THERE'S NO APP FOR THAT: PROTECTING USERS FROM MOBILE SERVICE PROVIDERS AND DEVELOPERS OF LOCATION-BASED APPLICATIONS

Daniel L. Pieringer[*]

TABLE OF CONTENTS

* J.D., University of Illinois College of Law, expected 2013. B.S., Northwestern University, 2006. The author would like to thank Professor Andrew D. Leipold for his guidance and expertise. He would also like to thank Melissa Maleske for her inspiration and his family, friends, and all of the people who helped him through the editing process for their advice and support.

I. INTRODUCTION

You probably don't know your cousin's phone number. You don't have to know it—like your emails, your social media networks of choice, and your current location, it is stored in your phone. The convenience of having all of that information at your fingertips has given mobile devices and accessories the potential to become a trillion-dollar industry, with consistently substantial growth in recent years and more anticipated in the near future.[1] The proliferation of smartphones and tablets has led to new usage patterns as well. Mobile devices now account for nearly 7% of all worldwide web traffic, with location-based services (LBS) providing consumers with countless new avenues for taking advantage of the ubiquity of wireless network access.[2]

Broadly speaking, LBS are a wide variety of different technologies that rely on, use, or incorporate the location of a device to provide or enhance a service.[3] More specifically, these various technologies locate mobile devices and provide users location-specific information, allowing a hungry consumer to access Yelp reviews of the nearest Chinese restaurant, get turn-by-turn directions there via Google Maps, then share her location with friends via Foursquare.[4] While that scenario demonstrates some of the more common uses of LBS, it is by no means an exhaustive list. Consumers utilize LBS in ever-increasing ways, with a recent study projecting that the industry could become a $10-billion-a-year business by 2016.[5]

LBS present a classic double-edged sword. On one hand, they innovate and deliver better products to their consumers, creating "a more dynamic user experience that adds value and convenience and changes the way people transact business and organize their activities and free time."[6] However, they

1. Dylan Byers, *The Future According to Eric Schmidt: Google Chairman Talks of the Next Trillion-Dollar Industry*, ADWEEK (June 23, 2011), http://www.adweek.com/cannes-lions-2011/future-according-eric-schmidt-132833.

2. Press Release, comScore, Inc., Smartphones and Tablets Drive Nearly 7 Percent of Total Web Traffic (Oct. 10, 2011), *available at* http://www.comscore.com/Press_Events/Press_Releases/2011/10/Smartphones_and_Tablets_Drive_Nearly_7_Percent_of_Total_U.S._Digital_Traffic.

3. CTIA—THE WIRELESS ASS'N, BEST PRACTICES AND GUIDELINES FOR LOCATION-BASED SERVICES 1 (version 2.0 2010).

4. Melissa Maleske, *Location-Based Mobile Apps Create Privacy Concerns*, INSIDE COUNSEL (Sept. 1, 2011), http://www.insidecounsel.com/2011/09/01/location-based-mobile-apps-create-privacy-concerns [hereinafter Maleske, *Privacy Concerns*]. In this example, LBS pinpoint a user's location using one of various different geolocational technologies, use that location to show the user various Chinese dining options in the vicinity and how other users have rated those options, map the most direct route to the user's chosen destination, and allow the user to share her final location with a network of other users.

5. Nathan Olivarez-Giles, *Location-Based Services to Become 10-Billion Industry by 2016, Report Says*, L.A. TIMES, June 11, 2011, http://articles.latimes.com/2011/jun/11/business/la-fi-locator-services-20110611.

6. FED. COMMC'NS COMM'N, LOCATION-BASED SERVICES: AN OVERVIEW OF OPPORTUNITIES AND

also open the door to risks that necessarily accompany the sharing of sensitive information with strangers. By definition, LBS require the collection of significant amounts of personal data that could prove dangerous in the wrong hands, and evidence continues to show that collectors of that data are not being responsible with it.[7]

Innovative technology sparking privacy concerns is nothing new. Legal academics have tackled similar privacy issues following the advent of the Internet, car phones, personal computers, direct deposit functionality, and grocery store frequent-shopper club cards.[8] The age of applications, however, brings with it new and unique circumstances. In previous tangles with privacy issues, consumers shared their information primarily with one known entity, be it a phone company, an Internet service provider, a bank, or a grocery store. Today, though, the booming mobile device industry thrives on applications contributed by third-party developers, many of whom are no more than industrious individuals operating out of their homes or offices.[9] As such, regulation of the LBS industry needs to go beyond just keeping Google and Apple in check. Legislators, regulators, and industry officials must be charged with protecting consumers from hundreds of thousands of developers who have access to unlimited sensitive information and very little accountability.[10] For better or worse, the answer is not in our phones.

This Recent Development will explore the various approaches to effective protection of consumer information. Part II of this Recent Development will provide background information on location-based services and detail the

---

OTHER CONSIDERATIONS 3 (2012), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-314283A1.pdf.

7. *See* Nancy J. King, *When Mobile Phones Are RFID-Equipped—Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 MICH. TELECOMM. & TECH. L. REV. 107, 127 (2008) (discussing the impact of RFID technology in phones that may allow businesses to locate and target consumers); Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, 6 J. L. & POL'Y FOR INFO. SOC'Y 119, 127 (2010) (evaluating the consequences of GPS capabilities in smartphones regarding the sharing of personal information); Kristin E. Edmundson, Note, *Global Positioning System Implants: Must Consumer Privacy Be Lost In Order for People to Be Found?*, 38 IND. L. REV. 207, 212 (2005) (discussing the implications of the sale of individual consumer data through mobile phone GPS tracking); Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010), http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html (investigating the wide array of private information being disseminated through iPhone and Android apps).

8. *See generally* Christine Anthony, *Grocery Store Frequent Shopper Club Cards: A Window Into Your Home*, 4 B.U. J. SCI. & TECH. L. 7 (1998) (warning the public that grocery store membership cards could expose sensitive personal information); Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1986–1987) (discussing the privacy concerns of personal computing); Harold E. Mortimer, *Current Legal Problems Facing Commercial Banks Participating in Electronic Funds Transfer Systems*, 95 BANKING L. J. 116 (1978) (discussing how new banking methods like wire transfers and direct deposit can allow for the storage and misuse of personal information); Major R. Ken Pippen, *Consumer Privacy on the Internet: It's "Surfer Beware"*, 47 A.F. L. REV. 125 (1999) (arguing that the Internet has unique qualities that require new laws and regulations); Timothy R. Rabel, *The Electronic Communications and Privacy Act: Discriminatory Treatment for Similar Technology, Cutting the Cord of Privacy*, 23 J. MARSHALL L. REV. 661 (1989–1990) (noting that the radio portion of wireless communication on cellular and cordless phones raises privacy issues); Carol R. Williams, *A Proposal for Protecting Privacy During the Information Age*, 11 ALASKA L. REV. 119 (1994) (arguing that computer technology poses significant privacy threats).

9. *See* Maleske, *Privacy Concerns*, *supra* note 4 ("[I]mplementation of industry best practices is uneven among smaller app developers.").

10. *See id.* ("[T]he debate rages as to whether the industry can be trusted to self-regulate . . . .").

various conceptions for handling geolocational technologies including multiple proposed laws, regulatory frameworks, and self-regulation within the industry. Part III will first survey the problems posed by location-based services, then analyze the benefits and detriments of proposed attempts to govern the industry. Finally, Part IV of this Recent Development will suggest what kinds of actions are needed to protect the public from the threats raised by location-based services, using recent reforms in the European Union as a guide.

II. BACKGROUND

This section will briefly discuss how LBS have developed and how the third parties use these technologies, then examine the real risks of LBS, evidence of those risks in recent years, and current attempts to regulate LBS to prevent future damage.

A. Evolution of Location-Based Services

Early LBS revolved around the Federal Communications Commission's (FCC) Enhanced 911 (E911) regulation of 1997, which required the cellular telephone industry to implement a system through which LBS could determine the location of a cellular phone within several hundred feet.[11] It did not take long for mobile service providers to realize that the same technology required by the FCC's E911 regulation could also enhance a user's experience of owning a cellular phone.[12] Now, fifteen years after E911 took effect, mobile devices are no longer "tracking devices" only after an emergency call, but also when a user wants to find the nearest coffee shop.[13] LBS, attacked even in their inception as emergency services, have proliferated to the point that sensitive data about millions of users can be compromised simply because those users are looking for a good place to eat.[14]

B. Types of LBS-Enabling Technology

There are many ways to break down the various technologies that enable LBS and thus make it such a thriving field. In the interest of simplicity, this Recent Development will take its lead from Lorrie Cranor, professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon

11. *See* Aaron Futch & Christine Soares, *Enhanced 911 Technology & Privacy Concerns: How Has the Balance Changed Since September 11?*, 2001 DUKE L. & TECH. REV. 38, 38 (noting that despite the apparent advantages of improving the response capabilities of emergency personnel, privacy groups were reluctant to submit "for fear that cellular phones might be turned into tracking devices for the benefit of both the government and private businesses").

12. *See* Gerry Christensen, *Evolution of Mobile Positioning and Location-Based Services*, EOGOGICS, http://www.eogogics.com/talkgogics/blog/LBS (last visited Sept. 18, 2012) (explaining how the technology could be used for navigation or finding nearby amenities).

13. Futch & Soares, *supra* note 11, at 38.

14. *See* Thurm & Kane, *supra* note 7 (referencing the findings of a Wall Street Journal investigation revealing the intrusive efforts by online-tracking companies to gather personal data from iPhone and Android users). See King, *supra* note 7, at 127, Tsai et al., *supra* note 7, at 127, and Edmundson, *supra* note 7, at 212 for other examples of intrusive behavior.

University.[15] In her research and her testimony for a collection of House committees examining LBS and consumer protection, Cranor uses four categories to view these methods.[16] First, the GPS method locates users through a device that triangulates a location based on signals it receives from a constellation of satellites.[17] Second, wireless positioning locates users by listening for signals or nearby WiFi access points and sending information about detected signals to a service that maintains a database of access point locations.[18] Third, cellular identification locates a user by triangulating their position based on cellular towers within signal range of their mobile phone.[19] Cellular identification is effective even when phones are not being used to place a call.[20] Finally, IP location locates a user by looking up the Internet protocol address of the user's device in a database that maps IP addresses to geographic locations. This does not yield as precise information about a user's location as other methods.[21]

C. The Risks of LBS

The risk of LBS is, generally, that the user's private information will be collected or shared without his or her knowledge or consent, then misused for purposes of which the user disapproves.[22]

1. Unwanted Eavesdropping or Tracking

Users of LBS risk their personal safety when unwanted third parties access their location information without their consent or knowledge. For example, location data willingly surrendered to an application like Foursquare has been accessed by other applications, including one called Girls Around Me, which used that information "to provide voyeuristic, opportunistic gentlemen the chance to scope out local women."[23] LBS also have made it easy for abusers to track their victims, with more than 25,000 adult victims of GPS stalking each year according to a U.S. Department of Justice report.[24]

15. LORRIE FAITH CRANOR, http://lorrie.cranor.org/bio.html (last visited Sept. 18, 2012).
16. Tsai et al., *supra* note 7, at 127.
17. *Id.*
18. *Id.* at 121–22.
19. *Id.* at 122.
20. *Id.* at 123.
21. *Id.*
22. King, *supra* note 7, at 138. This risk is distinct from simple oversharing, which is hardly exclusive to LBS. If a user indicates that he will be out of town for a week on a platform that also provides his home address and his home is burglarized while he is away, that is a product of poor judgment, not an LBS privacy issue. However, in some situations, a user can share his or her location and be unaware that third parties have access to such information. This Recent Development focuses on the latter problem.
23. Christina Bonnington, *How Location-Based Apps Can Stave Off the 'Creepy Factor'*, WIRED (Apr. 3, 2012, 5:57 PM), http://www.wired.com/gadgetlab/2012/04/location-based-app-creepiness/. Foursquare has revoked its application programming interface (API) access from Girls Around Me because such use violated its terms. *Id.*
24. KATRINA BAUM ET AL., U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE SPECIAL REPORT: STALKING VICTIMIZATION IN THE UNITED STATES 5 (2009); *see also* Justin Scheck, *Stalkers Exploit Cellphone GPS*, WALL ST. J. (Aug. 3, 2010, 7:44 PM), http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html (citing the report and describing some real-life consequences of GPS-

Presumably, many more people are stalked today because the means to do so are readily available. Misuse of personal information also includes unwanted tracking by employers or family members.[25]

> [W]e see that the top ranked expected risks are the following: revealing the location of your home to people you do not want to give your address to; being stalked; having people intrude on your private space; being found by someone you don't want to see; being found when you want to be alone; having the government track you; and being bothered by ads that use your location.[26]

Such risk is of mounting importance because of the exponential increase of minors with access to mobile devices equipped with LBS technology.[27] This Recent Development makes no judgment about the democratization of this technology except to point out that it has made a whole new population susceptible to the dangers of LBS. The dangers LBS pose to children was highlighted by the case of Skout, a flirting app that has been connected to three men accused of raping children they met using the service.[28]

2. Lack of Transparency and Security

Despite moderate efforts of some application providers to make using LBS more transparent,[29] many consumers still do not understand the risk exposure when they sign up.[30] Even if users understand that their location is

---

enabled stalking).

25. *See* Francoise Gilbert, *No Place to Hide? Compliance & Contractual Issues in the Use of Location-Aware Technologies*, 11 J. INTERNET L. 3, 10 (2007) (explaining that employers could use the technology to monitor when employees are "wandering" the building or in a cafeteria instead of their work spaces); Jill Yung, *Big Brother Is Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It*, 36 SETON HALL L. REV. 163, 165 (2005) ("Because GPS tracking systems can, have, and likely will continue to capture off-duty movements of employees, this form of surveillance is more nefarious than the types of employee monitoring programs debated elsewhere.").

26. Tsai et al., *supra* note 7, at 147.

27. *See* COMMON SENSE MEDIA RESEARCH, ZERO TO EIGHT: CHILDREN'S MEDIA USE IN AMERICA 9 (2011) (indicating that 52% of all children under the age of eight have access to mobile devices at home); FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING 4 (2012) (indicating that nearly 12,000 apps target kids across the Apple App Store and the Android Market, and concluding that "parents generally cannot determine, before downloading an app, whether the app poses risks related to the collection, use, and sharing of their children's personal information"); JOHN MORRIS, CTR. FOR DEMOCRACY & TECH., THE PRIVACY IMPLICATIONS OF COMMERCIAL LOCATION-BASED SERVICES 3 (2010) ("[A]s an increasing number of minors carry location-capable cell phones and devices, location privacy will become a child safety matter . . . ."); Jack Neff, *CyberTots: Pre-teens Drive iPad Purchases, Join Social Networks*, ADVERTISING AGE (Apr. 20, 2011), http://adage.com/article/news/pre-teens-drive-ipad-purchases-join-social-networks/227101/ (indicating that by age 11 half of children have their own mobile phones).

28. Nicole Perlroth, *After Rapes Involving Children, Skout, a Flirting App, Bans Minors*, N.Y. TIMES (June 12, 2012, 9:13 PM), http://bits.blogs.nytimes.com/2012/06/12/after-rapes-involving-children-skout-a-flirting-app-faces-crisis/. In each case, the victim agreed to meet with the offender, making this as much an oversharing issue as an LBS one. *Id.* However, Skout was sharing the victim's location with the offenders, and its decision to suspend the service for minors indicates an acknowledgement that better safeguards are necessary. *Id.*

29. *See, e.g.*, *Location-based services*, GOOGLE MAPS: HELP, http://support.google.com/maps/bin/answer.py?hl=en&answer=1725632 (last visited Sept. 18, 2012) (explaining how Google Maps' Google Location Server does not identify people and indicating how a user can opt out of the company's LBS services).

30. Gilbert, *supra* note 25, at 5 ("Many individuals are not aware of the existence of products bearing

being tracked by their mobile service provider and perhaps the developer of that particular application, they are unlikely to know where that information goes, how long it is stored, who has access to it, and how—or if—it is encrypted or anonymized.[31] The gathering and storage of such information increases the chances of unwanted exposure of a user's information, leaving them vulnerable to anything from credit card fraud to identity theft.[32]

3. Market Risks

Companies trying to use LBS to their advantage run the risk of going too far and violating users' trust. If they fail to adequately protect users' privacy, they could face a backlash. Professor Cranor's research supports this theory, concluding that people value their location privacy, are less comfortable sharing their location with strangers than with people they know, and want greater control of their location information.[33] A group of privacy and consumer organizations made the same argument in a letter urging U.S. Senators to adopt privacy protection legislation.[34]

> First, it is the technology of privacy that has turned the Internet . . . into the most robust platform for commercial activity in the world today. Without the safeguards made possible by encryption, and other privacy enhancing techniques, no consumer would dare provide a credit card number or personal information when connected to an unknown computer in a remote location. Second, privacy laws also encourage companies to develop services that minimize reliance on personal information while promoting a new business service or business model.[35]

Because privacy controls can be integral to expansion of commerce, ineffective controls create a risk of economic stagnation. Furthermore, because LBS use

---

RFID tags. Nor do they suspect that the so-convenient location-based services with travel or direction information may be recording their travel patterns. Without the proper safeguards, personal information may be collected without the user's consent. As a result, individuals cannot control whether information is collected or who has access to the location information and other information, whether for direct uses or for secondary uses."); Robert Siciliano, *Are Your Mobile Apps up to no Good?*, MCAFEE BLOG CENTRAL (Aug. 22, 2012, 5:36 AM), http://blogs.mcafee.com/consumer/are-your-mobile-apps-up-to-no-good ("What's troubling is that 33% of apps ask for more permissions than they need, 42% of users don't know what these permissions are and 84% of users don't pay attention to permissions when installing an app.").

31. Meleske, *Privacy Concerns*, *supra* note 4.

32. JANET JAISWAL & SAIRA NAYAK, TRUSTE, LOCATION-AWARE MOBILE APPLICATIONS: PRIVACY CONCERNS AND BEST PRACTICES 5 (2010), *available at* http://www.truste.com/pdf/Location_Aware_Mobile_Applications.pdf. Interestingly, LBS can also help prevent credit card fraud by providing a user's bank with location information and allowing the bank to prevent access to credit if someone tries to use the card in a spot that does not match the user's location. Users would still be vulnerable to credit card fraud if both their credit card and their mobile device are stolen, but that is not an LBS issue. Cynthia J. Larose, *Top 5 Commercial Data Security and Privacy Issues in 2012*, THOMSON REUTERS: NEWS & INSIGHT (Jan. 30, 2012), http://newsandinsight.thomsonreuters.com/Legal/Insight/2012/01_-_January/Top_5_commercial_data_security_and_privacy_issues_in_2012/.

33. Janice Y. Tsai et al., *Who's Viewed You? The Impact of Feedback in a Mobile Location-Sharing Application*, *in* CHI 2009 CONFERENCE PROCEEDINGS, PAPERS & NOTES 2003–12 (2009).

34. Letter from Am. Civil Liberties Union et al., to U.S. Senators John D. Rockefeller and Kay Bailey Hutchison (July 1, 2011), *available at* http://www.centerfordigitaldemocracy.org/sites/default/files/Privacy%20Groups%20Letter%20to%20US%20Congress%207.1.11.pdf.

35. *Id.*

is increasing exponentially in spite of the privacy concerns, a legal solution is necessary.

D. Evidence of Data Leaks

Problems like the ones described above are not rare. In April 2011, security experts discovered that iPhones and iPads were storing unencrypted and unprotected time-stamped lists of locations visited by the device's owners.[36] Google—like Apple, a major player in LBS—recently reached a settlement for privacy concerns surrounding the rollout of its social network Buzz in 2010.[37] The Federal Trade Commission (FTC) said in a statement that Google "used deceptive tactics and violated its own privacy promises to consumers" when it launched Buzz.[38] Facebook reached a similar settlement with the FTC after charges that it deceived consumers by telling them they could keep their information on Facebook private and then "repeatedly allowing it to be shared and made public."[39]

Third-party developers also have significant access to user information, and they have not yet shown a commitment to protecting it. In a test of 101 popular smartphone applications in late 2010, the Wall Street Journal found that "Fifty-six [apps] transmitted the phone's unique device ID to other companies without users' awareness or consent. Forty-seven apps transmitted the phone's location in some way. Five sent age, gender and other personal details to outsiders."[40] Also in 2010, an examination of eighty-nine applications found that "only 66% of the applications had privacy policies at all."[41] Among those that did have privacy policies, most collected and saved data including locations, personal profile information, and identifying web information like IP addresses—all for an indefinite period of time.[42] Additionally, where privacy controls existed, they were not easily accessible, usually requiring clicking through multiple screens before giving users the ability to modify their settings.[43]

---

36. Miguel Helft, *Jobs Says Apple Made Mistakes with iPhone Data*, N.Y. TIMES, Apr. 27, 2011, http://www.nytimes.com/2011/04/28/technology/28apple.html.

37. Press Release, Fed. Trade Comm'n, FTC Gives Final Approval to Settlement with Google over Buzz Rollout (Oct. 24, 2011), *available at* http://ftc.gov/opa/2011/10/buzz.shtm; *see* Seth Weintraub, *Google Reaches Agreement with FTC over Buzz*, CNN MONEY (Mar. 30, 2011, 11:01 AM), http://tech.fortune.cnn.com/2011/03/30/google-reaches-agreement-with-ftc-over-the-buzz-release (explaining that if Google Buzz users did not change their default settings, Google displayed a list of users' Gmail contacts in their profiles).

38. Press Release, Fed. Trade Comm'n, *supra* note 37.

39. Press Release, Claudia Bourne Farrell, Fed. Trade Comm'n, Facebook Settles FTC Charges that it Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), *available at* http://ftc.gov/opa/2011/11/privacysettlement.shtm. The FTC's complaint against Facebook listed eight counts, including one that charged the social media giant with sharing nearly all of users' personal data with third-party applications despite expressly stating otherwise. *Id.* Another count claimed that Facebook's "Verified Apps" program, which claimed to certify the security of participating applications, did no such thing. *Id.*

40. Thurm & Kane, *supra* note 7.

41. Tsai et al., *supra* note 7, at 131.

42. *Id.*

43. *Id.* at 132.

E. Current and Proposed Frameworks for Governing LBS

To their credit, legislators, regulators, and industry officials seem to recognize that LBS privacy controls are inadequate as currently designed.[44] This section of the Recent Development will explain the various steps Congress and regulatory agencies are considering protecting LBS users.

1. Self-Regulation

CTIA—The Wireless Association (CTIA), an industry trade group, handles current regulation of LBS.[45] The organization does so through its Best Practices and Guidelines for Location-Based Services.[46] These guidelines, which cover mobile carriers and application developers, revolve around the principles of user notification and user consent.[47] They emphasize that users should know how and when their data is collected and they should have the option to deactivate any location-tracking features.[48] The guidelines are intended to "promote and protect user privacy as new and exciting [LBS] . . . are developed and deployed."[49] However, because the guidelines are not mandatory, it is unclear if companies explicitly follow them often, if ever.

---

44. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at i (2012) [hereinafter FED. TRADE COMM'N, RECOMMENDATIONS], *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf ("[C]ompanies are collecting, storing, and sharing more information about consumers than ever before. Although companies use this information to innovate and deliver better products and services to consumers, they should not do so at the expense of consumer privacy."); THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, at i (2012), *available at* http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf ("When consumers provide information about themselves . . . they reasonably expect companies to use this information in ways that are consistent with the surrounding context. Many companies live up to these expectations, but some do not. Neither consumers nor companies have a clear set of ground rules to apply in the commercial arena."); WIRELESS TELECOMMS. BUREAU, FED. COMMC'NS. COMM'N, LOCATION-BASED SERVICES: AN OVERVIEW OF OPPORTUNITIES AND OTHER CONSIDERATIONS 1 (2012) [hereinafter FED. COMMC'NS COMM'N, LOCATION-BASED SERVICES], *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-314283A1.pdf ("[M]obile devices . . . enable the creation of a precise record of a user's locations over time. This can result in the creation of a very accurate and highly personal user profile, which raises questions of how, when and by whom this information can and should be used."); Jim Puzzanghera, *Apple, Google Try to Ease Lawmakers' Privacy Concerns*, L.A. TIMES, May 10, 2011, http://articles.latimes.com/2011/may/10/business/la-fi-privacy-20110511 ("Members of a Senate privacy subcommittee remained uneasy during a hearing Tuesday as Apple and Google executives defended their companies' practices while privacy and law enforcement experts warned that identity thieves, stalkers and other criminals still could obtain information about where people are and at what time."); Melissa Maleske, *LBS on the Hill*, INSIDECOUNSEL (Sept. 1, 2011), http://www.insidecounsel.com/2011/09/01/lbs-on-the-hill [hereinafter Maleske, *LBS on the Hill*] ("[A] Senate committee in May held hearings on [LBS], grilling Apple and Google on their privacy practices. In June, lawmakers on Capitol Hill introduced three bills that address LBS.").

45. *See* Maleske, *Privacy Concerns*, *supra* note 4 ("Absent clear rules or authority, the industry has taken to self-regulation. A few years ago, CTIA—The Wireless Association, an industry trade group, adopted a set of best practices to which carriers as well as app developers now broadly subscribe.").

46. *See* CTIA—THE WIRELESS ASS'N, *supra* note 3, at 1 ("CTIA Best Practices and Guidelines . . . are intended to promote and protect user privacy as . . . [LBS] . . . are developed and deployed.").

47. *Id.* at 1.

48. *Id.*; Maleske, *Privacy Concerns*, *supra* note 4.

49. CTIA—THE WIRELESS ASS'N, *supra* note 3, at 1.

2. Proposed Legislation

While no enacted legislation directly addresses LBS, several politicians have introduced bills that would tackle this technology. Senators John McCain and John Kerry introduced, in April 2011, a broad privacy bill called the Commercial Privacy Bill of Rights.[50] The bill calls for collectors of information to implement security measures to protect information they hold on to and provide clear notice to individuals on how and why that information is collected.[51]

Other attempts at legislation have taken a narrower approach, addressing LBS specifically. Senators Al Franken and Richard Blumenthal aim to close current loopholes in federal law with the Location Privacy Protection Act introduced in June 2011.[52] The bill proposes that LBS providers be required to obtain "express authorization" to collect and share location data from customers.[53] The Geolocational Privacy and Surveillance Act (GPS Act) attempts to establish a uniform standard for allowing government and law enforcement access to geolocation data.[54] It resembles the Franken-Blumenthal bill in that it requires user consent before collecting, using, or disclosing data, but differs in that it applies not only to commercial service providers but also government entities.[55]

3. Federal Regulation

In addition to legislative activity, federal regulators are stepping up to potentially play a key role in governing LBS. The FTC and the FCC have published recommendations this year, and the White House weighed in with a report in February.[56] The FTC has been examining the issues since 2008, seeking to protect consumers' privacy through two primary models: the notice-and-choice model and the harm-based model, each of which has its own flaws.[57]

The FTC seems to have improved on those models with their March report on protecting digital privacy.[58] The FTC's recommended approach

---

50. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011).

51. *Id.* §§ 101, 201.

52. Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011).

53. S. 1223 § 3 (defining "express authorization" as "affirmative consent after receiving clear and prominent notice" about what will be collected and to whom it will be disclosed).

54. Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011); *Frequently Asked Questions on Geolocation and the GPS Act*, WYDEN.SENATE.GOV, http://www.wyden.senate.gov/priorities/gps-act (last visited Sept. 5, 2012).

55. Maleske, *Privacy Concerns*, *supra* note 4.

56. *See generally* FED. COMMC'NS COMM'N, LOCATION-BASED SERVICES, *supra* note 44; FED. TRADE COMM'N, RECOMMENDATIONS, *supra* note 44; THE WHITE HOUSE, *supra* note 44.

57. FED. TRADE COMM'N., RECOMMENDATIONS, *supra* note 44, at 2. The notice-and-choice model "encourage[s] companies to develop privacy policies describing their information collection and use practices," but that led to "long, incomprehensible policies that consumers typically do not read, let alone understand." *Id.* The harm-based approach focuses on preventing specific harms like "physical security, economic injury and unwanted intrusions into [users'] daily lives," but it "fail[ed] to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored." *Id.*

58. *See id.* at 2–3 (listing the FTC's reform proposals).

hinges on widespread regulation that covers all commercial entities that could be linked to a specific consumer or device, simplified consumer choice, and increased transparency.[59] To accomplish those goals, the FTC proposed a "Do Not Track" list, which would serve as the blanket opt-out, or a "mechanism to allow consumers to control the collection and use of their online browsing data," mobile or otherwise.[60] According to the FTC's preliminary report, such a measure would be "[t]he most practical method of providing uniform choice for online behavioral advertising."[61]

Despite the far-reaching FTC recommendations, ultimately one entity alone will not effectively protect LBS users. The FTC acknowledged as much in its report, calling on Congress to enact "baseline privacy legislation" and noting that the FTC recommendations hope to spur better self-regulation in the industry.[62]

III. ANALYSIS

As noted above, location-based services pose new and significant challenges for governments and regulatory systems that were already struggling to keep up with previous generations of technological advancement. This part will discuss the advantages and disadvantages of various measures to improve privacy protection and examine the proper roles for the legislature, regulatory agencies, and the industry itself in dealing with the proliferation of LBS.

A. The Legislature

1. Legislation Generally

Various legislative proposals have admirably recognized the risks of LBS and tried to address them with new standards for mobile service providers and application developers. Unfortunately, the standard critique of legislative action on technology remains true in this case. Congress simply cannot act quickly enough for legislation to keep up with the pace of technology. Despite the best efforts of certain members of Congress, "technology has far outpaced the statutory protections, both regarding use of location in the commercial context, as well as protection of location from unwarranted government access."[63] There is little hope that Congress will be able to catch up either, as technology continues to advance rapidly and Congress still ponders whether it should step into the LBS arena.

---

59. *Id.* at vii–ix.

60. *Id.* at 4.

61. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, at vii (2010) [hereinafter FED. TRADE COMM'N, PROPOSED FRAMEWORK].

62. FED. TRADE COMM'N, RECOMMENDATIONS, *supra* note 44, at vii–ix.

63. MORRIS, *supra* 27, at 6.

2. Specific Proposed Laws

Each of the proposed bills to legislate LBS—while well-intentioned—is flawed in its own way.

The Commercial Privacy Bill of Rights (McCain-Kerry) fails to sufficiently protect consumers. First, it does not offer a "Do Not Track" option as proposed by the FTC.[64] A "Do Not Track" provision could give users a simple and clear way to opt out of being tracked online and via LBS.[65] Second, the bill treats Facebook and other social media marketers as special interests, allowing them to track users without proper safeguards.[66] This is an obvious flaw considering that social media marketers have been some of the biggest violators of privacy rights to date.[67] Third, the bill does not include a consumer right of action when privacy rights are violated.[68] A proper legislative framework for governing LBS must give consumers "the right to hold companies accountable for violating their privacy through a private right of action."[69] Finally, the bill usurps the FTC's lead role in protecting privacy and turns it over to the Department of Commerce.[70] The Department of Commerce seeks to promote the interests of business and therefore has a clear conflict of interest when asked to be the primary protector of consumer interests.[71]

The Location Privacy Protection Act (Franken-Blumenthal) targets LBS specifically and thus offers far more protection than the Commercial Privacy Bill of Rights.[72] For instance, one of the advantages of this bill is that it makes companies respond to consumer inquiry regarding whether they have certain location information and delete such information upon request.[73] But this proposal is still an imperfect framework for privacy protection for two reasons. First, critics are calling the private right of action the "glaring flaw" of the bill, saying it would give plaintiff's attorneys incentive to sue leading tech companies for huge amounts over what could be minor geolocation

64. *Consumer Groups Welcome Bipartisan Privacy Effort, But Warn Kerry-McCain Bill Insufficient to Protect Consumers' Online Privacy*, CENT. FOR DIGITAL DEMOCRACY (Apr. 18, 2011), http://www.democraticmedia.org/consumer-groups-welcome-bipartisan-privacy-effort-warn-kerry-mccain-bill-insufficient-protect-consum.

65. FED. TRADE COMM'N, PROPOSED FRAMEWORK, *supra* note 61, at 66–67.

66. *Consumer Groups Welcome Bipartisan Privacy Effort, but Warn Kerry-McCain Bill Insufficient to Protect Consumers' Online Privacy*, *supra* note 64.

67. *See generally* David Sarno, *Twitter Stores Full iPhone Contact List for 18 Months, After Scan*, L.A. TIMES, Feb. 14, 2012, http://www.latimes.com/business/technology/la-fi-tn-twitter-contacts-20120214,0,5579919.story; Weintraub, *supra* note 37; Press Release, Claudia Bourne Farrell, *supra* note 39; Press Release, Fed. Trade Comm'n, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Info. (Mar. 11, 2011), *available at* http://www.ftc.gov/opa/2011/03/twitter.shtm.

68. *Consumer Groups Welcome Bipartisan Privacy Effort, But Warn Kerry-McCain Bill Insufficient to Protect Consumers' Online Privacy*, *supra* note 64.

69. *Id.*

70. *Id.*

71. *Id.*

72. *See* Maleske, *LBS on the Hill*, *supra* note 44 (describing The Commercial Privacy Bill of Rights as "broader privacy legislation").

73. Hunton & Williams LLP, *Senators Franken and Blumenthal Co-Sponsor Location Privacy Protection Act*, PRIVACY & INFO. SECURITY L. BLOG (June 16, 2011), http://www.huntonprivacyblog.com/2011/06/articles/senators-franken-and-blumenthal-co-sponsor-location-privacy-protection-act/.

violations.[74] There has to be middle ground between this universal right of action and the complete forfeiture of a right of action as included in the McCain-Kerry bill. Second, there is no blanket opt-out option.[75] A blanket opt-out remains the simplest and clearest way to attain privacy protection.

The GPS Act (Wyden-Chaffetz-Goodlatte) differs from the Location Privacy Protection Act in that it applies to commercial service providers and government agencies, while the Franken-Blumenthal bill addresses only the former.[76] The GPS Act would create a "clear, uniform standard for government access to geolocation data" for use in tracking suspects, lending clarity to law enforcement and to private companies about when such sharing is appropriate and lawful.[77] Such clarity is lacking, even after the Supreme Court's recent holding that using a GPS tracking device to monitor a vehicle's movements on public streets is a search within the meaning of the Fourth Amendment.[78] Definitive guidelines on when location information can be shared with law enforcement is likewise helpful for private companies that collect and store such information.[79] Also, by creating criminal penalties for "surreptitiously using an electronic device to track a person's movement," the bill attempts to address the risk of GPS stalking.[80] However, the GPS Act falls substantially short of protecting users from the risks of LBS because it fails to address the problems of prolonged data storage and accidental data leaks.[81] Furthermore, the lack of a universal opt-out remains problematic.

The takeaway from this analysis is that legislation alone cannot and will not adequately protect consumer privacy in a world of ever-expanding LBS. That said, the legislature still has its place in an effective LBS governance regime. Without Congress taking the lead, the industry will not follow. Legislation should provide an effective framework beyond which the industry and regulatory agencies should fill in the gaps.

---

74. Tony Romm, *Franken, Blumenthal Introduce Privacy Bill*, POLITICO (June 15, 2011, 9:19 PM), http://www.politico.com/news/stories/0611/57062.html (quoting Steve DelBianco). DelBianco, executive director of NetChoice, a coalition promoting convenience, choice, and commerce on the Internet, has said that a violation could arise even when collectors of LBS data share with parents the geolocation of their children with smartphones. *Id.*

75. *See generally* Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011).

76. Jacqui Cheng, *Franken's Location-Privacy Bill Would Close Mobile-Tracking 'Loopholes'*, WIRED (June 17, 2011, 11:55 AM), http://www.wired.com/epicenter/2011/06/franken-location-loopholes/.

77. Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011); *Frequently Asked Questions on Geolocation and the GPS Act*, RON WYDEN: SENATOR FOR OREGON, http://www.wyden.senate.gov/priorities/gps-act (last visited Sept. 18, 2012). Without the Act, "[j]udges in different jurisdictions have issued conflicting rulings about what procedures law enforcement must follow—and how much evidence is necessary—to obtain individuals' geolocation data from private companies. This lack of clarity creates problems for law enforcement agencies and private companies, as well as uncertainty for customers." *Id.*

78. United States v. Jones, 132 S. Ct. 945, 946 (2012); RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R42511, *UNITED STATES V. JONES*: GPS MONITORING, PROPERTY, AND PRIVACY 2 (2012).

79. H.R. 2168; *Frequently Asked Questions on Geolocation and the GPS Act*, *supra* note 77.

80. *Frequently Asked Questions on Geolocation and the GPS Act*, *supra* note 77.

81. H.R. 2168. While the Act makes intentional sharing of geolocational information illegal, it does not address unintentional sharing, which is the heart of the LBS issue. *Id.*

B. The Regulatory Agencies

The FTC's proposal is crucial to effective governance of LBS. Its focus on simplicity and transparency and its abilities to enforce those principles in ways the industry currently cannot, are potential game-changers in an industry that to this point has relied on user ignorance or apathy to profit financially. The proposed "Do Not Track" list is the most obvious embodiment of the twin goals of simplicity and transparency. Designed as a user-friendly method to stop all LBS data collection and sharing, this universal option is perhaps the most important tool in the privacy protection belt. The "Do Not Track" provision would involve placing a persistent setting, like a cookie, on a consumer's web browser or mobile device signaling the user's choice to opt out of all tracking.[82] It would prevent users from having to make individual choices for every company or application.[83] It would also address the fact that those individual choices cannot always be trusted because different companies offer different mechanisms for privacy protection, and some are not as thorough or as effective as others.[84]

Though a step in the right direction, the FTC's proposal is not without its flaws. For one, businesses are concerned about a potential chilling effect on LBS. Without intrusive regulation, LBS helps "fund a variety of personalized content and services, but also allows businesses to innovate and develop new products and services that offer consumers convenience and cost savings."[85] Such benefits are naturally limited when regulation increases. As the widest-reaching proposal of LBS regulation in the United States to date, the FTC recommendations could prevent providers from taking advantage of their technology, which might not be better for consumers in the end.[86] A stall in technological advancement could cost consumers the benefit of the ever-growing list of services that in recent years have come to allow people to find friends and relatives in an emergency, to interact with their environment, and to take advantage of a more personalized consumer experience.[87]

A final hurdle deals with the role of the FCC in the regulatory framework. Historically, the FTC has served as the watchdog for general privacy and data security.[88] However, the FTC "is restricted by statute from regulating common carriers, including telecommunications common carriers, which fall under the FCC's jurisdiction."[89] The industry, not surprisingly, would rather work with one agency than two.[90] As such, streamlining the regulatory framework would be essential to effective governance of LBS. This will be discussed in greater

82. FED. TRADE COMM'N, PROPOSED FRAMEWORK, *supra* note 61, at 66.
83. *Id.* at 66–67.
84. *Id.* at 67.
85. *Id.* at iv.
86. Adam Thierer, *Initial Thoughts on FTC's Final Privacy Report*, TECH. LIBERATION FRONT BLOG (Mar. 26, 2012), http://techliberation.com/2012/03/26/initial-thoughts-on-ftcs-final-privacy-report/.
87. *Id.*
88. *See generally* FED. TRADE COMM'N, PROPOSED FRAMEWORK, *supra* note 61, at 3–6 (providing historical background to the FTC's focus on privacy issues).
89. Maleske, *Privacy Concerns*, *supra* note 4.
90. *Id.*

detail in Part IV.

C. The Industry

Regulation from within the industry often works where the legislature fails. The industry is in a better position to keep up with rapidly advancing technologies and amend its rules to accommodate those changes.[91] In fact, CTIA is currently making changes to its guidelines, a process that figures to be far easier and quicker than legislative amendment.[92]

The industry's self-regulated model of privacy protection has fallen short of adequate protection, as evidenced by the breaches of privacy protection that occur with regularity in today's system. CTIA's guidelines fall short in four main respects. First, they are not mandatory, so they cannot be effectively enforced.[93] Second, though they require notice and consent about location use and disclosure, they do not specify how those notices are delivered or what is required of them.[94] Third, if user information is compromised, the CTIA guidelines do not recommend steps to be taken to notify users.[95] Users might be left unaware that they are vulnerable until the offender reaches its settlement with the FTC. Finally, CTIA's guidelines have been unevenly implemented in third-party applications.[96]

Though industry regulation is an essential part of an effective system to protect consumers, such a system requires external efforts as well, as evidenced by the privacy breaches that occur so regularly now[97] without an effective deterrent. As long as breaches of consumer privacy are commonplace, consumers are not safe. Based on the failures of industry giants like Facebook, Apple, and Google, all within the last several years,[98] it is safe to assume that the industry cannot continue as the only party charged with regulating LBS.

---

91. *See generally* CTIA—THE WIRELESS ASS'N, *supra* note 3.

92. Christine Mumford, *U.S. Mobile Device Location Data Privacy Debate Considers EU, Industry-Based*, *in* 5 WCRR 24 (2010).

93. *See generally* CTIA—THE WIRELESS ASS'N, *supra* note 3 ("The Guidelines encourage LBS Providers to develop and deploy new technology to empower users to exercise control over their location information . . . ."); Maleske, *Privacy Concerns*, *supra* note 4.

94. *See generally The Collection and Use of Location Information for Commercial Purposes: Hearing Before the H. Energy and Commerce Committee's Subcommittees on Communications, Technology and the Internet and Commerce, Trade and Consumer Protection*, 111th Cong. (2010) (statement of Lorrie Faith Cranor, Associate Professor of Computer Science and of Engineering & Public Policy, Carnegie Mellon University).

95. *Id*.

96. Maleske, *Privacy Concerns*, *supra* note 4; *see also* Tsai et al., *supra* note 7, at 127 (stating that some applications are more flexible than others); Thurm & Kane, *supra* note 7 (describing the different ways that applications have applied the guidelines).

97. David Kravets, *FTC Slaps Myspace for Privacy Breaches*, WIRED (May 8, 2012, 3:36 PM), http://www.wired.com/threatlevel/2012/05/ftc-myspace-slap/ ("Federal regulators slapped Myspace's wrist Tuesday, finding that the company still exists and that it violated the privacy promises it made to its 10 remaining users.").

98. Sara Forden, *Google Said to Face Fine by U.S. over Apple Safari Breach*, BLOOMBERGBUSINESSWEEK (Aug. 9, 2012), http://www.businessweek.com/news/2012-08-09/google-said-to-face-fine-by-u-dot-s-dot-over-apple-safari-breach#p1.

IV. RECOMMENDATION

Having surveyed many potential approaches for governing the new challenges of LBS raised by the proliferation of applications and third-party developers, we are left with the question of which of these approaches best protects consumers' privacy without creating a chilling effect on the advantages of LBS and geolocational technology.

The first approach is a legislative strategy that could take any number of different forms to rein in the rampant oversharing of LBS data. The second approach is a regulatory approach in which the FTC, perhaps with assistance from the FCC, implements its own plan of action. The third approach is an industry-guided system of best practices.

A. Looking to the European Model

Where the isolated efforts of various regulating bodies are insufficient to fix a problem, a hybrid approach could be the answer. Here, European law regarding LBS and consumer privacy is instructive. The European Union approach features "comprehensive national laws, prohibitions against collection of data without a consumer's consent and requiring companies that process data to register their activities with government authorities."[99] This is "in stark contrast to the U.S. approach, which to date has been more ad hoc and industry-based."[100] In addition to its already consumer-friendly approach, the European Union proposed reforms to its data privacy protection scheme in January 2012 seeking to strengthen privacy rights, streamline regulation, and boost the digital economy.[101] The European Commission, which proposed the changes, aims for the reforms to make data protection in the European Union "future-proof and fit for the digital age."[102]

Specifically, European law contemplates six features of privacy protection that should also be at the core of the United States' scheme. Each feature is outlined below.

1. Explicit and Affirmative Consent

The European Union's directive requires user consent before any LBS data is collected, "the contours of which [the law] sets out in some detail."[103]

99. Cynthia J. Larose, Esq., *Top 5 Commercial Data Security and Privacy Issues in 2012*, THOMSON REUTERS: NEWS & INSIGHT (Jan. 30, 2012), http://newsandinsight.thomsonreuters.com/Legal/Insight/2012/01__January/Top_5_commercial_data_security_and_privacy_issues_in_2012.

100. *Id.*

101. Press Release, European Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012) [hereinafter EU Press Release I], *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46.

102. Press Release, European Comm'n, Why Do We Need an EU Data Protection Reform? (Jan. 25, 2012) [hereinafter EU Press Release II], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf.

103. Christine Mumford, *Location Privacy Advocates Draw Lessons from European, Industry-Based Approaches*, 5 Electronic Com. & L. Rep. Online (BNA) 413 (Mar. 17, 2010).

Location data may only be processed "with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service."[104] Such a clear guideline prevents misuse of data after use for relevant LBS purposes. Also, such consent must be explicitly provided—it cannot be assumed.[105] In the United States, under the current CTIA Guidelines, consent can be implicit or obtained as part of an agreement to general terms and conditions.[106] Furthermore, consent in Europe "requires informing the user of the type of data, the purpose of the collection, the duration of the collection and whether a third party will be doing the processing."[107] That final term is especially important in this new age of applications, in which third parties are more prevalent and often more mysterious and less accountable than other parties.[108]

2. Withdrawal of Consent

The EU directive also allows users to withdraw their consent at any time, "even on a case-by-case basis."[109] This so-called "right to be forgotten" is critical to a data protection regime because it allows users to better manage their risks.[110] Additionally, "there must be a simple and free means for a user to refuse the processing of location data for a specific connection or transmission."[111] When data is no longer useful for processing legitimate LBS services, then "there are no legitimate grounds for" the service providers retaining that information and the user can demand that it be deleted.[112] Like the requirement for explicit and affirmative consent, this ability to withdraw consent is essential for users to understand and manage the risks of privacy breaches when it comes to their location information. The CTIA guidelines have no such limitation on service providers holding onto user information. To its credit, the Location Privacy Protection Act proposed by Sens. Franken and Blumenthal incorporates a provision that allows for withdrawal of consent.[113]

3. Users' Access to Their Own Data

The European law also allows people easier access to their own data and the ability to transfer personal data between service providers.[114] Such

104. *Id.*
105. EU Press Release II, *supra* note 102.
106. CTIA—THE WIRELESS ASS'N, *supra* note 3, at 5.
107. Marc Rotenberg et al., Elec. Privacy Info. Ctr., Statement Before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary 8 (May 17, 2012), *available at* http://epic.org/privacy/location_privacy/EPIC-Location-Privacy-Statement-5-17-12.pdf.
108. *Id.*
109. Mumford, *supra* note 103.
110. EU Press Release II, *supra* note 102.
111. Marc Rotenberg et al., *supra* note 107.
112. EU Press Release I, *supra* note 101.
113. *See* Hunton & Williams LLP, *supra* note 73 (Senator Franken stating, "this legislation would give people the right to know what geolocation data is being collected about them and ensure they give their consent before it's shared with others" (internal quotation marks omitted)).
114. EU Press Release II, *supra* note 102.

provisions increase transparency and improve competition among services, respectively.[115]

4. Notification of Serious Data Breaches

The directive mandates that companies responsible for serious privacy breaches have to notify the victims without undue delay, within 24 hours when feasible.[116] Such a provision, absent from American regulation, clearly prioritizes consumer protection by increasing responsibility and accountability of companies and organizations processing sensitive data.

5. Distinction Between Information Needed to Enable a Transmission and Information Used for Value-Added Services

The European model differentiates between location information needed to enable transmission and location information used for value-added services.[117] In so doing, it restricts the processing of data to what is necessary for providing a service to the consumer, protecting users from unnecessary, and dangerous invasions of privacy. Under the current U.S. regime, no such distinction exists.

6. Coordinating Body

The European model is also worth emulating in its creation of a coordinating body to handle differences of interpretation and implementation. The EU directive created the Article 29 Working Party, which is a group of advisors from across the European Union that offers advice on the various LBS-related issues and explains enforcement mechanisms to member states and citizens.[118] The group is advisory and thus, non-binding.[119]

By putting these six elements together in a digital privacy protection plan, the United States can follow Europe's strong lead and protect LBS users from unwanted tracking and the ensuing risks without hindering the innovation of new technologies that enhance user experience and convenience.

V. CONCLUSION

The proliferation of location-based services and the increasing role of third-party application developers in the evolution of such technology indicate that privacy issues in the mobile industry are of growing importance. Based on the rash of privacy breaches in recent years, it is clear that the governance of LBS has failed to keep up with the technology. Politicians and privacy watchdogs alike must be commended for their recent calls to action, having

115. *Id.*
116. *Id.*
117. *See* Mumford, *supra* note 103 (describing how service providers must inform users of the type of location data being used and for what purpose).
118. *Id.*
119. *Id.*

brought LBS to the public's attention. But each proposed law or regulation falls short in some key respect. Using the European approach as a model, the United States should take immediate steps toward a more comprehensive approach that starts with federal legislation and encourages simplicity and transparency for consumers. Only once such a system is adopted will Americans be adequately protected from the mobile devices they so often trust blindly.