prohibits the interception and collection of consumer geolocation data without primary consumer consent.[279] The GPS Act, however, attempts to include governmental actors in addition to nongovernmental actors,[280] thereby addressing the Fourth Amendment issues surrounding governmental use of consumer citizen geolocation data.[281] While it is outside the scope of this Note to analyze the bill in light of the recent Supreme Court ruling of *United*

272. Location Privacy Protection Act of 2011 § 2713(d)(5)(A)–(B).

273. Theodore Eisenberg & Geoffrey P. Miller, *Attorneys Fees in Class Action Settlements: An Empirical Study* 20 tbl.1 (NYU Ctr. for Law and Bus., Working Paper No. CLB-03-017, 2003) (finding that the average attorney fee in private class actions was 21.9 percent and the median was 23.2 percent, far below the oft-quoted one-third).

274. Location Privacy Protection Act of 2011 § 2713(d)(5)(B).

275. *See* FED. R. CIV. P. 23; *supra* Part IV.D.2.

276. Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. § 2602 (2011).

277. Geolocational Privacy and Surveillance Act Bill Summary & Status, Library of Congress THOMAS, http://thomas.loc.gov (select "bill number" and search "S.1212") (last visited Oct. 27, 2012).

278. Press Release, Ron Wyden, Senator for Oregon, Wyden Amendments to Cyber Bill Clarify Rules for GPS Tracking; Seek Privacy Protection in the Cloud (July 31, 2012), http://www.wyden.senate.gov/news/press-releases/wyden-amendments-to-cyber-bill-clarify-rules-for-gps-tracking-seek-privacy-protection-in-the-cloud-.

279. *See* Geolocational Privacy and Surveillance Act § 2602(a). This Note analyzes the Senate version (S. 1212), as the House version (H.R. 2168) is substantially similar.

280. *Id.* § 2601(8).

281. *See supra* Part II.C.

States v. Jones,[282] in regards to private actors the GPS Act falls short in its privacy protection as it contains no provisions regarding how consent is to be given or received.[283]

In addition, the bill's enforcement mechanism is grossly inadequate.[284] The GPS Act adopts a private cause of action against parties other than the United States engaged in the interception, disclosure, and intentional use of geolocation data.[285] In addition to punitive damages, the victims are eligible for the greater of (1) the sum of actual damages suffered plus the profits made by the violator as a result of the violation, or (2) statutory damages of whichever is the greater of $100 per day the violation occurred or $10,000.[286] In addition to having many of the same problems as the LPPA, the GPS Act's complicated and small remedy renders class actions nearly impossible.[287] This may mean an increase in individual suits brought, or it may mean that consumers bring virtually no actions—neither class nor individual. Also, the possibility of punitive damages, statutory damages, and actual damages plus profits will cause the regime to be very cumbersome, opaque, and ineffective.[288]

C. Mobile Device Privacy Act

Representative Ed Markey (D-MA) recently introduced the Mobile Device Privacy Act to the House of Representatives on September 12, 2012.[289] The bill will require that any entity that sells a mobile device, a mobile service, or offers an app for download must provide "clear and conspicuous disclosure"[290] to consumers as required by yet-to-be-promulgated FTC rules.[291] Such disclosure must specifically include that an app or company has installed a particular monitoring software, what type of information the app or program is monitoring and transmitting, with whom the collector might share the information, how the collector and third parties will use the

---

282. *United States v. Jones* recently held that the placement of a tracking device on a car that transmitted geolocation data for twenty-eight days was a search under the Fourth Amendment. 132 S. Ct. 945, 949, 954 (2012).

283. *See* Geolocational Privacy and Surveillance Act §§ 2601–2602.

284. *See id.* § 2605.

285. *Id.* § 2605(a).

286. *Id.* § 2605(b)(2), (c).

287. *See supra* Part IV.C.1.

288. *See supra* Part IV.C.

289. Wendy Davis, *Lawmaker Proposes New Privacy Safeguards for Mobile Users*, ONLINE MEDIA DAILY (Sept. 12, 2012, 5:55 PM), http://www.mediapost.com/publications/article/182903.

290. Mobile Device Privacy Act, H.R. 6377, 112th Cong. § 2(a), (c) (2012).

291. *See id.* § 2(a).

information, and what the consumer can do to prohibit further collection, even if they have provided permission in the past.[292] The collector must obtain consumer consent prior to the time when the monitoring software first begins collecting and transmitting information and must also permit the consumer to revoke consent at a later date.[293] Also, the bill requires the collecting companies to add security measures in order to better protect consumer information.[294]

The FTC and FCC enforce all requirements,[295] but the state attorneys general[296] and a private cause of action worth up to $1,000 and attorneys' fees[297] are alternative means sanctioned by the bill to protect the disclosure requirement specifically.

Although certainly the closest to a proper and useful solution to this complicated issue, there are still several very critical shortcomings. First, the disclaimer is too general; few, if any, consumers will read or fully understand when they first begin using the services or product collecting their personal data. It lacks sufficient granularity in consent; it also lacks a blanket opt-out when first using the program or service. In addition, although this bill does include a structure for a private remedy, the state attorneys general can preempt these suits. These private remedies are too small at only $1,000 per claim. Taken together, the bill lacks the private-enforcement mechanism necessary to avoid the risks and inefficiencies discussed above.[298]

D. Other Contenders

There are several other bills introduced in Congress, but all are insufficient to address the implicit concerns of consumer-geolocation-data privacy. The Commercial Privacy Bill of Rights Act of 2011 proposes an excellent statutory framework for both online and geolocation privacy,[299] suggests a remedy of $16,500 per day of infraction,[300] and properly preempts state law.[301] The bill includes opt-in provisions that are constitutionally suspect,[302]

---

292. *See id.* § 2(b).
293. *See id.* § 3.
294. *See id.* § 4(a).
295. *See id.* § 6.
296. *See id.* § 6(d).
297. *See id.* § 6(e).
298. *See supra* Part IV.E.1.
299. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 3(5) (2011).
300. *See id.* § 404(a).
301. *See id.* § 405(a).
302. *See id.* § 202(a)(3); U.S. West, Inc. v. FCC, 182 F.3d 1224, 1230 (10th Cir. 1999).

however, and it empowers the FTC to take the leading role in rulemaking and enforcement.[303] Such a solution would likely eclipse any class action–based regulation and would result in all of the risks and inefficiencies that come with a regulatory regime.[304]

Another contender, the Electronic Communications Privacy Act Amendments Act of 2011, introduced by Senator Leahy (D-VT), addresses only governmental actors and their intrusion on citizen privacy.[305] The Do-Not-Track Online Act of 2011, introduced by Senator Rockefeller (D-WV), also delegates the FTC full rulemaking power in order to solve the problem.[306] Besides the fact that the bill attempts to address all Internet privacy concerns along with geolocation concerns, the bill prescribes a weak civil penalty, permitting a maximum liability of $15 million per company[307]—a drop in the bucket for companies the size of Google and Apple. These bills are clearly insufficient as regulatory structures of consumer privacy.

Congress should enact a statute creating a framework that requires companies to notify consumers of data collection before it occurs.[308] A collecting company must inform consumers that the company is collecting data, for what purpose, what security measures the collecting company is taking to protect the data, and with whom the company may or may not share or sell the data.[309] Also, consumers must be able to opt out of specific data elements on the granular level, not simply affirm or deny a request for data to be collected generally, meaning that consumers should be able to prohibit the sharing of information with all third-party companies.[310] Consumers must be able to access their information, correct any incorrect data, or delete any and all information, meaning that each company must have an app or website comprehensively structured to permit the average consumer to be able to delete any information stored by the company. Congress should create a federal class action regime, allowing $15,000 per successful claim of geolocation data misappropriation.

---

303. Commercial Privacy Bill of Rights Act of 2011 § 402.

304. *See supra* Part IV.E.1.

305. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. § 2713 (2011).

306. Do-Not-Track Online Act of 2011, S. 913, 112th Cong. § 3(a)(1) (2011) ("[The Do-Not-Track Online Act] require[s] the Federal Trade Commission to prescribe regulations regarding the collection and use of personal information obtained by tracking the online activity of an individual, and for other purposes.").

307. *See id.* § 3(b)(2)(B).

308. *See* FED. TRADE COMM'N 1998, *supra* note 151, § 3(A)(1).

309. These suggestions follow very closely the categories of the first four FTC Fair Information principles. *See id.* § 3(A)(1)–(4).

310. *See id.* § 3(A)(1)–(2).

VI. CONCLUSION

The infringement of consumer property in terms of the creation, collection, and sale of geolocation data is a grave problem in need of a serious solution. Multiple companies are using their GPS chips and WPS databases to track the locations of mobile devices, using the data for company purposes, and selling the data to third parties.[311] The consumer is largely unaware that this transaction is occurring, to whom the data may be distributed, and who may be able to purchase the information.[312] Currently, the consumer receives no notification of the security measures taken to keep this information safe, or of what he can do to either limit or eliminate information he does not wish others to retain.[313]

Congress should act to solve this privacy and information crisis by enacting a comprehensive framework and a reasonable remedy that will easily permit a private enforcement regime. Some of the bills in Congress come close to formulating an adequate privacy regime; however, each has deficiencies in one or more areas.[314] Congress should alter one of the existing bills or introduce a new piece of legislation.

The ever-continuing march of technological advancement is not only a good thing, it is essential to economic expansion as it facilitates the optimization of resources through efficiency increases. Technology, with its feathers of silicon and eggs of information sharing, truly is the golden goose of the modern era. Ultimately, however, the misappropriation of geolocation data by companies may be threatening the very lifeblood of our gilded fowl. Consumer privacy is of central importance, and Congress must act to protect it.

Timothy J. Van Hal[*]

311. *See supra* Part I.A–C.

312. *See supra* Part I.C.

313. *See supra* Part I.C.

314. *See supra* Part V.

* J.D. Candidate, Vanderbilt University Law School, 2013; B.A., Government, Georgetown University, 2009. The Author wishes to express his heartfelt gratitude to his family members for their unwavering support, for without them this Note would never have been possible. Additionally, the Author would like to thank Daniel Gervais, FedEx Research Professor of Law, Vanderbilt University Law School, and Director, Vanderbilt Intellectual Property Program, for his input, support, and advice on this Note from its inception, as well as Katie Kuhn, Francie Kammeraad, Mike Dearington, and Shane Valenzi of the VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW for their edits.