A Check-in on Privacy After *United States v. Jones*: Current Fourth Amendment Jurisprudence in the Context of Location-Based Applications and Services

by KATHRYN NOBUKO HORWATH*

> My alarm clock goes off. Presumably on my iPhone 4, because it's very important to me that I own the latest technology. I hit snooze. I can't *believe* I have to get up by 9 a.m. to make it to my place of work before 10 a.m. where I am paid to be creative and knowledgeable about "the internet," just in general.
> I check Twitter.
> I check Facebook.
> I casually thumb through emails I've received since going to bed. . . .
> I take a shower. . . .
> I check Twitter.
> I check Facebook.
> I check-in to my apartment on Foursquare,[1] which I've named something cute and clever because for some reason I think people actually care what I call my apartment on a mobile application named after a

* Juris Doctor Candidate, 2013, University of California, Hastings College of the Law; Senior Articles Editor, Volume 40 of the *Hastings Constitutional Law Quarterly*; Bachelor of Arts in Sociology and Anthropology, 2009, University of California, Berkeley. The author would like to thank Professor Hadar Aviram for her guidance, the editors of the *Hastings Constitutional Law Quarterly*, especially Jonathan August for his patience and sagacity, and her family and friends for their support.

1. Foursquare is a location-based social networking service that enables users to "check in" to places they visit and share their location with their friends. As of 2012, Foursquare has over twenty-five million users and three billion check-ins, with millions of check-ins daily. Launched in 2009 by co-founders Dennis Crowley and Naveen Selvadurai, the company is based in San Francisco, California. (*About foursquare*, FOURSQUARE.COM, http://foursquare.com/about/ (last visited Apr. 7, 2013).

> children's playground game. They don't. I just wanted the mayorship, let's be honest. . . .
> I walk to the BART station, which is about 3 blocks from my house.
> I check Twitter.
> I check Facebook.
> I check-in to BART on Foursquare, because everyone needs to know that I'm about to take public transportation. . . . To be fair: I've heard if you check into BART 10 times you get the "Trainspotter" badge. I don't know why this is important to me. But it is. I need that badge. . . .
> I get to work. . . .
> I check Twitter.
> I check Facebook.
> I get lunch at some place that is overpriced. I check in to their establishment on Foursquare.
> When I return to work, I will sign up for a social networking site that is new. It will involve:
> 1) Taking artsy pictures and sharing them with people.
> 2) Telling people about the music I'm listening to.
> 3) Telling people what I'm doing, right now, this instant, right now, this instant, no seriously, right now.
> 4) Telling people what I've eaten.
> 5) Doing all four of these things at once while then distrubuting [*sic*] this to Twitter, Facebook and Foursquare.[2]

Introduction

You sacrifice some privacy when you leave your home. Someone might see you enter the abortion clinic or AIDS testing center, a strip club or gay bar, a picket line or Occupy protest, or notice you and your secretary leaving a hotel together. Obtaining this information used to be expensive.[3] Your enemies had to pay someone to follow you around and it was difficult to keep surveillance a secret because you could notice

2. Drew Hoolhorst, *A Day in the Life of a Modern San Franciscan*, ROCKET SHOES (July 12, 2011) http://www.rocket-shoes.com/a-day-in-the-life-of-the-modern-san-franciscan/.

3. Andrew J. Blumberg & Peter Eckersly, *On Locational Privacy, and How to Avoid Losing It Forever*, ELECTRONIC FRONTIER FOUNDATION, 2 (Aug., 2009) https://www.eff.org/files/eff-locational-privacy.pdf.

your tail skulking in your shadow.[4] Today, obtaining this information is cheap. Information about your location "is quietly collected by ubiquitous devices and applications, and available for analysis to many parties who can query, buy or subpeona [*sic*] it."[5] The technological transformation from visual surveillance to remote tracking has eroded our locational privacy, i.e., "the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use."[6]

Apple, AT&T, and the government are not solely to blame—we check in on Foursquare and Facebook Places[7], broadcast our location in real-time using Google Latitude[8], and let OkCupid[9] use our location to find us people to date nearby. Use of location-based applications and services ("LBS") like these is not only commonplace, it is becoming increasingly necessary to fully participate in society today. However, when we use privacy controls to limit who can access this information, we do not expect that the government will obtain it. Existing privacy law does not provide enough protection for our digital location information. If digital privacy law does not evolve to comport with modern technologies and society's use of them, then Big Brother will be a reality.

In *United States v. Katz*, the Supreme Court held that the FBI's use of an electronic eavesdropping device to record Katz's private conversation in a public telephone booth constituted a search within the meaning of the Fourth Amendment.[10] Recognizing "the vital role that the public telephone has come to play in private communication,"[11] the Court held both that physical intrusion is not necessary to constitute a

4. *Id.* at 2.

5. *Id.*

6. *Id.* at 1.

7. Announced in August 2012, Places enables Facebook users to share their location and the friends they are with in real time from their mobile device. (Michael Eyal Sharon, *Who, What, When, and Now. . .Where*, THE FACEBOOK BLOG (Aug. 18, 2010) https://blog.facebook.com/blog.php?post=418175202130.

8. Google Latitude enables users to share their location and see where their friends are on a map in real time. Latitude's "location history" feature optionally records and analyzes a user's location and time spent at each place over time.

9. OkCupid is a free online dating website with over eight million users. In 2011, OkCupid launched the "Locals" feature, enabling users to locate and chat with matches within close proximity. (Kat Hannaford, *OkCupid Adds Grindr-Like Location Feature for Quick Shags or Romantic Dates*, GIZMODO (Aug. 12, 2011), http://gizmodo.com/5830259/okcupid-adds-grindr+like-location-feature-for-quick-shags-or-romantic-dates).

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

11. *Id.* at 353.

search and "being 'in public' is not a binary state—that is, one can be exposed to the public in some respects but not in others."[12] Just like the telephone in the 1960s, electronic communications, such as email, text messages and LBS user location information, play a vital role in private communication today.

This note will discuss whether current Fourth Amendment jurisprudence adequately protects user location information obtained from LBS, and if not, what changes can be made to ensure our right to privacy in this digital information. In Part I, the concept of LBS and a technical description of how it works will be discussed. Part II will summarize the Supreme Court's recent decision in *United States v. Jones* on warrantless prolonged use of a GPS tracking device and will outline the Fourth Amendment jurisprudence underpinning the Court's logic. Part III will deliver an in-depth description of federal statutory law that applies to the seizure of electronic information. Part IV will debate whether and to what extent LBS user location data is protected under applicable federal statutes and will analogize to current case law on similar electronic communications. Part V will survey recently proposed reforms to the Electronic Communications Privacy Act of 1986 ("ECPA").[13]

This note concludes that LBS user location information—and electronic communications generally—must receive Fourth Amendment protection, despite the fact that they are transmitted through intermediaries and their content is possibly shared with more than one person. The law changes incrementally, while technology does not. Technological change is disruptive. Current Fourth Amendment jurisprudence is outdated and will soon be overwhelmed, structurally unable to bear the wave of new LBS on the horizon. As information technology continues to reshape American life, we need clear and strong rules to protect the privacy of our electronic communications. The goal of this note is to emphasize the importance of treating electronic communications, including LBS user location information, with the restraint dictated by the Fourth Amendment.

12. Jay Stanley, *The Crisis in Fourth Amendment Jurisprudence*, AMERICAN CONSTITUTION SOCIETY, 14 (May 2010), http://www.acslaw.org/files/ACS%20Issue%20Brief%20-%20Stanley%204th%20Amendment.pdf.

13. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, *100 Stat. 1848* (codified as amended in scattered sections of 18 U.S.C.).

I. LBS Technology

A. What is LBS?

In the United States, 101.3 million mobile subscribers use smartphones as of January 2012.[14] A recent report by venture capital firm, Kleiner Perkins Caufield & Byers shows that there are 172 million smartphone subscribers in the United States as of the fourth quarter of 2012.[15] 50.4% of mobile subscribers in the United States own a smartphone,[16] and 46% of American adults have a smartphone.[17] 67% of adults ages eighteen to twenty-four have a smartphone, and 71% of adults ages twenty-five to thirty-four have a smartphone.[18] 28% of American adults use mobile or social location-based services of some kind.[19] 55% of smartphone owners use their device to get location-based directions and recommendations, and nearly one in five access check-in services via their device, with 36% of eighteen to twenty-four year olds and 32.5% of twenty-five to thirty-four year olds using geosocial services such as Foursquare and Facebook Places.[20]

Location-based mobile applications and services are "any application or service that receives a consumer's location and provides that consumer with information or services tailored to that location."[21] LBS offer a wide array of services: navigation tools to help users reach

14. *comScore Reports January 2012 U.S. Mobile Subscriber Market Share, More Than 100 Million U.S. Mobile Subscribers Now Use Smartphones*, COMSCORE (Mar. 6, 2012), http://www.comscore.com/Press_Events/Press_Releases/2012/3/comScore_Reports_January_2012_U.S._Mobile_Subscriber_Market_Share.

15. Mary Meeker, *2012 KPCB Internet Trends Year-End Update*, (Dec. 3, 2012) http://www.slideshare.net/kleinerperkins/2012-kpcb-internet-trends-yearend-update.

16. *America's New Mobile Majority: a Look at Smartphone Owners in the U.S.*, NIELSON (May 7, 2012) http://blog.nielsen.com/nielsenwire/online_mobile/who-owns-smartphones-in-the-us/.

17. Aaron Smith, *Nearly half of American adults are smartphone owners*, PEW INTERNET, 2 (Mar. 1, 2012), http://pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf.

18. *Id.* at 4.

19. Kathryn Zickuhr & Aaron Smith, *28% of American adult use mobile and social location-based services*, PEW INTERNET, 2 (Sept. 6, 2011), http://pewinternet.org/~/media//Files/Reports/2011/PIP_Location-based-services.pdf

20. *Nearly 1 in 5 Smartphone Owners Access Check-in Services Via their Mobile Device*, COMSCORE (May 12, 2011), http://www.comscore.com/Press_Events/Press_Releases/2011/5/Nearly_1_in_5_Smartphone_Owners_Access_Check-In_Services_Via_their_Mobile_Device.

21. Nicole A. Ozer, Chris Conley, Hari O'Connell, Ellen Ginsburg & Tamar Gubins, *Location-Based Services: Time for a Privacy Check-in*, ACLU OF NORTHERN CALIFORNIA, 2 (Nov., 2010), http://dotrights.org/sites/default/files/lbs-white-paper.pdf.

their destination[22] (e.g.. Google Maps); local search applications to help users find and review nearby businesses (e.g., Yelp); location sharing applications that allow users to check in to their location and share it with their friends (e.g., Foursquare, Facebook Places); social networking[23] applications that allow users to geotag content such as photos and posts and share it with their friends (e.g., Facebook, Twitter); ambient social networking applications that run in the background on a smartphone and enhance serendipity by alerting users in real-time to nearby friends or individuals with whom they have affinity (e.g., Google Latitude, Highlight, Sonar); and dating applications that allow users to find romantic and sexual partners nearby (e.g., OkCupid, Grindr). Currently, many users access LBS through mobile phones, but other location-aware devices, such as tablets and laptops can also be used to access many LBS.[24]

By using LBS, users "allow companies to compile detailed profiles of their lives: the places they visit, the events they attend, the people they meet, and more."[25] Many LBS collect and store this sensitive information in accordance with terms of service and privacy policies, creating detailed profiles for use in targeted advertising and other purposes.[26] Selling this user data, usually in aggregated form, to external partners enables LBS to provide a free service to users. Partnering with LBS presents an opportunity for mobile advertisers and publishers to increase their conversion rates; using detailed information about consumers to serve targeted advertisements and deliver relevant content to users based on their location at any moment.[27] As smartphones and LBS proliferate, more and more companies will possess detailed and sensitive information about users.[28] Commercial possession of user information presents serious privacy implications for users.

Currently, it is unclear what legal protections are afforded LBS user-location information, and some even argue that Fourth

22. *Id.* at 1.

23. Sara E. Brown, Note, *An Illusory Expectation of Privacy: The ECPA is Insufficient to Provide Meaningful Protection for Advanced Communication Tools*, 114 W. VA. L. REV. 277, 289 ("social networking is a controlled communication knowingly shared in a specific manner to a specific person or a specific group of people. . . . [It is] a communication *knowingly shared the way the user intends*." (emphasis added)).

24. Ozer et al., *supra* note 21, at 1.

25. *Id.*

26. *Id.* at 2, 3.

27. Conversion rate is the proportion of visitors to a website who take a desired action as a result of subtle or explicit requests from advertisers.

28. *Id.* at 3.

Amendment jurisprudence and statutory law may extinguish Fourth Amendment protection in such information.[29] The Supreme Court has held that an individual has no reasonable expectation of privacy in their bank records and the phone numbers they dial, even if they intend the third party to whom this information is provided to keep that information secret, because they assume the risk that the third party will share that information with the government. But LBS users do not necessarily expect that the information they communicate to intended recipients via non-sentient electromechanical devices and software applications will be accessible by service providers' individual employees who could disclose that information to the government. Furthermore, users do not expect that by providing their information to LBS, the government can stand in the shoes of commercial entities, vitiating Fourth Amendment protection of LBS user location information.

Although enacted to extend restrictions on the government's ability to access electronic communications, the Electronic Communications Privacy Act of 1986[30] allows the government to compel disclosure of some user data merely under a subpoena or pursuant to a court order with prior notice.[31] Whether user location information held by LBS falls into this category is unknown, and no case law exists on the subject. LBS users should not have to choose between adopting new technologies that advance the progress of society and forsaking the legal protections afforded them under the Fourth Amendment.

B. How LBS Determine Your Location

The technology behind LBS, and the user data collected by LBS, has implications for the level of Fourth Amendment protection afforded users' location information. LBS determine location in four ways: GPS, cell-site information ("CSI"), Wi-Fi geolocation, and user actions specifying their current location.[32] Currently, the most accurate way to determine a user's location is GPS. A GPS device locates its position by determining the transit time of messages it receives from at least three satellites in orbit high above the Earth; then, through a process called trilateration, these values are used to draw spheres around the device

29. Christian Levis, Note, *Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 191, 207 (2011) ("Regardless of where something falls within the ECPA, individuals lose any reasonable expectation of privacy they may have in information that is knowingly disclosed to the public.").

30. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, *100 Stat. 1848* (codified as amended in scattered sections of 18 U.S.C.).

31. Stored Communication Act of 1986, 18 U.S.C. § 2703(b)(B)(i-ii).

32. Levis, *supra* note 29, at 197–98.

with their intersection indicating the device's exact position on the ground.[33] In a cell phone, the receiver is a chip within the phone.[34]

A cell phone transmits and receives signals throughout a cellular network, which is divided into cells.[35] A cell site, also referred to as a cell tower, is the point where three cells meet.[36] When a cell phone is turned on, it scans the strength of every potential cell site by periodically transmitting a signal to the network.[37] When a call is placed, the phone connects to the cell site with the strongest signal.[38] To avoid dropping a call when the signal strength of site servicing the call decreases, the call transfers to an adjacent cell site with a stronger signal.[39] Cell site data is captured as a cell phone scans the network for the cell site with the strongest signal.[40] Cell site data can be interpreted in real-time or historically from company records to determine the location of a cell phone at any given time.[41]

The Wi-Fi geolocation method "uses various location-based clues," such as "the media access control ('MAC') address of other available Wi-Fi networks, cell towers, Bluetooth . . . radio-frequency identifier ('RFID'), Cell-ID and GPS signal" to determine the location of a phone currently accessing the Internet.[42] A user can voluntarily specify their location by "checking in," "tagging" content, or broadcasting their location by running a LBS networking app in the background.

C. What LBS Know About You

LBS access a user's location data stored on their device and information obtained through integration with social networks to spotlight people and places around them.[43] The level of access granted is determined by a set of controls called permissions. In order to gain permission, most privacy policies inform users about: (1) the type of

33. *Id.*

34. Derek P. Richmond, Comment, *Can You Find Me Now?—Tracking the Limits on Government Access to Cellular GPS Location Data*, 16 COMMLAW CONSPECTUS 283, 285 (2007).

35. Aaron Blank, Article, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 RICH. J.L. & TECH. 3, ¶ 5 (2011).

36. *Id.*

37. *Id.* at ¶ 6.

38. *Id.*

39. *Id.* at ¶ 6.

40. *Id.* at ¶ 10.

41. *Id.*

42. Levis, *supra* note 29, at 200.

43. *Id.* at 201.

information collected; and (2) the purpose for collecting that information.[44] By allowing a requested permission, a user consents to the collection of their information by the LBS.[45] LBS companies subsequently collect and mine user data for a variety of "legitimate business purposes," including serving targeted ads, improving relevancy, and improving the service.[46]

In his concurrence in *United States v. Jones*, Justice Samuel Alito suggests that while new technologies "may provide increased convenience or security at the expense of privacy, [] many people may find the tradeoff worthwhile."[47] LBS users consent to the collection and mining of their user data in exchange for free use of the app or service. Perhaps what we should be concerned about is the aggregate of user data—not just what an app knows about *me*, but what it knows about *us*—because this powerful knowledge about human behavior and decision making can be leveraged to design persuasive technologies.[48]

How LBS work technically and what they know about users has implications for the Fourth Amendment protection afforded to LBS user location information. Since LBS user location information is a form of electronic communication, it is governed by the ECPA. The technical attributes of electronic communications determine how LBS user data is classified under the ECPA; this classification in turn determines the standard that the government must meet to compel disclosure of electronic communications from service providers. Privacy protection afforded by the ECPA is intended to reflect the reasonable expectation of privacy a user holds in his electronic communications. In this way, the ECPA is built on a foundation of Fourth Amendment law.

Before we can understand how the ECPA will play a role in governing LBS information, it is crucial to first look at the evolution of

44. *Id*. at 202–203. For an example of how privacy policies inform users, check out Foursquare's privacy policy, *available at* https://Foursquare.com/legal/privacy (last updated Jan. 28, 2013).

45. *Id*. at 207.

46. Smith v. Maryland, 442 U.S. 735, 743 (1979).

47. United States v. Jones, 132 S.Ct. 945, 962 (Alito, J., concurring).

48. Alexander Furnas, *It's Not All About You: What Privacy Advocates Don't Get About Data Tracking on the Web*, THE ATLANTIC (Mar. 15, 2012), http://www.theatlantic.com/technology/archive/2012/03/its-not-all-about-you-what-privacy-advocates-dont-get-about-data-tracking-on-the-web/254533/ ("Detailed knowledge of individuals and their behavior coupled with the aggregate data on human behavior now available at unprecedented scale grants incredible power. Knowing about all of us—how we behave, how our behavior has changed over time, under what conditions our behavior is subject to change, and what factors are likely to impact our decision-making under various conditions—provides a roadmap for designing persuasive technologies.").

Fourth Amendment jurisprudence and its most recent controversial case.

II. *United States v. Jones* and Fourth Amendment Law

In January 2012, the Supreme Court held in *United States v. Jones* that the government's warrantless installation of a GPS device on a target's vehicle and its use of that device to track the vehicle's movements constituted a search because it was a physical trespass on a constitutionally protected area.[49] But what of the situation in which the government conducts prolonged surveillance without physical trespass; for instance, remotely tracking a target through his GPS-enabled smartphone or obtaining a Foursquare user's check-in history? By basing their holding in property-based theory, the majority sidestepped the larger issue of whether the government's use of a GPS device to monitor the movements of the target's vehicle for twenty-eight days violated his reasonable expectation of privacy.[50]

Lower federal and state courts have decided whether data obtained from a GPS tracking device,[51] cell-site location information,[52] email[53] and Facebook posts[54] receive Fourth Amendment protection. Whether users have a reasonable expectation of privacy in their LBS location information—and whether and to what extent it receives Fourth Amendment protection—is unclear. Like the government's use of a GPS device to monitor Jones' location over a prolonged period of time, LBS can create a record of a user's location information over time, revealing intimate details about that user's life. However, unlike in *Jones*, the government need not accomplish a physical trespass to obtain LBS location data. Therefore, the Court's decision in *Jones* does not

49. 132 S.Ct. 945, 949-50 (2012) (majority opinion).

50. *Id.* at 954 (majority opinion) ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."); *see also id.* ("We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to Katz analysis; but there is no reason for rushing forward to resolve them here.").

51. United States v. Garcia, 474 F.3d 994 (7th Cir. 2007); United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010) *cert. denied*. 131 S. Ct. 671 (U.S. 2010) and *cert. granted*, 131 S. Ct. 3064 (U.S. 2011) and *aff'd in part sub nom. Jones*, at 945.

52. In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No. 10-MC-0897 (JO), 2010 WL 5437209 (E.D.N.Y. 2010).

53. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

54. Crispin v. Christian Audigier, 717 F. Supp. 2d 965 (9th Cir. 2010).

proscribe the government's ability to obtain LBS data in violation of a user's reasonable expectation of privacy.

A. Foundational Fourth Amendment Case Law

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[55]

The Framers drafted the Fourth Amendment to protect against the use of general warrants and writs of assistance, which they considered tyrannical remnants of English law that threatened "personal security, personal liberty, and private property."[56] Today, Fourth Amendment jurisprudence is in need of reform. The two principal problems are third-party doctrine and the reasonable expectation of privacy test, which when applied to LBS user location information—among other electronic communications—extinguish its Fourth Amendment protection.[57] The Fourth Amendment case law that forms the foundation for *Jones* and why the Court's affirmation of the D.C. Circuit on narrow trespass grounds rather than the reasonable expectation of privacy test is crucial for future LBS cases. Additionally, although it went beyond the immediate issue—a situation involving a physical trespass—the Court's statement about a situation in which no physical trespass by the government occurs has a bearing on whether LBS user location information receives Fourth Amendment protection.

Citing *United States v. Knotts*, the government argued in the D.C. Circuit Court companion to *Jones*, *United States v. Maynard*, that the defendant did not have a reasonable expectation of privacy in his movements in an automobile on public streets.[58] In its opinion, however,

55. U.S. CONST. amend. IV.

56. Weeks v. United States, 232 U.S. 383, 390-91 (1914) (internal citations omitted) *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961).

57. Stanley, *The Crisis in Fourth Amendment Jurisprudence*, *supra* note 12, at 1.

58. United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010). *See* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

the D.C. Circuit distinguished the government's prolonged surveillance of Jones from the surveillance of an automobile traveling on public streets in *Knotts*.[59] In *Knotts*, the government attached a beeper to a container of chloroform prior to purchase by one of Knotts's co-conspirators.[60] Police officers followed the vehicle in which the container had been placed, maintaining visual contact with the vehicle and monitoring the radio signals emitted from the beeper to track the vehicle's movement on public streets.[61] Relying on information acquired during the short-term surveillance, officers obtained a search warrant for a cabin occupied by Knotts and discovered a drug laboratory, leading to his conviction.[62]

Justice Rehnquist, writing for the Court, recited the evolution of Fourth Amendment jurisprudence from *Olmstead v. United States*[63] through *Katz v. United States*.[64] In *Olmstead*, the Court held that a Fourth Amendment violation required a physical trespass by the government into a constitutionally protected area.[65] In *Katz*, the Court evolved the doctrine and held that:

> [T}he Fourth Amendment protects people not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[66]

Justice Harlan's concurrence in *Katz* created the famous two-prong test to determine whether a government action is a search under the Fourth Amendment: "first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[67]

Applying *Katz* in *Knotts*, the Court determined that the government's use of the beeper to monitor Knott's co-conspirator as he

59. *Maynard*, 615 F.3d at 556.
60. *Knotts*, 460 U.S. at 277.
61. *Id.*
62. *Id.* at 279.
63. Olmstead v. United States, 277 U.S. 438 (1928).
64. Katz v. United States, 389 U.S. 347 (1967).
65. *Knotts*, 460 U.S. at 280 (discussing *Olmstead*).
66. *Katz*, 389 U.S. at 351.
67. *Id.* at 361.

drove with the container on public streets was not a search or seizure under the Fourth Amendment because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[68] In support of its holding, the Court cited a lesser expectation of privacy in automobiles,[69] and public exposure of a person's movements while traveling in an automobile on public thoroughfares.[70] The Court noted that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[71]

Further developing Fourth Amendment jurisprudence, in *Kyllo v. United States*, the Supreme Court held that the government's use of a thermal imaging device not in general public use from a public vantage point to measure the heat emanating from a man's home constituted a search within the meaning of Fourth Amendment.[72] Justice Scalia specifically authored his opinion with an eye towards the "long view" of the Fourth Amendment and the ability of future technologies to invade one's right to privacy.[73] The government's use of the thermal imager was presumptively unreasonable without a warrant because it revealed "details of the home that previously would have been unknowable without physical intrusion."[74] The Court rejected the distinction between "off the wall" and "through the wall" surveillance, drawing a "firm but also bright" line at the "entrance to the house."[75] Simply put, the Fourth Amendment is implicated when the government intrudes upon the privacy of the home, a constitutionally protected area.[76] The Court's decisions in *Katz*, *Knotts*, and *Kyllo* all focus squarely on the target's reasonable expectation of privacy.

68. *Knotts*, 460 U.S. at 280, 285.

69. *See* Carroll v. United States, 267 U.S. 132, 151 (1925) (ready mobility of automobiles creates an inherent exigency: destruction of evidence); Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (automobiles are used for transportation on public roadways exposing occupants and contents to public view); California v. Carney, 471 U.S. 386, 392–93 (1985) (automobiles are readily mobile and subject to regulation and inspection.).

70. *Knotts*, 460 U.S. at 281–282 (When a person "travel[s] over the public streets he voluntarily convey[s] to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.").

71. *Id.* at 282.

72. Kyllo v. United States, 533 U.S. 27, 30–31 (2001).

73. *Id.* at 40.

74. *Id.*

75. *Id.* at 36.

76. *Id.* at 34.

The problem with the reasonable expectation of privacy test is that it involves a degree of circularity.[77] "[P]eople get only the privacy that they expect to get. Under this standard, even the most reprehensible invasions of privacy might lose constitutional protection if a realistic person is forced to conclude that their privacy will in fact be invaded . . ."[78] Jay Stanley suggests that replacing "expectation" with "desire for" or "intention to preserve" would eliminate the circularity.[79]

According to a survey by Morgan Stanley, 91% of people keep their phone within three feet of themselves twenty-four hours a day.[80] Unlike GPS devices affixed on vehicles that monitor the target's movements only when he is in the vehicle, phones kept within a three-foot radius at all times expose a target's movements *everywhere*, even within his home as he moves from the bedroom to the bathroom. This revelation of the "details of the home" is precisely what the Fourth Amendment is designed to protect. The government need not commit a physical trespass to monitor a target's location simply by remotely accessing location data from his phone. After the Court's holding in *United States v. Jones*, whether this kind of surveillance without a warrant would constitute an unconstitutional search is unclear.

Although not the controlling opinion on the government's prolonged surveillance of Jones, the D.C. Circuit's rationale in *Maynard* for ruling that Jones had a reasonable expectation of privacy in his movement maps well onto the case of LBS user location information. In *Knotts*, the Court held that the defendant did not have a reasonable expectation of privacy in his movements on public roadways because he exposed his movements to the public.[81] In *Maynard*, the D.C. Circuit refused to apply the public exposure doctrine articulated in *Knotts* to prolonged surveillance:

> First, unlike one's movement during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively

77. Stanley, *The Crisis in Fourth Amendment Jurisprudence*, *supra* note 12, at 5.

78. *Id.*

79. *Id.*

80. Mary Meeker, David Joseph, and Richard Ji, *Technology/Internet Trends*, MORGAN STANLEY RESEARCH (Oct. 18, 2007), http://www.slideshare.net/misteroo/web2-139178.

81. United States v. Knotts, 460 U.S. 276, 281–282 (1983). (*See also* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.")).

> nil. Second, the whole of one's movements is not exposed constructively even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[82]

To determine whether something is exposed to the public "we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do."[83] In the case of driving one's car, "[a] reasonable person does not expect anyone to monitor and retain a record of every time he drives his car . . . rather he expects each of those movements to remain disconnected and anonymous."[84] Although using LBS such as Foursquare and Facebook Places can deliberately connect a user's movements from place to place and affirmatively make known their identity to a circumscribed audience, users do not necessarily expect that their LBS location information will be accessible by persons outside of that chosen audience, including the government. LBS users can try to claim a reasonable expectation of privacy in their location information when they utilize privacy settings to limit the audience with whom they share it.[85]

To arrive at its holding that Jones had a reasonable expectation of privacy in the aggregate of his movements as surveilled by the government twenty-four hours a day for twenty-eight days, the D.C. Circuit applied mosaic theory to Fourth Amendment law.[86] Mosaic theory posits that the whole may reveal more than the sum of its parts.[87] The rationale behind mosaic theory is that "subjects [have] a privacy interest in the aggregated 'whole' distinct from their interest in the 'bits of information' of which it [is] composed."[88] Applying mosaic theory in *Maynard*, the D.C. Circuit determined that "[p]rolonged surveillance

82. United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).

83. *Id.* at 559.

84. *Id.* at 563 (internal quotation marks omitted).

85. *See* United States v. Pineda-Moreno, 591 F.3d 1212, 1215 (2010) (holding that a warrantless attachment of a mobile tracking device to the underside of Pineda-Moreno' vehicle while it was parked in his driveway was not a search and that he had no reasonable expectation of privacy in it because he did not take steps to exclude passersby).

86. *Maynard*, 615 F.3d at 565 ("prolonged GPS monitoring reveals an intimate picture of the subject life that he expects no one to have.").

87. *Id*. at 558.

88. *Id*. at 561 (quoting United States Department of Justice v. Reporters Committee for Freedom of the Press, 498 U.S. 749, 764 (1989)).

reveals types of information not revealed by short-term surveillance" or by "any individual trip viewed in isolation."[89] Similar concerns arise when looking at LBS information over a long period of time.

B. The Facts of *United States v. Jones*

In 2004, Antoine Jones came under suspicion of trafficking cocaine and became a target of an investigation by the FBI and the Metropolitan Police Department.[90] In 2005, the government obtained a warrant authorizing the installation and use of a GPS tracking device on Jones' vehicle for ten days in the District of Columbia.[91] On the eleventh day—after the warrant expired—the government installed a GPS tracking device to the undercarriage of Jones' vehicle while it was parked in a public parking lot located in Maryland.[92] The government used the GPS device to track the vehicle's movements for twenty-eight days.[93] The location data obtained by the government's use of the GPS device provided key evidence supporting Jones' conviction for drug trafficking.[94]

On appeal, Jones argued that the government's installation of a GPS device on his vehicle without a valid warrant and its use of the device to track his movements twenty-four hours a day for twenty-eight days constituted a search in violation of his Fourth Amendment right to privacy.[95] As previously described, the D.C. Circuit held that the government's warrantless use of the GPS device to monitor the movements of Jones' vehicle for twenty-four hours a day for twenty-eight days "was a search because it defeated Jones' reasonable expectation of privacy."[96] This note argues, *infra*, that the standard articulated by the D.C. Circuit for evaluating whether or not a person's expectation of privacy is reasonable is a fair and workable standard for determining Fourth Amendment protection of LBS user location information.

89. *Id.* at 562.
90. United States v. Jones, 132 S.Ct. 945, 948 (2012).
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.* at 948–49; United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010).
95. *Maynard*, 615 F.3d at 555.
96. *Id.* at 555–56.

C. The *Jones* Decision

In *Jones*, the Supreme Court unanimously affirmed *Maynard* in that the government's warrantless installation of a GPS tracking device to Jones' vehicle and its use of that device to monitor the vehicle's movements on public streets constituted a search under the Fourth Amendment.[97] The wide variety of rationales used by the court in Justice Scalia's majority opinion, Justice Sotomayor's concurrence, and Justice Alito's concurrence will certainly have wide ranging effects on future LBS cases.

1. Scalia Majority

Justice Scalia took a property-based approach in *Jones*, ruling that the attachment of the GPS device to Jones' vehicle for the purpose of monitoring the vehicle's movements on public streets constituted a search within the meaning of the Fourth Amendment.[98] Putting to use his brand of originalism, Justice Scalia posited, "[t]he text of the Fourth Amendment reflects its close connection to property,"[99] and that the Court must preserve the "degree of privacy against the Government that existed when the Fourth Amendment was adopted."[100] Justice Scalia declared that the reasonable expectation of privacy test articulated in *Katz* supplemented, but did not displace, the common-law trespassory test.[101] The government's attachment of a GPS device to Jones' vehicle was simply a physical invasion into a constitutionally protected space for the purpose of obtaining information, thus violating the Fourth Amendment.[102]

Furthermore, Justice Scalia determined it was unnecessary to conduct an analysis of Jones' reasonable expectation of privacy in his movements because the government's trespass on Jones' vehicle was sufficient to find a Fourth Amendment violation.[103] However, he stated

97. United States v. Jones, 132 S.Ct. 945, 951 (2012).

98. *Id*. at 949 ("The Government physically occupied private property for the purpose of obtaining information. . . . such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

99. *Id*.

100. *Id.* at 950 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

101. *Id.* ("The Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding."); *see also id.* at 952 ("the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.).

102. *Id.* at 949.

103. *Id.* at 950.

that searches conducted without physical trespass "involving merely the transmission of electronic signals . . . would *remain* subject to *Katz* analysis."[104] Justice Scalia did not address the length of time for which warrantless tracking accomplished without physical trespass would be constitutionally permissible.[105]

2. Sotomayor Concurrence

Justice Sotomayor agreed with the majority that *Katz*'s reasonable expectation of privacy test did not repudiate the common-law tresspassory test: "When the Government physically invades personal property to gather information, a search occurs."[106] Like Justice Scalia, Justice Sotomayor concluded that, "in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'"[107] Justice Sotomayor's view that the reasonable expectation of privacy test still applies in the absence of a trespass supports the argument that LBS location data should receive constitutional protection—a user demonstrates his subjective expectation of privacy in his location information by utilizing privacy settings, and society recognizes that it is reasonable to expect that information shared with a finite audience will remain private.

Unlike Justice Scalia, however, Justice Sotomayor problematized the application of the reasonable expectation of privacy test to technological advancements that allow the government to conduct prolonged surveillance without committing physical trespass, such as GPS-enabled smartphones.[108] Justice Sotomayor suggested that attributes of GPS surveillance—such as its ability to "generate[] a precise, comprehensive record of a person's [] movements that reflect a wealth of detail about her familial, political, professional, religious, and sexual associations," and the government's ability to "store such records and efficiently mine them for information years into the future"; as well as its potential for abuse by law enforcement[109]—be taken into account when assessing society's reasonable expectation of privacy in the sum of

104. *Id.* at 953.

105. *Id.* at 954.

106. *Id.* at 955 (Sotomayor, J., concurring).

107. *Id.* at 954–955 (quoting Kyllo, 533 U.S. at 33).

108. *Id.* at 956.

109. *Id.* ("GPS is monitoring is cheap in comparison to conventional surveillance techniques and by design, proceeds surreptitiously.").

a person's public movements.[110] Like the D.C. Circuit in *Maynard*, Justice Sotomayor would ask "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on."[111] Similarly, LBS users do not expect that the location information they share to a restricted audience will be accessible by the government for use in criminal proceedings against them.

3. Alito Concurrence

Justice Alito concurred in the judgment that the government's attachment and use of the GPS device to monitor Jones' movements constituted a search, but reached that result by determining that the government's long-term monitoring of the movements of Jones' vehicle violated his reasonable expectation of privacy.[112] Justice Alito argued that 18th-century tort law of trespass to chattels should not apply to a 21st-century surveillance technique like GPS.[113] Unlike the majority, Justice Alito argued that *Katz* did not merely supplement, but indeed repudiated the trespassory doctrine.[114] He was unsettled by the fact that accomplishing prolonged surveillance without committing a technical trespass is afforded no protection under the Court's theory.[115]

Although Justice Alito argued that the case should have been decided according to *Katz*'s reasonable expectation of privacy test, he admitted the test "involves a degree of circularity" and "judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[116] Additionally, Justice Alito acknowledged that, "technology can change those expectations."[117] For these reasons, Justice Alito suggested that Congress is best suited to regulate law enforcement's use of GPS

110. *Id.*

111. *Id. See also* United States v. Maynard 615 F.3d 544, 563 (D.C. Cir. 2010) ("We ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do."); *Id.* at 558 ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car.").

112. *Jones*, 132 S.Ct. 958 (Alito, J., concurring).

113. *Id.* at 957.

114. *Id.* at 960.

115. *Id.*

116. *Id.* at 962.

117. *Id.*

tracking technology by enacting legislation to protect against invasions of privacy occasioned by new technology.[118]

4. Implications of Jones

Although unanimous in its decision, the Court split divisively as to why a search occurred in *Jones*. Using a property-based approach, the majority held that a search occurred because the government physically invaded a constitutionally protected space.[119] Four justices, however, did not buy the property line of reasoning and failed to agree that the simple attachment of the GPS device to Jones' vehicle was a search.[120] Alarmingly, should one justice join these four in a future case, it is possible that the Court could "establish[] a majority holding that the installation of [a] GPS device does not require a warrant."[121] While the Court's opinions suggest that short-term monitoring without a warrant may be legal[122]—particularly when accomplished without physical trespass[123]—it appears that five justices are "willing to accept the principle that government surveillance over time can implicate an individual's reasonable expectation of privacy."[124] The line dividing permissible short-term monitoring from illegal extended monitoring is unclear, but tracking Jones for four weeks certainly falls on the side of an unconstitutionally lengthy surveillance.[125]

Unlike vehicles, which people enter and exit upon inception and termination of a trip, cell phones are carried on one's person and "can be monitored indoors where the expectation of privacy is the

118. *Id.* at 962, 964 (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. . . . A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety n a comprehensive way.").

119. *Id.* at 953 (majority opinion).

120. *Id.* at 958 (Alito, J., concurring) ("It is clear that the attachment of the GPS device was not itself a search.").

121. Jesse Koehler, *United States v. Jones Decided?*, BERKELEY TECH. L.J. (Mar. 5, 2012) http://btlj.org/2012/03/05/united-states-v-jones-decided/.

122. *Jones*, 132 S.Ct. at 964 (Alito, J., concurring) ("Relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. . . . But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

123. *Id.* at 954 (majority opinion).

124. United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012).

125. *Jones*, 132 S.Ct. at 964 (Alito, J., concurring) ("the line was surely crossed before the 4-week mark").

greatest."[126] Because people have their smartphone in their pocket or purse constantly, often charging their phone at their bedside, the government's monitoring of an individual by remotely tracking the location of his smartphone is potentially a great deal more invasive than monitoring the location of his vehicle by GPS.[127] In *United States v. Karo*, the Court held that the government's placement of a beeper on a container that was tracked to reveal its presence in the interior of a home was an impermissible search because the beeper enabled the government to apprehend details about the interior that would otherwise be unknowable without physical intrusion.[128] Crucial in *Karo*, however, was the fact that the beeper was used to track the whereabouts of a container, not an individual. Tracking the location of a smartphone may reveal intimate details about the inside of a home that could be obtained only by physically entering the home and visually surveilling it. As discussed *infra*, it is problematic to define privacy according to the four walls of a home.[129] The fact that smartphone tracking can reveal an individual's location everywhere he travels is an invasion of privacy, regardless of whether his location is inside a home.

III. Fourth Amendment Protection of LBS User Location Information

Now with a thorough understanding of Fourth Amendment jurisprudence, it is possible to look at current federal law and its interplay with LBS. This section will first define and explain one of the key concepts underpinning federal law before examining the statutes themselves.

126. In re Application of the United States of America for Historical Cell Site Data (hereinafter "*Historical Cell Site Data*"), 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010).

127. In *Graham*, the defendants argued that "allowing the government to retroactively track or surveil a suspect through his cellular telephone, a device he likely carries with him at all hours of the day and to constitutionally protected places such as his home or church" is an unconstitutional invasion of privacy. *See also Historical Cell Site Data*, 747 F. Supp. 2d at 834–35 (S.D. Tex. 2010) ("Cell phones are frequently used in the home or in other places not open to public view: one study shows that at least 52% of cell phone calls are made indoors; another study indicates that two out of three adults sleep with their cell phone nearby.").

128. 468 U.S. 705, 715 (1984).

129. Jim Harper, *Kerr Defends the Third-Party Doctrine*, The Technology Liberation Front (May 30, 2008), http://techliberation.com/2008/05/30/kerr-defends-the-third-party-doctrine/.

A. Third-Party Doctrine in the Context of LBS

The third-party doctrine is the principle that voluntary revelation of information to a third party relinquishes Fourth Amendment protection of that information because one assumes the risk that the third party will convey that information to the government, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[130] Under a strict interpretation of third-party doctrine, a user's disclosure of his location information to LBS vitiates his Fourth Amendment protection in that information.[131]

Scholars like Oren Kerr argue that third-party doctrine has utility in modern society because it prevents criminals from using third party technologies to avoid detection.[132] Additionally, Kerr points out that third-party doctrine is really nothing more than a "consent doctrine," and that it results in weak privacy protection for electronic information.[133] Specifically, he identifies three ways in which there is weak privacy protection: first, users cannot retain a reasonable expectation of privacy in information revealed to third parties; second, the government does not need to first obtain a warrant based on probable cause to subpoena the target's materials in the possession of a third party; and third, under private search doctrine, even if the Fourth Amendment protects information entrusted to a third party, as a private actor the third party may divulge that information to the government without committing a Fourth Amendment violation.[134]

130. United States v. Miller, 425 U.S. 435, 443 (1976) (holding no reasonable expectation of privacy in bank records because they are "negotiable instruments to be used in commercial transactions" and "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business"). *See also* Smith v. Maryland, 442 U.S. 735, 743 (1979) (holding that the government's installation of a pen register was not a search because telephone users lack a reasonable expectation of privacy in the numbers they dial and distinguishing the pen register used in *Smith* that did not acquire the content of communications from the listening and recording device used in *Katz*); *see also* United States v. White, 401 U.S. 745, 752 (1971) (holding that a government informant's use of a concealed radio transmitter during conversations with White did not violate the Fourth Amendment because a criminal assumes the risk that his accomplice is cooperating with law enforcement).

131. Orin S. Kerr, *The Case for Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) ("Information loses Fourth Amendment protection when it is knowingly revealed to a third party.").

132. *Id.* at 580.

133. *Id.*

134. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It* (hereinafter "*A User's Guide*") 72 Geo. WASH. L. REV. 1208, 1211–1212 (2004).

Justice Sotomayor's invitation to reconsider third-party doctrine was the most disruptive portion of the Court's opinion in *Jones*.[135] She concluded that "[t]he premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties."[136] Furthermore, Justice Sotomayor stated she "would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[137] Thus, strict third-party doctrine should not vitiate Fourth Amendment protection of that location information, as LBS users disclose their location for the limited purpose of enabling the functionality of the LBS or sharing their location information with a bounded audience. Justice Sotomayor's reasoning is particularly prescient as in the course of participating in modern society, we entrust a great deal of private information to third parties, particularly over the Internet.[138] Failing to adopt her wisdom and abiding by a strict third-party doctrine undermines the privacy protections contemplated by the Founders in drafting the Fourth Amendment.

At the time the Fourth Amendment was adopted in the late 1700s, the "'home' was a useful proxy for 'what should be protected'" because peoples' personal and professional lives centered there and it was the technology of the time.[139] Today, technology enables people and their things to be mobile. The "deep reservoirs of information . . . collected by third-party service providers today . . . are the modern iteration of our 'papers and effects.'"[140] In 2013, it simply no longer makes sense for the home to define the scope of Fourth Amendment rights.

Recall in *Katz*, the Court held, "the Fourth Amendment protects people, not places."[141] As technology increasingly pervades contemporary life, the Fourth Amendment should be construed to ensure a consistent level of privacy protection that is apropos in a free

135. United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

136. *Id.*

137. *Id.*

138. *Id.* For example, e-commerce, online banking, email, chat, and Google search.

139. Harper, *supra* note 129.

140. Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1402 (2008).

141. Katz v. United States, 389 U.S. 347, 351 (1967).

society.[142] This was precisely the Founders' intent in drafting the Fourth Amendment. In his dissent in *Olmstead v. United States*, Justice Brandeis famously wrote:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.[143]

To ensure that the Fourth Amendment continues to be effective in protecting peoples' privacy—and to ensure that America stays at the forefront of technological innovation and social change—the application of third-party doctrine must be circumscribed to reflect evolving technological realities.[144] Congress attempted to do just this when it enacted the Electronic Communications Privacy Act. However, as will be shown, because the ECPA stands on a foundation of shaky law, such as third-party doctrine, and has not been updated to account for new technologies like LBS, it fails to afford LBS user location information adequate privacy protection.

B. The Electronic Communications Privacy Act

When modern communication technologies gained wide adoption in the early 1980s, Congress became concerned that existing Fourth Amendment protections left electronic communications vulnerable to government interception and private disclosure.[145] Congress enacted the ECPA to extend "Fourth Amendment-like privacy protections"[146] to "then-nascent forms of telecommunications and computer technology like cellular phones, pagers, and electronic mail."[147] The statute imposes limitations on the ability of third-party service providers "to voluntarily

142. Harper, *Kerr Defends the Third-Party Doctrine*, *supra* note 129.

143. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, L. dissenting).

144. Timothy Lee, *Why the 'Third Party Doctrine' Undermines Online Privacy Protections*, TECHDIRT (June 20, 2008), http://www.techdirt.com/articles/20080530/2014171272.shtml.

145. Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 372 (2009).

146. Kerr, *A User's Guide*, *supra* note 134, at 1212.

147. In Re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), No. 10-GJ-3793, 2011 WL 5508991 (E.D. Va. Nov. 10, 2011).

disclose information about their . . . subscribers to the government" and "on the government's ability to compel providers to disclose information in their possession about their . . . subscribers."[148]

Currently, no statute specifically regulates access to user data.[149] User location data collected by LBS is presumably governed by the ECPA.[150] The ECPA consists of three titles: Title I, which amended Title III of the Federal Wiretap Act,[151] protects the interception of wire, oral, or electronic communications while in transit;[152] Title II, the Stored Communications Act ("SCA"), protects electronic communications held in storage;[153] and Title III, the Pen Register Statute, prohibits the use of pen registers or trap and trace devices to intercept the "content" of electronic communications in transit.[154] Additionally, an electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include . . . any communication from a tracking device."[155]

Each title has a different standard that the government must meet to compel disclosure of different classes of electronic communications. These standards are designed to comport with "the amount of privacy an individual can reasonably expect in communications that fall within each class."[156] In *Jones*, the majority declared that the *Katz* reasonable expectation of privacy test did not displace the trespassory test; and although he did not rule on the issue, Justice Scalia suggested, "where a classic trespassory search is not involved . . . resort must be had to *Katz*

148. Kerr, *A User's Guide*, *supra* note 134, at 1212–13.

149. Levis, *supra* note 27, at 204; *see also* Parker Higgins, *Highlighting a Privacy Problem: Apps Need to Respect User Rights From the Start*," ELECTRONIC FRONTIER FOUNDATION (Mar. 8, 2012) https://www.eff.org/deeplinks/2012/03/highlighting-privacy-problems-apps-need-respect-user-rights-start ("the California Online Privacy Protection Act of 2003 requires operators of online services that collect personally identifiable information from California residents to conspicuously post and comply with a privacy policy.").

150. Levis, *supra* note 29, at 204.

151. The Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. § 3711 (Jun. 19, 1968).

152. Title I of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1984 (codified as amended at 18 U.S.C. §§ 2510–2522 (2006)).

153. Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1984 (codified as amended at 18 U.S.C. §§ 2701–12 (2006)).

154. Title III of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1984 (codified as amended at 18 U.S.C. §§ 3121-27 (2006)).

155. 18 U.S.C. § 2510 (2006).

156. Levis, *supra* note 29, at 205.

analysis."[157] The government's potential use of LBS to track individuals presents precisely this situation in which no physical trespass is involved.

Title I of the ECPA requires that the government obtain a warrant based on probable cause that the electronic communication to be intercepted contains evidence of a crime.[158] The SCA requires only that the government "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[159] The Pen Register Statute merely necessitates that the government's application for a court order contain "a certification . . . that the information likely to be obtained is relevant to an ongoing criminal investigation."[160] The Communications Assistance for Law Enforcement Act ("CALEA") limits the government's ability to obtain information about a subscriber's physical location "solely pursuant" to the Pen Register Statute.[161]

Whether and to what degree a LBS user's location data is protected under the EPCA depends on six classifications. First, whether real-time LBS location information, such as a user's location broadcasted via Google Latitude, is an electronic communication "in transit" under Title I. Second, whether real-time location information is content or non-content information. Third, once LBS location information is in "storage," if the LBS is classified as a remote computing service ("RCS") or an electronic communications service ("ECS"). Fourth, whether the aggregate of a user's historical location information, such as their Foursquare or Facebook Places check-in history, is content or non-content information. Fifth, whether a GPS-enabled smartphone used to access LBS is a "mobile tracking device" as defined under the Pen Register Statute. And sixth, whether an exception to the ECPA applies.[162]

However, under third-party doctrine, regardless of whether information is protected under the ECPA, an individual relinquishes his reasonable expectation of privacy in information he discloses to the

157. United States v. Jones, 132 S.Ct. 945, 955 (2012).

158. Levis, *supra* note 29, at 205.

159. 18 U.S.C. § 2703(d) (2006).

160. 18 U.S.C. § 3122(b)(2) (2006).

161. 47 U.S.C. § 1002(a)(2) (2006).

162. Levis, *supra* note 29, at 211.

public.[163] Justice Sotomayor's concurrence indicating the possibility of a shift in Fourth Amendment jurisprudence away from strict application of third-party doctrine, however, places a premium on a user's decision to allow a LBS to broadcast his location publicly or to limit the audience that can view the user's information.[164] Arguably, an individual user's LBS privacy settings are the best evidence of his reasonable expectation of privacy in the information he shares, rather than a blanket rule that any disclosure to a third party vitiates that reasonable expectation. This interpretation has already gained favorable acceptance in the Ninth Circuit when the court in *Crispin v. Christian Audigier* held that "a review of plaintiff's privacy settings would definitively settle the question" of whether the plaintiff should be entitled to a reasonable expectation of privacy in his Facebook posts.[165]

1. Protection of LBS User Location Information Under the ECPA

As previously discussed, Title I of the ECPA applies to communications in transit.[166] Ambient LBS that allow users to broadcast their location in real-time fall under Title I because this location information is being transmitted from one user to another continuously as he or she travels from place to place to place. Google Latitude, for example, does not store a historical log of user location information; Google Latitude's privacy policy states: "Google stores only the most recent automatic update or location selection you manually entered."[167] The government therefore must obtain a warrant to legally intercept a user's real-time LBS location information.[168] Intercepting is defined as the "aural or other acquisition of the contents of any . . . electronic . . . communication through the use of any electronic . . . device."[169]

Under the Pen Register Statute, a "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[170] A smartphone, therefore, is a

163. *Id.* at 207. *See also* 18 U.S.C. § 2511(2)(g) ("It shall not be unlawful under the SCA for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.").

164. United States v. Jones, 132 S.Ct. 945, 957 (2012). (Sotomayor, J., concurring).

165. Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 991 (9th Cir. 2010).

166. 18 U.S.C. §§ 2510-2522 (2006).

167. Google Latitude*, Privacy*, GOOGLE, INC. http://sites.google.com/a/pressatgoogle.com/latitude/privacy (last visited Apr. 7, 2013).

168. Levis, *supra* note 29, at 205.

169. 18 U.S.C. § 2510(4) (2006).

170. 18 U.S.C. § 3117(b) (2006).

tracking device. GPS, CSI, Wi-Fi, and user actions that specify location can be used to track a smartphone user's movement. Ambient social networking LBS like Google Latitude enable a user to broadcast his or her location in real-time publicly, to friends of friends, or only to friends. It is no longer necessary for the government to physically invade property or maintain visual surveillance to track individuals; they can remotely track a user's GPS-enabled smartphone or determine a user's location by intercepting his or her real-time LBS location information. The CALEA, however, limits the Government's ability to use the Pen Register Statute to acquire a subscriber's physical location information.[171]

Stringent application of third-party doctrine and public exposure doctrine would cut against the privacy protections afforded LBS user location information by the Wiretap Act and the CALEA. By using ambient LBS, a user exposes his location to other users of the app; he might limit which users may view his location, or he might share it publicly. However, ambient LBS broadcast a user's location not just when he is in public outside. Google Maps for Android now enables users to find out exactly where they are indoors, such as inside a shopping mall or an airport.[172] It provides a detailed floor plan and even determines which floor the user is on.[173] Theoretically, the government could use this technology to pinpoint a target's exact location inside his home. In *Karo*, the Supreme Court held that it was a violation of the Fourth Amendment for the government to track the location of a beeper inside a home without a warrant.[174] Arguably, using LBS to indicate your location while inside your home and publicly sharing that information is similar to inviting the general public into your home. But if a LBS user takes affirmative steps to limit the audience with whom he shares his location, then surely pinpointing the user's location inside his home without a warrant should be a violation of the Fourth Amendment under the Court's rationale in *Karo*.

a. Protection of LBS User Location Information Under the SCA

Congress enacted the SCA because the Fourth Amendment does not address a multitude of potential breaches of privacy presented by

171. Levis, *supra* note 29, at 218–19.

172. *A New Frontier for Google Maps: mapping the indoors*, GOOGLE, INC. (Nov. 29, 2011) http://googleblog.blogspot.com/2011/11/new-frontier-for-google-maps-mapping.html.

173. *Id.*

174. United States v. Karo, 468 U.S. 705, 719 (1984).

the advent of the modern technology.[175] The SCA limits the ability of the government to compel service providers to disclose information about their customers and subscribers, and limits an Internet Service Providers's ("ISP") right to voluntarily disclose this information to the government.[176] The SCA has been described by the Ninth Circuit as "a complex, often convoluted, area of the law," and because "the SCA was written prior to the advent of the Internet . . . the existing statutory framework is ill-suited to address modern forms of communication."[177]

To fall under the SCA, an electronic communication must be in storage, where "[e]lectronic storage is defined as any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[178] Once it is established that a communication is in storage, it is necessary to determine if the service provider is a provider of an electronic communications service ("ECS") or a remote computing service ("RCS"). An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[179] A RCS, on the other hand, is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[180] A service provider's classification as an ECS or RCS depends on "the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time)."[181] If the service provider does not fit within either of these categories then only basic Fourth Amendment protections apply.[182] Explaining how the SCA has been applied to electronic communications such as Facebook posts will help to clarify the difference between an ECS and a RCS.

The Ninth Circuit held in *Crispin*, that a Facebook post "is not protectable as a form of temporary, intermediate storage."[183] The court said that "there is no temporary, intermediate step for wall postings or

175. Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 971 (9th Cir. 2010) (internal quotation marks and citations omitted).

176. *Id.* at 972.

177. *Id.* (internal citations omitted).

178. 18 U.S.C. § 2510 (2006).

179. 18 U.S.C. § 2510(15) (2002).

180. 18 U.S.C. § 2711(2) (2001).

181. Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 987 (9th Cir. 2010).

182. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, *supra* note 134, at 1213.

183. *Crispin*, 717 F. Supp. 2d at 989.

comments" because a Facebook post, unlike email, can be deemed received without being opened.[184] Once made, Facebook posts and comments are stored for backup purposes.[185] As a result, Facebook posts and comments are "in storage," and thus fall within the SCA. With respect to posts and comments, Facebook is an ECS provider because it provides users the ability to communicate with their friends.[186] Facebook is also a RCS provider because it stores user-generated content on its servers for the benefit of the user and the audience he designates.[187] Importantly, the Ninth Circuit stated in dicta that "the number of users who can view the stored message has no legal significance."[188]

A LBS is classified as an ECS when it is being used as form of communication between one person and another; one person who wants to share where they are and the other who wants to find out their friend's location. A LBS is an RCS when it is being used as a storage service to enable users to access a history of their whereabouts, and to enable the application to access historical location information for business purposes. Like Facebook posts and comments, there is no temporary, intermediate step for LBS location information. Once a user broadcasts his location or checks-in, this location information is immediately accessible to him or other users via the application. Depending on the application, LBS location information is also in storage once it resides on the application's servers for either backup or storage purposes for the benefit of the user and his friends. Thus, Foursquare and Facebook check-ins are also in storage because a user's check-in is posted on his or her profile immediately.

Whether a LBS is classified as an ECS or a RCS determines the standard that the government must meet to compel disclosure of LBS user location information. The government must obtain a search warrant to compel an ECS "to disclose contents of communications in its possession that are in temporary 'electronic storage' for 180 days or less."[189] To compel disclosure of content that has been in electronic storage for more than 180 days—including detailed records about the subscriber's use of the service—the government must obtain a search

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.* at 990.

188. *Id.*

189. Kerr, *A User's Guide*, *supra* note 134, at 1218.

warrant, or with prior notice to the subscriber it can obtain a subpoena[190] or a court order known colloquially as a "2703(d) order," if it provides "specific and articulable facts" showing that the content to be compelled is "relevant and material to an ongoing criminal investigation."[191] To compel non-content information from either an ECS or RCS, the government can obtain a search warrant,[192] a 2703(d) order,[193] or do so with the subscriber's consent.[194] With merely a subpoena however, the government can obtain "basic subscriber information" including name, address, telephone number, and call records.[195] A public ECS and RCS may not voluntarily disclose to the government content or non-content subscriber information unless it fits within an exception to the ECPA.[196]

Content is defined as "any information concerning the substance, purport, or meaning of that communication."[197] Content information is distinguishable from non-content information as "[c]ontent information is the communication that a person wishes to share or communicate with another person. . . . [N]oncontent information . . . is information about the communication that the network uses to deliver and process the content information."[198] On its face, a glimpse of a user's real-time location from ambient LBS is analogous to seeing someone walking down the street, and since the information inferred from visual apprehension is not protected under the Fourth Amendment, it makes sense that neither is real-time LBS location information. Yet a single check-in on Foursquare or Facebook actually is content information that is protected because a user checks-in to share his location with his friends and some LBS enable users to interact with the check-in by adding user-generated content such as a comment or review. Interestingly, Foursquare defines "content" in their terms of use as including "*any* location information."[199] And, when real-time location data is monitored over an extended period of time, or logged and accessed historically in the aggregate, inferences can be drawn about a

190. 18 U.S.C. § 2703(b)(1)(B) (2009).

191. Kerr, *A User's Guide*, *supra* note 134, at 1218 (quoting 18 U.S.C. § 2703(d) (2009)).

192. 18 U.S.C. § 2703(c)(1)(A) (2009).

193. 18 U.S.C. § 2703(c)(1)(B) (2009).

194. 18 U.S.C. § 2703(c)(1)(C) (2009).

195. Kerr, *A User's Guide*, *supra* note 134, at 1219–20 (citing 18 U.S.C. § 2703(c)(2) (2009)).

196. *Id.* at 1223 (citing 18 U.S.C. § 2702 (2008)).

197. 18 U.S.C. § 2510(8) (2002).

198. Kerr, *A User's Guide, supra* note 134, at 1228.

199. *Terms of Use, Content*, FOURSQUARE LABS, INC. (Jan. 29, 2013), http://Foursquare.com/legal/terms (emphasis added).

person's activities and associations to reveal an "intimate picture" of his life.[200]

Apparent in the discussion *supra*, the ECPA is overly technical and difficult to apply. In my opinion, under the SCA, LBS are ECS because regardless of whether they are later used for storage purposes their immediate use is as a form of communication. Therefore, to compel disclosure of LBS user location information in the form of a single check-in or aggregated historical location information that is less than 180 days old, the government should be forced to obtain a search warrant. The fact that the government may obtain LBS user content greater than 180 days old under a lesser standard than probable cause is particularly problematic because the more location data it can accumulate, the more accurately it can identify patterns to paint a detailed picture of a person's life.

IV. Application of the ECPA in Current Case Law on Electronic Communication Technologies Similar To LBS

To anticipate how real-time and historical LBS user location information is protected under the ECPA, it should be analogized to other forms of electronic communication such as cell-site information, email, and content on social networking sites for which a body of case law already exists. The cases that follow consider "whether a third-party service provider's right of access to [electronic] communication extinguishes the subscriber's reasonable expectation of privacy in the content of such communications."[201]

Those cases that hold that a user's reasonable expectation of privacy in his or her electronic communications is not extinguished by a third party service provider's right of access distinguish *United States v. Miller* and its progeny because modern communications technologies reveal a great deal more private information than bank records.[202] Those cases that hold that a user does not have a reasonable expectation of privacy in his electronic communications argue that users voluntarily convey this information to their service providers, extinguishing their

200. *EPCA Reform: Why Now?*, DIGITAL DUE PROCESS COALITION (2010) http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Apr. 7, 2013).

201. In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information (hereinafter "*In re Application*"), 2010 WL 5437209, 3 (E.D.N.Y. 2010).

202. *See* United States v. Miller, *supra* note 128. *See also* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

expectation of privacy under third-party doctrine.[203] The ECPA's weakness is reflected in the fact that federal courts lack any sort of consensus about how the statute applies to modern communications technologies.

A. Cell Site Location Information

In *In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, the Eastern District of New York held that mosaic theory as applied in *Maynard* was appropriate to apply to historical cell site information.[204] A cell phone user has a reasonable expectation of privacy in her historical cell site information because she does not "voluntarily expose[] information about her location," and these records "can effectively convey details that reveal the most sensitive information about a person's life-information that goes far beyond the ordinary course of the service provider's business."[205] Because granting the government access to cell site information records implicated the Fourth Amendment, the Eastern District required the government to make a showing of probable cause to obtain it.[206]

In *In re Application of the United States of America for Historical Cell Site Data*, cell site location data was "sufficient to plot the target's movements hour by hour for the duration of the 60 day period."[207] Similar to the Eastern District of New York, the Southern District of Texas also applied *Maynard*'s rationale that prolonged surveillance reveals an "intimate picture" of the target's life.[208] Since a cell phone user does not "knowingly expose" or "voluntarily convey" his cell site location information to his service provider in any meaningful way, "the bare possibility of disclosure by a third party cannot by itself dispel all expectation of privacy."[209] The court here held that cell site data is subject to Fourth Amendment protection and the government may not obtain it without a warrant based on probable cause.[210]

203. United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012).

204. *In re Application*, 2010 WL 5437209, 3.

205. *Id.* at 2–3.

206. *Id.* at 4.

207. In re Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 839 (S.D. Tex. 2010).

208. *Id.* at 835.

209. *Id.* at 839.

210. *Id.* at 845.

Counter to those two cases is *United States v. Graham*, in which the District of Maryland held that no Fourth Amendment violation occurred by granting the government's application for a 2703(d) order for historical cell site data under the SCA's "specific and articulable facts" standard.[211] The court concluded the Fourth Amendment did not protect historical cell site data because it is not reasonable to hold an expectation of privacy in it.[212] Applying a strict interpretation of the third-party doctrine, the defendants voluntarily conveyed their location to their cellular provider by using their phones and the historical cell site data "were business records kept in the ordinary course of business by the Defendants' cellular provider."[213]

United States v. Skinner dealt with the government's use of GPS data to track a target without engaging in a physical trespass, precisely the situation raised at the beginning of this note.[214] In *Skinner*, the Sixth Circuit ruled that the government's use of GPS location information from a target's cell phone to track its real-time location was not a violation of the Fourth Amendment because the target did not have a reasonable expectation of privacy in that data.[215] The court held that when determining whether a defendant's reasonable expectation of privacy has been violated, a court should examine the information that the defendant disclosed to the public, not what information the police knew.[216] Distinguishing *Jones*, the Sixth Circuit said there was no physical trespass and "no [] extreme comprehensive tracking is present in this case."[217]

In her concurring opinion in the judgment only, Judge Donald engaged in the kind of forward thinking that is necessary to protect LBS user location information under the Fourth Amendment. Judge Donald would have found that the tracking was a search within the meaning of the Fourth Amendment because Skinner's expectation of privacy in the GPS data emanating from his cell phone was reasonable.[218] To Judge Donald, Skinner's erroneous belief about, or ignorance of, a cell phone's GPS capabilities and the fact that he most likely did not anticipate that his phone was trackable shows that he had a subjective expectation of

211. United States v. Graham, 846 F. Supp. 2d 384 (D. Md., 2012).

212. *Id.*

213. *Id.* at 403.

214. United States v. Skinner, 690 F.3d 772 (6th Cir., 2012).

215. *Id.* at 775.

216. *Id.* at 779.

217. *Id.* at 780.

218. *Id.* at 786 (Donald, J., concurring in part and concurring in judgment).

privacy in his GPS data.[219] More importantly, the fact that "society is prepared to recognize a legitimate expectation of privacy in the GPS data emitted from any cell phone," requires that such information gathering mandates a warrant.[220]

Under the rationale of some of these cases, LBS user location information might not be protected. Although a user's location data in the aggregate reveals an "intimate picture" of his life, LBS users "knowingly expose" and "voluntarily convey" their location to the application, which is analogous to a cellular service provider. In other words, LBS users know or should know that by using LBS they are they are disclosing their location information to the LBS, and therefore consenting to possible compelled disclosure of that data to the government.[221] Unlike cell phone users who inadvertently reveal their location by virtue of carrying a cell phone that is turned on, LBS users intentionally share their location with the application.

But LBS users likely do not expect that by providing their location information to the application or service, the government can acquire it. Even if a LBS privacy policy or terms of service states that the company may disclose user information, it is futile to point to legal fine print and map a negligence standard onto criminal law to argue that users' expectations of privacy are not reasonable because these agreements are very rarely read.[222] In other words, if a user did not have actual knowledge of the privacy policy, it is difficult to argue that they did not have a subjective expectation of privacy in their LBS location information. Furthermore, in California, at least, contracts of adhesion are not enforced if contrary to people's expectations.[223] Unless a user

219. *Id.* at 784 (Donald, J., concurring in part and concurring in judgment).

220. *Id.* at 785 (Donald, J., concurring in part and concurring in judgment).

221. Kerr, *The Case for Third-Party Doctrine*, *supra* note 129, at 588. *See also* In Re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d. 114 (E.D. Va. Nov. 10, 2011) (holding that Twitter's disclosure of petitioners' IP address to the government was not a search because petitioners did not have a reasonable expectation of privacy in their IP address, which was subject to examination by Twitter).

222. In Re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d. 114 (E.D. Va. Nov. 10, 2011) (holding that petitioners had a lessened expectation of privacy in their IP address because by creating a Twitter account and using the service, they agreed to Twitter's privacy policy and "knew or should have known that their IP address was subject to examination by Twitter").

223. California Civil Code Section 1670.5(a) provides a court with several options: "If the court as a matter of law finds the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result." California courts have been at the vanguard of deeming Internet contract clauses unconscionable, and hence unenforceable.

shares his location publicly, the fact that he has circumscribed the audience with whom he shares it is evidence of his subjective expectation of privacy.

And although checking-in to a coffee shop on Foursquare is not a necessity in modern life like dialing a phone number or maintaining a bank account, LBS user location data encompasses so much more than a Foursquare check-in. We do many things on our smartphones that are necessary to participate in society: making or taking a call, checking and sending email, or using Google Maps for directions. Since our location information can be ascertained from uses like these, some LBS usage can almost be said to involve involuntary disclosures of our location information. For these reasons, I believe that a better standard than the reasonable expectation of privacy test would be whether a person intends to limit access to his location information in a way that society recognizes as reasonable. The fact that a person uses LBS in furtherance of criminal activity should not matter—"numerous courts have held that privacy expectations are not diminished by the criminality of a defendant's activities."[224]

B. Email

In *Rehberg v. Paulk*, the Eleventh Circuit stated that by sending an email to a third party, the sender loses a reasonable expectation of privacy in it.[225] However, in *United States v. Warshak*, the Sixth Circuit held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a

See Comb v. Pay Pal, Inc., 218 F. Supp. 2d. 1165 (2002) (holding that a user agreement's arbitration clause was unconscionable because it was a contract of adhesion; the clause lacked mutuality, and it had the practical effects of precluding joinder of claims, and allowing prohibitive arbitration fees.).

224. United States v. Skinner, 690 F.3d 772, 785 (6th Cir. 2012). (Donald, J., concurring in part and concurring in judgment).

225. Rehberg v. Paulk, 598 F.3d 1268, 1281–82 *opinion vacated and superseded on reh'g,* 611 F.3d 828 (11th Cir. 2010) *cert. granted,* 131 S. Ct. 1678 (2011). On rehearing, the Eleventh Circuit cited the Sixth Circuit's decision in Guest v. Leis, 255 F.3d 325, 333 (6th Cir.2001) which "reasoned that a person would lose a legitimate expectation of privacy in a sent email that had already reached its recipient, analogizing an emailer to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of a letter." Rehberg v. Paulk, 611 F.3d at 843–44 (11th Cir. 2010) *cert. granted,* 131 S. Ct. 1678 (2011) (internal citations omitted). However, the Eleventh Circuit declined to rule on the issue of Rehberg's right to privacy in his emails and decided the case on narrower grounds. *See also* United States v. Lifshiftz, 369 F.3d 173, 190 (2d Cir. 2004) (holding that "[i]ndividuals . . . may not . . . enjoy [] an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient."); United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (declining to decide the issue of "whether there is a constitutional expectation of privacy in e-mail.").

commercial ISP," notwithstanding the fact that the third party ISP had access to the emails.[226] The Sixth Circuit distinguished emails from the bank records involved in *Miller*, reasoning that emails potentially contain "confidential communications," whereas bank records are "simple business records."[227] Furthermore, the court pointed out that the ISP is "not the intended recipient of the emails," whereas the bank uses bank records "in the ordinary course of business."[228] The Sixth Circuit concluded that the government must obtain a warrant based on probable cause to compel an ISP to disclose the contents of an email.[229]

Like email, check-ins and aggregated historical location data are potentially sensitive in nature. And like email, LBS user location information is sent, received, and stored by the service provider. Arguably, a user's friends are the only intended recipients of his or her location information. Yet Foursquare users earn badges for checking-in, requiring the application itself to receive and categorize the user's location. Some users allow LBS to determine their location to receive personalized recommendations, while many LBS use location information in the ordinary course of business by mining this data to provide a better service for users, to iterate on the application, and to provide user information to advertisers to enable them to serve targeted ads.[230] Under the Sixth Circuit's rationale in *Warshak*, Fourth Amendment protection of LBS user location information would not be extinguished merely because the LBS has access to it.

C. Social Networks

In *Crispin*, the Ninth Circuit held that a user of a social networking site has a personal privacy right in information on his or her profile or in his or her inbox.[231] The court concluded that a Facebook wall, like private electronic bulletin board services ("BBS"), is classified as an ECS under the SCA.[232] Given that some Facebook walls are restricted, it deserved ECS classification, whereas a completely public BBS does not merit protection under the SCA.[233] Since Facebook posts are accessible

226. 631 F.3d 266, 288 (internal citations omitted).

227. *Id.*

228. *Id.*

229. *Id.*

230. *Foursquare Labs, Inc. Privacy Policy, What Personal Information Does Foursquare Collect?*, FOURSQUARE LABS, INC. (Jan. 29, 2013), http://foursquare.com/legal/privacy.

231. Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 974 (9th Cir. 2010).

232. *Id.*; *See also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002).

233. *Crispin*, 717 F. Supp. 2d at 981.

only to an audience selected by the user, the Facebook wall (now Timeline) is "not strictly 'public.'"[234] The case was remanded so that the parties could "develop a further evidentiary record regarding plaintiff's privacy settings and the extent of access allowed to his Facebook wall."[235] The Ninth Circuit suggested that the plaintiff's privacy settings were dispositive of his reasonable expectation of privacy in the content of his wall posts.[236] If the plaintiff limited access to his Facebook wall, then the subpoenas should be quashed; if it was accessible to the public, then the subpoenas should be granted.[237]

Foursquare and Facebook check-ins are most similar to Facebook posts when their access is restricted to other users who the user selects rather than publicly available. A check-in on Facebook Places is literally posted to a user's timeline; therefore, under *Crispin*, a user has a reasonable expectation of privacy in his check-ins. And a user's Foursquare history functions similarly to a Facebook timeline in that the user and his friends may comment on check-ins. Under the rationale of *Crispin*, so long as the user restricts access to his location information he retains a reasonable expectation of privacy in that information, even though the third party LBS has access to it.

D. Summary

In only a few short years, case law has already considered electronic communication technologies governed by the ECPA, and most of the opinions were ultimately decided on the basis of the individual's reasonable expectation of privacy and the applicability of third-party doctrine, rather than through parsing the statute. Many of the decisions made on those bases resulted in unjust holdings that jeopardize our right to privacy in what we do with our smartphones, while only a few judges properly felt that electronic communications should receive robust Fourth Amendment protection. If a LBS user publicly broadcasts his location or publicly shares his check-ins, then even in the aggregate his location information is not protected under the Fourth Amendment and it does not fall under protection of the ECPA. If the user deliberately makes his location publicly available, he assumes the risk that the government will obtain this information and use it against him. But as

234. *Id.* at 980.

235. *Id.* at 991.

236. *Id.* ("a review of plaintiff's privacy settings would definitively settle the question").

237. *Id.* ("Given that the only information in the record implied restricted access, the court concludes that Judge McDermott's order regarding . . . subpoenas [seeking Facebook wall postings] was contrary to law.").

users become more aware of and concerned about digital privacy, they are sharing less publicly.

Even if many LBS users do not mind if an application or the government can access their location information because they are law-abiding citizens, we should be concerned as the government's acquisition and use of this information may have disproportionate effects on minorities. A recent Pew Internet study found that:

> Geosocial services and automatic location-tagging are most popular with minorities. . . . Hispanics are the most active in these two activities, with a quarter (25%) of latino smartphone owners using geosocial services and almost a third (31%) of ;atino social media users enabling automatic location-tagging. However, though only 7% of white smartphone owners use geosocial services.[238]

LBS offer benefits such as "self-expression and socialization."[239] Human beings' social nature motivates us to use LBS. This desire for social connection "can trigger systemic biases in the mechanisms that people use to evaluate privacy risks" and explains why "notwithstanding its well known privacy risks . . . [people] systematically underestimate those risks."[240] This is more evidence for the proposition that smartphone users likely do hold a subjective expectation of privacy in their location information emanating, voluntarily or not, from their phones. Furthermore, as discussed *supra*, use of LBS is becoming ever more important to participate fully in today's technologically advanced society. For millions of Americans, social networking and LBS are fast approaching the same essential communication role as the telephone and email.[241] It is necessary to reconcile the growing importance of LBS as a form of modern communication with the fact that LBS user location information may not receive adequate privacy protection under the Fourth Amendment or the ECPA. Two bills currently in the Senate

238. Zickuhr & Smith, *supra* note 19, at 3.

239. Brown, *supra* note 23, at 307.

240. *Id.* *See also* Zickuhr & Smith, *supra* note 19, at 7 ("Many social media sites, including social networking sites such as Facebook and the status-updating service Twitter, enable users to set up the service to automatically post information about their current location along with their updates on the site. Our survey found that 14% of social media users take advantage of these services, and have set up their account to automatically include their location in their posts.").

241. Brown, *supra* note 23, at 305–306.

attempt to address this conflict by amending the ECPA and by establishing stringent privacy protections for geolocation information.

V. Potential ECPA Reform

Simply put, the "ECPA does not clearly state the standard for governmental access to location information."[242] This leaves LBS users "confused about the security of their data" when the government requests access and companies are "unable to assure their customers that subscriber data will be uniformly protected."[243] Digital Due Process, a coalition of privacy advocates, academics, companies, and think tanks has articulated a clear principle of ECPA reform: "simplify, clarify and unify the EPCA standards."[244] This requires that the government obtain a search warrant based on probable cause to compel disclosure of "communications that are not readily accessible to the public," regardless of their age; and "preserv[e] the legal tools necessary for [the Government] to enforce laws . . . and protect the public."[245]

In May 2011, Senator Patrick Leahy introduced S. 1011, the "Electronic Communications Privacy Act Amendments of 2011."[246] Senator Leahy is pushing for ECPA reform to "protect American's privacy, . . . encourage American innovation and instill confidence in American consumers."[247] Senator Leahy's bill includes provisions specifically for a "geolocation information service," defined as "the provision of a global positioning service or other mapping, locational, or directional information service."[248] LBS are a classified as a geolocation information service provider under the bill.

242. *EPCA Reform: Why Now?*, DIGITAL DUE PROCESS COALITION (2010) http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Apr. 7, 2013).

243. *Id.*

244. *Our Principles*, DIGITAL DUE PROCESS COALITION (2010) http://www.digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Apr. 7, 2013).

245. *Id.*

246. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112s1011is/pdf/BILLS-112s1011is.pdf.

247. David Carle, *Leahy Chairs SJC Hearing to Explore Reforms to Digital Privacy Laws*, PATRICK LEAHY FOR UNITED STATES SENATOR FOR VERMONT (Sept. 22, 2010) http://www.leahy.senate.gov/press/press_releases/release/?id=ce247be0-71ab-4fd4-a37d-12d765e9726f.

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

The bill also "requires that the government obtain either a search warrant or a court order under the Foreign Intelligence Surveillance Act to access or use an individual's smartphone or other electronic communications device to obtain geolocation information."[249] Furthermore, the bill distinguishes between real-time and historical geolocation information, providing a legal standard for each. The government must obtain a search warrant to acquire real-time geolocation information from a service provider, while to obtain historical geolocation information, either a search warrant or a court order is sufficient.[250] In addition to these reforms, the ACLU of Northern California suggests that a warrant be required to use cell phones as tracking devices, and that a suppression remedy be available for evidence obtained in violation of the ECPA.[251]

In June 2011, Senator Ron Wyden (D-OR) introduced S. 1212, the Geolocational Privacy and Surveillance Act ("GPS Act"). The bill amends the EPCA "to specify the circumstances in which a person may acquire geolocation information."[252] Modeled after the Wiretap Act, the GPS Act requires that the government obtain a warrant to acquire geolocation information and provides an exclusionary remedy, "prohibit[ing] unlawfully intercepted geolocation information from being used as evidence."[253]

Conclusion

In conclusion, the Court's excavation of the trespass doctrine in *United States v. Jones* and Justice Sotomayor's invitation to reconsider whether third-party doctrine has a place in the digital age has disrupted Fourth Amendment Jurisprudence. Yet, by using a property-based approach to find a Fourth Amendment violation in that case, the Court sidestepped the larger question of whether the government's prolonged surveillance of Jones violated his reasonable expectation of privacy. Taken a step further, deciding this question might have led the Court to discuss the situation in which the government tracks an individual for an

249. *Id.*

250. *Id.*

251. *Privacy Laws Don't Auto-Update. Demand a Privacy Upgrade.*, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA (2012) http://dotrights.org/lawmakers (last visited Apr. 7, 2013).

252. Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (2011) *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112s1212is/pdf/BILLS-112s1212is.pdf.

253. *Section-by-Section Summary, Geolocation and Privacy Surveillance ("GPS") Act*, UNITED STATES SENATOR RON WYDEN http://wyden.senate.gov/issues/issue/?id=b29a3450-f722-4571-96f0-83c8ededc332#sections (last visited Apr. 7, 2013).

extended period of time without physical trespass. Since the Court did not decide this question, we are left to parse outdated and overly technical statutory law and to analogize LBS user location information to case law about similar electronic communications.

Americans are using LBS more and more to identify themselves and to reap the benefits of this technology. But LBS user location information does not fit neatly within existing Fourth Amendment law or federal statutory law. Consequently, it is unclear whether, and to what extent, this sensitive information is protected from government intrusion. Since LBS user location information is precisely the kind of sensitive information that the Founders sought to protect from governmental intrusion, courts should accept Justice Sotomayor's invitation and reconsider the application of not only third-party doctrine, but also the reasonable expectation of privacy test to electronic communications like LBS user location information. The ecosystem of social, local, and mobile applications and services is growing rapidly, changing markets and driving innovation. It is important that digital privacy laws neither stifle innovation nor discourage its adoption.