Golden Gate University Law Review

Volume 43 | Issue 3 Article 5

August 2013

Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data

Alexandra D. Vesalga
Golden Gate University School of Law

COMMENT

LOCATION, LOCATION, LOCATION: UPDATING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT TO PROTECT GEOLOCATIONAL DATA

*ALEXANDRA D. VESALGA**

INTRODUCTION

User data is the new currency.[1] Technology companies, like all companies, earn success in the marketplace by building and maintaining relevance to consumers and society. Today's technology users demand easy accessibility and manifest utility in web products. Technology companies achieve these objectives by understanding their customers through data about their use of the service. This data includes information about when, where, and how users access web services—basic logs detail the time, date, and location of a user, how a user came to find the product, and what a user viewed while on the website or

* Editor-in-Chief, *Golden Gate University Law Review*, J.D., 2013, Golden Gate University School of Law; B.A., Philosophy, San Francisco State University, 2007. I am indebted to Kyle Mabe, Kate Baldridge, and Ed Baskauskas for their invaluable edits to this Comment, and to the entire *Law Review* Editorial Board for their diligence and grace throughout the year. I am eternally grateful to my family for their boundless support, and to the academics, scholars, and thinkers of every generation.

[1] *See, e.g.*, *Clicking for Gold: How Internet Companies Profit from Data on the Web*, ECONOMIST, Feb. 25, 2010, *available at* www.economist.com/node/15557431 (explaining the enormous value of user data to Google and other Internet companies); Wesley Gee, *Internet Tracking: Stalking or a Necessary Tool for Keeping the Internet Free?*, 20 COMMLAW CONSPECTUS 223 (2011) (describing how user data drives the Internet advertising industry).

application.[2] Geolocational data—data that pinpoints a user's location—is among the most useful, vital, and coveted data for technology companies, as it allows a web service to make relevant suggestions based on a user's real-time location and improves the relevance of targeted online advertising.[3]

Serious privacy concerns accompany the surging popularity of location-based services on the web.[4] The law has failed to keep pace with advances in technology and does not consistently protect the geolocational information that is collected from users in the course of their daily online activities. Current legal standards governing the disclosure of user data have long been a frustration for courts,[5] technology service providers,[6] and privacy scholars.[7] But more disconcerting is the growing divide between these standards and users' common expectations of privacy. As technology progresses and legislative protection of electronic communications remains stagnant, this divide widens.

This Comment is concerned with the Electronic Communications Privacy Act's (ECPA's) failure to consistently protect the geolocational data associated with electronic communications. ECPA was crafted in 1986 to protect electronic communications, a fledgling technology at the time.[8] Today, ECPA remains largely unchanged and still controls the

---

[2] *See, e.g.*, *Privacy Policy, Information We Collect, Log Information*, GOOGLE, www.google.com/intl/en/policies/privacy/ (last modified July 27, 2012); *Privacy Policy, Log Data*, TWITTER, www.twitter.com/privacy (last visited Apr. 13, 2013); *Privacy Notice, Examples of Information Collected*, AMAZON, www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496 (last updated Apr. 6, 2012).

[3] *See* Dan Tynan, *Why Location Privacy Is Important*, IT WORLD (June 25, 2010, 3:31 PM), www.itworld.com/mobile-amp-wireless/112204/why-location-privacy-important?page=0,0 (describing the surging popularity of location-based services); *see also* Gee, *supra* note 1.

[4] *Mobile Life: Which Feature and Apps Hold the Strongest Appeal Around the World?*, TNS, www.tnsglobal.com/mobile-life/country/feature/us/ca (2012 market research study indicating that 40% of mobile users in the United States currently use location-based services, and 29% of those who do not currently use location-based services are interested in the services); *see also* Tynan, *supra* note 3.

[5] Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) ("a statute as complex as the Wiretap Act, which is famous (if not infamous) for its lack of clarity"); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004).

[6] *Who We Are*, DIGITAL DUE PROCESS, www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited Apr. 24, 2013) (listing members of the coalition, including Apple, Google, Amazon, and Microsoft).

[7] *Id.* (listing members of the coalition, including the ACLU, Electronic Frontier Foundation, and Liberty Coalition).

[8] 18 U.S.C.A. §§ 2510–2522 (Westlaw 2013); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848; Press Release, Sen. Patrick Leahy, Leahy Marks 25th Anniversary of ECPA, Announces Plan To Mark Up Reform Bill (Oct. 20, 2011), *available at*

government's right to access individuals' electronic communications.[9] Senator Leahy, who originally drafted ECPA, has called for reform of the Act, stating that "today, this law is significantly outdated and outpaced by rapid changes in technology."[10] Senator Leahy has proposed significant changes to the Act that would eliminate many of its outmoded standards and offer increased protection of individuals' privacy.[11] The proposed amendments, however, fail to address one key privacy issue: how much data *about* a communication can be compelled from a web service provider by the government without a warrant. This ambiguity has led to the disparate treatment of different types of geolocational data in the courts. While proposed amendments to ECPA would alleviate many of the law's inadequacies, they stop short of properly protecting geolocational data and fail to comprehensively address inconsistencies in the courts' treatment of searches of this data.

Part I of this Comment explores the importance and popularity of location-based web services. Part II discusses the different technologies that drive these services, and the services themselves. Part III explains how the law treats the disclosure of geolocational data, and examines how courts have analogized electronic communications to traditional communications, resulting in conflicting rules about the disclosure of geolocational data. Part IV argues that these rules fail to properly protect users' reasonable expectations of privacy, and proposes that ECPA be amended to affirmatively and equally protect all types of geolocational data, regardless of the underlying technology. Finally, Part V examines technology providers' frustration with the current state of the law.

I. LOCATION MATTERS

The most obvious benefit of geolocational technologies is to Internet users. Services utilizing geolocational data are ubiquitous in Americans' everyday lives:[12] search engines use geolocational data to provide relevant search results on their desktop and mobile products, online map services use geolocational data to determine the starting point for directions, an entire social networking phenomenon based solely on

---

www.leahy.senate.gov/press/press_releases/release/?id=56C35200-EFDC-497A-9EAF-A75B498515B8; *see generally* Kerr, *supra* note 5, at 1209–13.

[9] Kerr, *supra* note 5, at 1208.

[10] Press Release, Sen. Patrick Leahy, *supra* note 8.

[11] Press Release, Sen. Patrick Leahy, Leahy, Lee Introduce Legislation To Update Electronic Communications Privacy Act (Mar. 19, 2013), *available at* www.leahy.senate.gov/press/leahy-lee-introduce-legislation-to-update-electronic-communications-privacy-act.

[12] *Mobile Life: Which Feature and Apps Hold the Strongest Appeal Around the World?*, *supra* note 4; *see also* Tynan, *supra* note 3.

location has emerged, and platforms offering relevant goods and services in users' immediate vicinity abound.[13]

Geolocational information also delivers two palpable benefits to web service providers. First, this information allows web services to better understand their user bases and respond with more robust services, improving the convenience and value of technology products in the marketplace.[14] Second, user data, particularly geolocational data, is vital to the third-party advertising market.[15] Sir Martin Sorrell, CEO and founder of WPP, one of the world's largest advertising companies, says "Location targeting is the holy grail that we . . . are looking for."[16] The global Internet advertising industry saw $88 billion in revenue in 2012, and is expected to grow by 15% in 2013.[17] Because geolocational data reveals users' locations, advertisers can effectively target advertising to users based on their cities of residence and travel, the businesses and areas they frequent, or their precise location at a given time.[18] With Internet advertising, relevance is king, and the more data a web service has about its users, the more revenue it can draw from third-party advertisers.[19] Third-party advertising is the financial cornerstone of the Internet and the reason that many popular web services are free for users.[20]

---

[13] These technologies are discussed in more detail *infra* Part II. For insight on lesser-known geolocational services, *see* Testimony of Alan Davidson, Dir. of Pub. Policy, Google Inc., Before the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law (May 10, 2011), *available at* www.judiciary.senate.gov/pdf/11-5-10%20Davidson%20 Testimony.pdf.

[14] *See* CHARLES STEINFIELD, DEP'T OF TELECOMM., MICH. STATE UNIV., THE DEVELOPMENT OF LOCATION BASED SERVICES IN MOBILE COMMERCE 7-9 (2004), *available at* www.msu.edu/~steinfie/elifelbschap.pdf.

[15] *See, e.g.*, *Clicking for Gold: How Internet Companies Profit from Data on the Web*, *supra* note 1; *see also* Gee, *supra* note 1.

[16] Stuart Dredge, *WPP's Sorrell Hails the Power of Apps*, THE GUARDIAN (Feb. 15, 2011, 6:53 PM), www.guardian.co.uk/technology/appsblog/2011/feb/15/wpp-sir-martin-sorrell-mobile-apps.

[17] Ryan Faughnder, *Web Advertising To Grow Faster than Broad Market in 2013*, BLOOMBERG (Nov. 20, 2012, 10:29 AM), www.bloomberg.com/news/2012-11-20/web-advertising-to-grow-faster-than-broad-market-in-2013.html.

[18] *See* Steve Olenski, *Is Location Based Advertising the Future of Mobile Marketing and Mobile Advertising?*, FORBES (Jan. 17, 2013, 10:16 AM), www.forbes.com/sites/marketshare/2013/01/17/is-location-based-advertising-the-future-of-mobile-marketing-and-mobile-advertising/.

[19] *See* Greg McFarlane, *How Does Google Make Its Money?*, INVESTOPEDIA (Nov. 22, 2012), www.investopedia.com/stock-analysis/2012/what-does-google-actually-make-money-from-goog1121.aspx (explaining how Google's algorithms generate relevant advertisements).

[20] *See id.*; *see also* Gee, *supra* note 1.

II. THE TECHNOLOGIES AT ISSUE: "OMNISCIENCE" IS SPELLED 01001111 01101101 01101110 01101001 01110011 01100011 01101001 01100101 01101110 01100011 01100101[21]

Three distinct technologies are used by web service providers to determine a user's location: Internet Protocol addresses (IP addresses), cell sites, and the Geological Positioning System (GPS).[22] Today, IP addresses are used primarily by Internet-connected devices such as computers and tablets (while connected to a wireless network), while cell sites and GPS are used by mobile devices—Internet-connected smartphones and tablets (while connected to a telephonic, "3G" or "4G" network).[23] Developing technologies seek to use IP addressing technology as a primary and comprehensive geolocational tool for both mobile and desktop products.[24] Each of these technologies is discussed in turn.

A. IP ADDRESSES

To connect to and browse the Internet, a user must have an IP address.[25] An IP address routes information and data to other servers and computers, and allows the user to access websites and data on the Internet.[26] IP addresses are binary (ones and zeros), but they can be translated into a readable format that displays four numbers between 0 and 255 separated by periods.[27] Many Internet users are unaware of what their IP address is, or even what an IP address is in general.[28] While IP address records do not themselves disclose the identities of Internet users, a user can be "matched" to a particular IP address through the records of their Internet Service Provider (ISP).[29] Proposed legislation has unsuccessfully sought to require ISPs to retain this data for one year.[30]

---

[21] BINARY TRANSLATOR, www.binarytranslator.com/index.php (last visited Apr. 24, 2013).

[22] STEINFIELD, *supra* note 14, at 4-6 tbls. 1, 2.

[23] *Id.*

[24] *See Skyhook Location and Performance*, SKYHOOK, www.skyhookwireless.com/location-technology/performance.php (last visited Apr. 24, 2013).

[25] *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 119-20 (E.D. Va. 2011).

[26] *Id.*

[27] *Id.* at 119.

[28] *Id.* at 120.

[29] United States v. Vosburgh, 602 F.3d 512, 523 (3d Cir. 2010).

[30] Protecting Children from Internet Pornographers Act of 2011, H.R. 1981, 112th Cong. § 4(a)(1).

IP addressing takes two forms: static and dynamic.[31] A static IP address is a permanent, fixed address assigned to a particular computer or other device every time it connects to the Internet,[32] while dynamic IP addressing assigns new IP addresses at random, often each time a user connects to the Internet.[33] Because static addressing does not convey any tangible benefit to most Internet users,[34] and because rapid growth of the Internet in both popularity and scope has led to concerns of imminent IP address exhaustion, dynamic IP addressing is most common for general Internet consumers.[35] To alleviate the shortage of available IP addresses while new addressing technology is developed, ISPs have moved to dynamic addressing to allocate IP addresses when they are not in use.[36] This allows IP addresses to be "time-shared" by Internet users.[37]

When a user browses the Internet, every website he or she visits automatically captures the user's IP address.[38] Websites can use an IP address to triangulate a user's location by analyzing the wireless and cellular network points in that vicinity.[39] The accuracy of IP geolocational information has vastly improved in recent years,[40] with

---

[31] Ashish Mundhra, *GT Explains: What Is an IP Address and Difference Between a Static and Dynamic IP Address?*, GUIDING TECH (Dec. 16, 2011), www.guidingtech.com/8987/gt-explains-what-is-an-ip-address-and-difference-between-a-static-and-dynamic-ip-address/.

[32] *Id.*

[33] *Id.*

[34] COMM. ON COMMC'NS POLICY OF THE INST. OF ELEC. & ELECS. ENG'RS, U.S. OF AM., NEXT GENERATION INTERNET: IPV4 ADDRESS EXHAUSTION, MITIGATION STRATEGIES AND IMPLICATIONS FOR THE U.S. 10-11, *available at* www.ieeeusa.org/policy/whitepapers/IEEEUSAWP-IPv62009.pdf [hereinafter IPV4 MITIGATION]. For a simplified explanation, *see IPv4 Address Exhaustion*, WIKIPEDIA, www.en.wikipedia.org/wiki/IPv4_address_exhaustion#Exhaustion (last modified Apr. 3, 2013).

[35] IPV4 MITIGATION, *supra* note 34, at 5. Because dynamic IP addressing is most common for Internet users, this Comment focuses on that technology and its attendant privacy concerns, and will not discuss the distinct privacy concerns associated with static IP addressing.

[36] *Id.*

[37] *Id.*

[38] *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 120 (E.D. Va. 2011).

[39] *See, e.g.*, *Windows Internet Explorer 9 Privacy Statement*, MICROSOFT, www.windows.microsoft.com/en-US/Internet-explorer/products/ie-9/windows-Internet-explorer-9-privacy-statement (last updated Mar. 2011); *Location-Aware Browsing, How Does it Work?*, MOZILLA, www.mozilla.org/en-US/firefox/geolocation/ (last visited Apr. 24, 2013). To try this first-hand, see IP GEOLOCATOR, www.ipligence.com/geolocation (last visited Apr. 13, 2013).

[40] Thomas Lowenthal, *IP Address Can Now Pin Down Your Location to Within Half a Mile*, ARS TECHNICA (Apr. 22, 2011, 10:15 AM), www.arstechnica.com/tech-policy/2011/04/getting-warmer-an-ip-address-can-map-you-within-half-a-mile/.

recent technology capable of pinpointing users within half a mile in densely populated areas.[41]

Desktop web services have long capitalized on the ability of IP addresses to identify a user's location.[42] For instance, Google's search engine reads a user's location via his or her IP address to automatically return suggested, locationally relevant search results.[43] If one accesses Google's search function from a home computer in San Francisco, and enters the search term "best restaurants," the first suggested search term is "best restaurants in San Francisco."[44] Google Maps obtains a user's location for purposes of populating directions from that location, or to show services or goods in the user's immediate area.[45]

Social networking service providers also use this technology in their desktop products to enrich users' experience and increase connectivity between users. For example, Facebook automatically reads a user's city and state and includes that location on the user's updates, and allows users to share more specific locations, such as a restaurant or a store.[46] Similarly, Twitter allows users the option to include locational information in their updates.[47]

More recently, online retailers have started using IP addresses to automatically populate information about their physical store locations nearest to a user,[48] to adjust online retail pricing according to a user's location, and to tailor deals to users based on users' geography.[49] Web browsers have also created products that utilize the increased accuracy of geolocational information derived from users' IP addresses, with "location-aware browsing" products, by which the web browser will share a user's precise location with a website, so that the website may

---

[41] YONG WANG ET AL., TOWARDS STREET-LEVEL CLIENT-INDEPENDENT IP GEOLOCATION (2011), *available at* static.usenix.org/events/nsdi11/tech/full_papers/Wang_Yong.pdf.

[42] *Mobile Life: Which Feature and Apps Hold the Strongest Appeal Around the World?*, *supra* note 4; *see also* Tynan, *supra* note 3.

[43] *Location Settings*, GOOGLE, https://support.google.com/websearch/answer/179386?hl=en (last visited Apr. 24, 2013).

[44] *Id.*

[45] *Automatic Location*, GOOGLE, https://support.google.com/maps/bin/answer.py?hl=en&answer=1259155&topic=1687353&ctx=topic (last visited Apr. 24, 2013).

[46] *How Do I Add My Location to a Post?*, FACEBOOK, www.facebook.com/help/115298751894487/?q=location&sid=06zq64xzSCyA5IXtv (last visited Apr. 24, 2013).

[47] *FAQs About the Tweet Location Feature*, TWITTER, www.support.twitter.com/articles/78525-faqs-about-the-tweet-location-feature (last visited Apr. 13, 2013).

[48] *See, e.g.*, *Store Locator*, GAP, www.gap.com/customerService/storeLocator.do?mlink=5058,5746857,CS_Footer_StoreLocator&clink=5746857 (last visited Apr. 24, 2013); ANTHROPOLOGIE, www.anthropologie.com (last visited Apr. 24, 2013).

[49] Jennifer Valentino-Devries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J., Dec. 24, 2012, at A1.

provide locationally relevant information.[50] IP address geolocational technology continues to rapidly advance and may soon parallel or eclipse the accuracy of other geolocational technologies.[51]

B. MOBILE POSITIONING

Mobile positioning—the ability of a mobile service provider to trace a user's precise location—occurs by analyzing two forms of data: cell site data and GPS data.[52] All mobile service providers collect cell site data as part of routing and transmitting phone calls.[53] Cellular phones operate by searching for and connecting to cell sites, which contain transmitters that allow users to connect to a cellular network to make calls and receive data on their phones.[54] This process occurs constantly while the phone is powered on, even while in an idle state.[55] Cellular phones scan available surrounding cell sites approximately once every seven seconds, or more often as the signal level changes.[56] This process occurs automatically without any action by the user,[57] suggesting users are often unaware that their cell phones are tracking their locations.[58]

Cell site data triangulates a user's movements and location with extraordinary precision.[59] Federal Communications Commission (FCC) regulations require all cellular service providers to identify users' locations within 492 feet for 95% of calls placed, and within 164 feet for 67% of calls placed.[60] By way of reference, the average city block in Manhattan is between 750 and 920 feet long.[61] Cell site data, then, is often capable of tracking a user's location to the specific block the user is on. However, cell site data is often even more accurate—FCC

---

[50] *See Frequently Asked Questions, What Is Location-Aware Browsing?*, MOZILLA, www.mozilla.org/en-US/firefox/geolocation/ (last visited Apr. 14, 2013); *How To Use Chrome, Location Sharing*, GOOGLE, https://support.google.com/chrome/bin/answer.py?hl=en&answer=142065&topic=14666&ctx=topic (last visited Apr. 14, 2013).

[51] Lowenthal, *supra* note 40; *see also Skyhook Location and Performance*, SKYHOOK, www.skyhookwireless.com/location-technology/performance.php.

[52] *Definition of Mobile Positioning*, PC MAG ENCYCLOPEDIA, www.pcmag.com/encyclopedia_term/0,2542,t=mobile+positioning&i=47145,00.asp (last visited Apr. 14, 2013).

[53] *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005).

[54] *Id.*

[55] *Id.* at 751.

[56] *Id.* at 750.

[57] *Id.* at 751.

[58] *Id.* at 754.

[59] *Id.* at 751.

[60] *Id.* at 755.

[61] Michael Pollak, *Knowing the Distance*, N.Y. TIMES, Sept. 17, 2006, *available at* www.nytimes.com/2006/09/17/nyregion/thecity/17fyi.html?_r=0.

regulations represent the "floor" of accuracy, that is, the minimum requirement.[62] Marketplace competition and service complications in densely populated cities incentivize many mobile service providers to divide cell sites into increasingly smaller areas.[63] Although employed to improve service coverage, these smaller cell sites have the ancillary effect of improving geolocational information, because there are more data points from which to triangulate a user's location.[64] In urban areas, many service providers go even further, using "microcell" technology, where each cell has a range of just forty feet.[65] In areas where microcell technology is utilized, the location of a user can be identified with great specificity—often to the building, floor of a building, or even a particular room.[66]

Because cellular phones rescan available networks every few seconds, or every time the signal changes, cell site data is capable of tracking not only a user's location with great accuracy, but also his or her movements.[67] This, again, is particularly true in urban areas where the base location changes with rapid frequency as users move between microcells, which cover very small areas.[68]

Modernly, many mobile devices, particularly smart phones, are equipped with GPS chips.[69] A mobile GPS chip is capable of tracing a user's location with even more precision than cell sites—often within ten meters.[70] Because GPS functions properly only while the device is outdoors, most mobile companies use a combination of cell site and GPS data for their devices.[71] Despite the differences in technology, cell sites and GPS achieve the same result—they both pinpoint a user's location—and are used interchangeably for purposes of determining a user's location.[72]

---

[62] *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 832 (S.D. Tex. 2010).

[63] *Id.*

[64] *Id.* at 833.

[65] *Id.*

[66] *Id.*

[67] *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 756 (S.D. Tex. 2005).

[68] *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. at 833.

[69] *Id.* at 831-32; STEINFIELD, *supra* note 14, at 3-4.

[70] *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 832; STEINFIELD, *supra* note 14, at 3-4.

[71] *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 831-32; STEINFIELD, *supra* note 14, at 3-7.

[72] *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 831-32; STEINFIELD, *supra* note 14, at 3-7.

Web service providers have capitalized on mobile positioning technology in a number of ways. Mobile location-based services are explosively popular, with new services being offered every day.[73] Location-based services have become a staple in mobile applications focused on transportation;[74] daily deal offerings;[75] goods, services, and entertainment;[76] social networking;[77] dating;[78] and even politics.[79]

Trends in social networking demonstrate how phenomenally popular location-based services are in the mobile market. While many mobile applications utilize location services for pragmatic purposes, such as getting directions or finding a nearby restaurant, a number of social networking applications are based solely on sharing one's location—

---

[73] *See Location Apps Research*, SKYHOOK, www.skyhookwireless.com/locationapps/ (last visited Apr. 24, 2013); *see also Mobile Life: Which Feature and Apps Hold the Strongest Appeal Around the World?*, *supra* note 4; Tynan, *supra* note 3.

[74] *E.g.*, GOOGLE MAPS MOBILE APPLICATION, www.google.com/mobile/maps/ (last visited Apr. 14, 2013) (mobile map service with real-time navigation); TAXI MAGIC MOBILE APPLICATION, www.taximagic.com/en_US (last visited Apr. 14, 2013) (mobile taxicab booking service); LYFT, www.lyft.me/ (last visited Apr. 14, 2013) (mobile ride-sharing service); ZIPCAR MOBILE APPLICATION, www.zipcar.com/iphone (last visited Apr. 14, 2013) (mobile car rental service); HOPSTOP MOBILE APPLICATION, itunes.apple.com/us/app/id303217144?mt=8 (last visited Apr. 14, 2013) (mobile public transportation router); TAKE ME TO MY CAR, www.takemetomycar.anresgroup.com/ (last visited Apr. 14, 2013) (mobile application allows users to save the location of their car and retrieve directions to their parking spot later); PARKMOBILE, us.parkmobile.com/members/why-park-mobile/ (last visited Apr. 14, 2013) (mobile application finds nearby parking spots).

[75] *E.g.*, GROUPON MOBILE APPLICATION, www.groupon.com/mobile (last visited Apr. 14, 2013) (daily deal service); LIVING SOCIAL MOBILE APPLICATION, www.livingsocial.com/mobile (last visited Apr. 14, 2013) (daily deal service); BINGGO, www.binggodeals.com/ (last visited Apr. 14, 2013) (local daily deal aggregator that shows all deals close to a user).

[76] *E.g.*, AROUNDME, www.aroundmeapp.com (last visited Apr. 14, 2013); YELP! MOBILE APPLICATION, www.yelp.com/yelpmobile (last visited Apr. 14, 2013); FOURSQUARE, www.foursquare.com (last visited Apr. 14, 2013).

[77] *E.g.*, FACEBOOK MOBILE APPLICATION, play.google.com/store/apps/details?id=com.facebook.katana&hl=en (last visited Apr. 14, 2013); FACEBOOK HOME, www.facebook.com/home#home (last visited Apr. 14, 2013) (Facebook's mobile applications allow users to "check in" at their current locations, and notifies users when they are close to their friends); INSTAGRAM MOBILE APPLICATION, play.google.com/store/apps/details?id=com.instagram.android (last visited Apr. 14, 2013) (mobile photo-sharing application allows users to tag their current location).

[78] *E.g.*, MEET MOI, www.meetmoi.com (last visited Apr. 14, 2013) (mobile application finds and automatically introduces users who are near each other and share common interests); OK CUPID MOBILE APPLICATION, www.okcupid.com/mobile-apps (last visited Apr. 14, 2013) (popular dating site allows mobile users to browse people in their immediate vicinity); SINGLES AROUND ME, www.singlesaroundme.com (last visited Apr. 14, 2013); HOW ABOUT WE MOBILE APPLICATION, www.howaboutwe.com/mobile-about (last visited Apr. 14, 2013) (allows users to post suggested dates at nearby venues).

[79] *See* Lauren Johnson, *Geolocation Will Be Game-Changer for the 2012 Political Elections*, MOBILE MARKETER (July 6, 2012), www.mobilemarketer.com/cms/news/advertising/13249.html (explaining how President Barack Obama and Mitt Romney utilized location data for targeted advertising and campaign information).

location for location's sake.[80] This trend has become so popular that it now has its own secondary market. For instance, Facebook, like most popular social networking sites, has long had a feature that allows users to share their locations with their friends.[81] Emerging secondary mobile applications take this one step further, tracking users' real-time locations and sharing them with all of their social networks, notifying users when their friends[82] or professional acquaintances[83] are nearby. Other services allow users to set up notifications and gather information based on their own or others' locations.[84] As geolocational technologies advance in accuracy, location-based web services are quick to adapt, offering services that are increasingly location-specific.[85]

One thing is clear from examining the mobile market: location-based services are redefining the technology marketplace and are shaping users' everyday lives. These services will undoubtedly continue to expand in number and scope as technology advances, for both desktop and mobile web services.

---

[80] *E.g.*, FOURSQUARE, www.foursquare.com (last visited Apr. 14, 2013); GLYMPSE, www.glympse.com (last visited Apr. 14, 2013).

[81] *Share Where You Are*, FACEBOOK, www.facebook.com/about/location (last visited Apr. 24, 2013).

[82] *See, e.g.*, HIGHLIGHT, www.highlig.ht (last visited Apr. 24, 2013) (mobile application that indicates when members of users' social networks are nearby).

[83] *See, e.g.*, UNSOCIAL, www.unsocial.mobi (last visited Apr. 24, 2013) (mobile application that indicates when connections in users' professional networks are nearby).

[84] *See Location-Based Services: Are They There Yet?*, COMPUTER WORLD (May 3, 2012, 6:00 AM), www.computerworld.com/s/article/9226785/Location_based_services_Are_they_there_yet_? (discussing up-and-coming location-based mobile applications such as Neer, which allows users to set up geolocational-specific notifications for themselves and their loved ones, such as a notification that their spouse is leaving work, or a reminder that they need milk when they enter the grocery store); Anneke Jong, *How To Stalk Your Friends Online (It's Not Creepy Anymore!)*, THE DAILY MUSE (Dec. 14, 2012), www.thedailymuse.com/tech/how-to-stalk-your-friends-online-its-not-creepy-anymore/# (explaining mobile applications such as Glympse, which allow users to share their real-time movements with friends).

[85] *See* Brian Honigman, *How Location-Based Social Networks Are Changing the Game for Businesses*, ENTREPRENEUR (Jan. 9, 2013), www.entrepreneur.com/blog/225436 (describing trending indoor location-based services, which interact with users based on their location *inside* a particular venue, such as offering a deal on a shirt they are looking at in a department store); *see also Location Based Services*, CNET, news.cnet.com/8300-5_3-0.html?keyword=location+based+services (last visited Apr. 14, 2013) (articles discussing emerging location-based services, such as Adobe's plan for a location-linked mobile application that will prompt users to download relevant mobile applications, for instance when they enter a museum or check in to a hotel).

III. HOW THE LAW APPLIES TO GEOLOCATIONAL DATA

A. ECPA

Nearly all modern Internet activities, both desktop and mobile, come within ECPA's sweeping definition of "electronic communications": "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."[86] ECPA governs the disclosure of users' communications as well as the data that accompanies those communications.[87]

ECPA classifies communications based on the status of their transmission, and it treats searches of communications differently based on that status.[88] Communications intercepted during transmission are subject to stringent warrant requirements under the Wiretap Act.[89] Communications accessed from storage, however, are subject to more relaxed standards under the Stored Communications Act (SCA).[90]

The SCA defines "storage" 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."[91] Today, most electronic communications fall within this broad definition of "stored" because they are routed through and stored on third-party servers as part of their transmission.[92]

Popular communication media[93] such as web-based email and social networking sites store content their users send through their services, as

---

[86] 18 U.S.C.A. § 2510(12) (Westlaw 2013).

[87] *Id.*

[88] *Compare* 18 U.S.C.A. § 2511 (Westlaw 2013), *with* 18 U.S.C.A. §§ 2702, 2703 (Westlaw 2013); *see also* Kerr, *supra* note 5, at 1231-33.

[89] 18 U.S.C.A. § 2511 (Westlaw 2013).

[90] 18 U.S.C.A. § 2510 (Westlaw 2013).

[91] 18 U.S.C.A. § 2510(17) (Westlaw 2013).

[92] Kerr, *supra* note 5, at 1209-10.

[93] *See Nielsen Tops of 2012: Digital*, NIELSEN (Dec. 20, 2012), www.nielsen.com/us/en/newswire/2012/nielsen-tops-of-2012-digital.html (indicating that Facebook is the second most popular application for iPhones, with 28 million unique users monthly); *see also* Chloe Albanesius, *How Many U.S. Users Does Facebook Have, Will It Affect an IPO?*, P.C. MAG (June 14, 2011), *available at* www.pcmag.com/article2/0,2817,2386896,00.asp (150 million estimated American Facebook users in 2011); *Most Popular Email Clients*, DIGITAL INSPIRATION (Aug. 6, 2009), www.labnol.org/Internet/email/most-popular-email-clients/9340/ (indicating that, in 2009, over 40% of email users access their email from a web-based service).

well as data about that activity.[94] For example, when an email is sent through Gmail—Google's email service—it is stored on Google's servers.[95] Similarly, when a Facebook or Twitter user posts content on his or her personal page or sends a private message to another user, that content is routed through and stored on the respective websites' servers.[96] In addition to users' actual communications, websites log and store a host of data about each communication, including the IP address associated with each communication.[97] Like the communications themselves, this data is kept on the service providers' servers, making the data "stored" for purposes of the SCA.[98]

Similar to web service providers, digital and mobile phone service providers log data about their users' activity, including cell site and GPS data associated with users' devices.[99] There is, however, some variance in the amount of data retained by mobile service providers. Some service providers keep comprehensive cell site records that detail a user's location even when the phone is idle,[100] while others keep cell site records based on only a user's call and text messaging activity.[101] Based on surveys of mobile phone use in 2010, it is estimated that mobile location data covering even just the call and text messaging activity of an average user would reveal between twenty and fifty-five location points per day.[102] Mobile service providers collect this data both to comply with FCC regulations and to improve their services.[103] For the same

---

[94] Kerr, *supra* note 5, at 1209-10.

[95] *What Happens to My Messages Stored on Gmail's Servers?*, GOOGLE, https://support.google.com/mail/answer/13288?hl=en (last visited Apr. 24, 2013).

[96] *Information We Receive About You*, FACEBOOK, www.facebook.com/about/privacy/your-info (last visited Apr. 24, 2013); *see also* Steve Campbell, *How Does Facebook Work? The Nuts and Bolts [Technology Explained]*, MAKE USE OF (Feb. 27, 2010), www.makeuseof.com/tag/facebook-work-nuts-bolts-technology-explained/ (explaining Facebook's storage system); *Information Collection and Use*, TWITTER, www.twitter.com/privacy (last visited Apr. 24, 2013); *see also How Twitter Stores 250 Million Tweets a Day Using MySQL*, HIGH SCALABILITY (Dec. 19, 2011, 9:05 AM), highscalability.com/blog/2011/12/19/how-twitter-stores-250-million-tweets-a-day-using-my sql.html (explaining Twitter's storage system).

[97] *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 119 (E.D. Va. 2011); *see also* Kerr, *supra* note 5, at 1219-20.

[98] Kerr, *supra* note 5, at 1227-28.

[99] U.S. DEP'T OF JUSTICE, RETENTION PERIODS OF MAJOR CELLULAR SERVICE PROVIDERS (2010), *available at* www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf.

[100] *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 833-34 (S.D. Tex. 2010).

[101] *Id.*

[102] *Id.* at 835.

[103] *Id.* at 833-34.

reasons as IP addresses, mobile activity and associated data are likewise considered "stored" by the SCA's definition.[104]

In addition to the status of a communication as "stored," the distinction between "content" and "non-content" has a substantial effect on the way communications data may be obtained by the government.[105] By the SCA's standards, when the "content" of a communication is sought, a search warrant is required in most cases.[106] However, when "non-content" records of stored communications or subscriber information are sought, they can be obtained directly from the third party that stores the individual's information, such as a website, ISP, or mobile service provider, through a court order.[107] ECPA provides little guidance in its definition of "content": "any information concerning the substance, purport, or meaning of [a] communication."[108] ECPA does, however, list a number of non-content records: "telephone or instrument number[s] or other subscriber number[s] or identit[ies], including any temporarily assigned network address[es]."[109]

Geolocational data's status as "stored" and the data's status as "non-content" both create questions of which standard applies when the government seeks to compel disclosure of user data from web service providers.[110] While the Fourth Amendment requires probable cause for issuance of a search warrant,[111] the SCA's standard for the issuance of a court order is much lower: "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."[112] To determine whether a warrant is required or a search can be conducted with a court order under the SCA's less stringent "reasonableness" standard, courts often look to traditional Fourth Amendment principles.[113]

---

[104] United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *7 n.6 (S.D. Fla. July 30, 2012).

[105] Kerr, *supra* note 5.

[106] 18 U.S.C.A. § 2703(a) (Westlaw 2013).

[107] 18 U.S.C.A. § 2703(c)(2), (d) (Westlaw 2013).

[108] 18 U.S.C.A. § 2510(8) (Westlaw 2013).

[109] 18 U.S.C.A. § 2703(c)(2)(E) (Westlaw 2013).

[110] *See generally* Kerr, *supra* note 5.

[111] U.S. CONST. amend. IV.

[112] 18 U.S.C.A. § 2703(d) (Westlaw 2013).

[113] *See generally* Kerr, *supra* note 5.

B. THE FOURTH AMENDMENT

Courts consistently analogize searches of electronic communications to searches of traditional communications in determining whether the communications at issue (and the data associated with those communications) are entitled to Fourth Amendment protection. It is well established that the Fourth Amendment protects individuals against the unreasonable search and seizure of their "persons, houses, papers, and effects"[114] and allows a search warrant to issue only on a showing of probable cause.[115] Two exceptions to the Fourth Amendment are relevant here: the third-party doctrine, and the question of whether any protectable "content" of a communication is sought. Courts have drawn a distinction between searches of communications and searches of routing information *about* a communication on both of these bases.[116]

1. *The Third-Party Doctrine, Historically*

The Fourth Amendment extends only to searches where an individual has "exhibited an actual (subjective) expectation of privacy,"[117] and that expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[118] Courts have long held that individuals relinquish any reasonable expectation of privacy in information they knowingly reveal to third parties.[119]

When analyzing searches of geolocational data, courts often make analogy to the routing and addressing information associated with traditional communications. The Supreme Court has held that individuals possess no reasonable expectation of privacy in addressing information on the outside of a piece of postal mail because this routing information must be disclosed to employees of the United States Postal Office to ensure the mail is delivered from one place to another.[120]

The Court came to a similar conclusion regarding telephonic communications in *Smith v. Maryland*, in which a pen register—a device that records the telephone numbers dialed from a phone—was installed

---

[114] U.S. CONST. amend. IV.

[115] *Id.*; Minnesota v. Carter, 525 U.S. 83, 88 (1998); Katz v. United States, 389 U.S. 347, 365 (1967).

[116] *See generally* Kerr, *supra* note 5.

[117] *Katz*, 389 U.S. at 361.

[118] *Id.*

[119] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[120] *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

on the defendant's phone at the behest of law enforcement.[121] The Court found that the defendant had no reasonable expectation of privacy in the phone numbers he had dialed for two reasons.[122] First, the phone numbers were fully revealed to a third party—the phone company—and, second, the phone numbers were part of business records legitimately kept by the phone company for purposes of billing and call completion.[123]

The Court employed this business-records exception again in *United States v. Miller*, in which it found that the defendant had no reasonable expectation of privacy in his banking records, which were disclosed to the bank during the transaction process.[124] The Court held that, because the defendant had fully conveyed the details of his financial transactions to the bank, the records of those transactions were not his "private papers" for purposes of the Fourth Amendment, but rather business records belonging to the bank, such that the search of those records did not violate the defendant's Fourth Amendment rights.[125]

2. *The Issue of "Content," Historically*

Fourth Amendment jurisprudence, like ECPA, offers less protection to "non-content" or "records" of a communication than the actual "content" of a communication, on the basis that no "search" occurs when the government seeks non-content.[126] The Supreme Court addressed the question of content in *Smith*, holding that the installation of the pen register did not constitute a "search," because the defendant's actual conversations were not surveyed, and the information garnered by the pen register was not part of the content of the communication.[127]

In addressing the question of content, the *Smith* Court revisited *Katz v. United States*,[128] in which the defendant had his portion of conversations recorded by an eavesdropping device attached to a public phone booth.[129] The defendant moved to suppress this evidence on the

---

[121] *Smith*, 442 U.S. at 737.

[122] *Id.* at 744.

[123] *Id.*

[124] United States v. Miller, 425 U.S. 435, 442 (1976).

[125] *Id.* at 440.

[126] *In re* Application of U.S. for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 818 (S.D. Tex. 2006) (citing Katz v. United States, 389 U.S. 347, 353-54 (1967)).

[127] Smith v. Maryland, 442 U.S. 735, 741-42 (1979).

[128] *Id.* at 739.

[129] *Katz*, 389 U.S. at 348.

basis that it was obtained through an illegal search.[130] The Court found that the search was indeed illegal, stating famously that the Fourth Amendment "protects people, not places," and that the defendant's end of the conversations were entitled to protection as content.[131] *Katz* marked a significant shift in Fourth Amendment jurisprudence, which had previously recognized privacy rights only with respect to searches that physically invaded private spaces.[132]

In *Smith*, however, the Court distinguished *Katz* on the basis that Smith's conversations were not actually overheard—the pen register had only recorded the numbers dialed from his phone.[133] The Court found that this did not amount to "content" of a communication:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.[134]

For the *Smith* Court, then, the data accompanying the defendant's phone calls was not "content," and thus not protected under the Fourth Amendment.[135]

3. *The Third-Party Doctrine, Modernly*

a. IP Addresses

Federal courts have unanimously interpreted the third-party doctrine established in *Smith* and *Miller* to apply to IP addresses and have held that Internet users have no reasonable expectation of privacy in their IP addresses because they are voluntarily conveyed to third parties—the users' ISPs and web service providers.[136] To this end, courts have held

---

[130] *Id*.

[131] *Id*. at 351.

[132] *Id*. at 352-53.

[133] *Smith*, 442 U.S. at 741.

[134] *Id*. at 741 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

[135] *Id*. at 741-42.

[136] *E.g.*, United States v. Bynum, 604 F.3d 161, 164 & n.2 (4th Cir. 2010); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); United States v. Forrester, 512 F.3d 500, 509-10 (9th Cir. 2008); *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 138 (E.D. Va. 2011).

that the information can be compelled by the government under the less stringent "reasonableness" standard in the SCA.[137]

New Jersey, however, has recognized the importance of protecting users' IP addresses, finding a reasonable expectation of privacy in this data under its state constitution.[138] Historically, New Jersey has avidly protected individual privacy and, although the language in its constitution parallels that of the Fourth Amendment,[139] New Jersey courts have consistently recognized stronger privacy protections than their federal counterparts.[140] New Jersey has recognized a reasonable expectation of privacy in both banking records and phone numbers dialed.[141] On these bases, New Jersey courts have held that Internet users do not relinquish a reasonable expectation of privacy in revealing their IP addresses to third parties.[142]

b. Mobile Positioning Data

The question of whether mobile positioning data is subject to the third-party doctrine is exceedingly more complex.[143] Generally, prospective positioning data (i.e., data that traces a user's movements and location in real-time) cannot be compelled without a warrant.[144] Historical positioning data, however, has seen less uniform treatment in federal courts.[145]

Some courts have aptly held that historical mobile positioning data is not "voluntarily conveyed" by an individual to his or her service provider because it is automatically collected without any action by the

---

[137] *See, e.g.*, *Bynum*, 604 F.3d at 164 & n.2; *Perrine*, 518 F.3d at 1204; *Forrester*, 512 F.3d at 509-10 (9th Cir. 2008); *In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d at 138.

[138] State v. Reid, 945 A.2d 26, 28 (N.J. 2008).

[139] N.J. CONST. art. I, ¶ 7 ("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 warrant shall issue except upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the papers and things to be seized.").

[140] *Reid*, 945 A.2d at 32.

[141] *Id*. at 28; State v. Hunt, 450 A.2d 952, 957 (N.J. 1982).

[142] *Reid*, 945 A.2d at 31-32.

[143] *See* United States v. Jones, No. 05-0386 (ESH), 2012 WL 6443136, at *1 (D.D.C. Dec. 14, 2012) (calling the search of defendant's mobile geolocational data a "vexing question of Fourth Amendment jurisprudence").

[144] *Id*. at *3 & n.5.

[145] *Id*. at *5 & n.9.

user.[146] These courts have noted that most users are probably unaware that this data is even logged by their service providers:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."[147]

For this reason, a number of courts that have addressed the issue have declined to apply the third-party doctrine to mobile geolocational data.[148]

But a number of federal courts have come to the opposite conclusion, strictly applying the third-party doctrine established in *Smith* and *Miller* to historical mobile positioning data, and finding no reasonable expectation of privacy in the data.[149] These courts have declined to apply the Fourth Amendment to the data, and have allowed searches under the SCA's "reasonableness" standard.[150]

3. *The Issue of "Content," Modernly*

Courts still rely on *Smith*'s definition of "content" when examining searches of both traditional and electronic communications, generally finding that IP addresses and mobile geolocational data are "non-content

---

[146] *E.g.*, *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 756 (S.D. Tex. 2005).

[147] *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317-18 (3d Cir. 2010) (emphasis removed) (quoting Amici Electronic Frontier Foundation, American Civil Liberties Union, and ACLU of Texas' Brief in Opposition to the Government's Request for Review 21, *available at* www.aclutx.org/documents/01142011CellPhoneAmicus.pdf).

[148] *E.g.*, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317-18; *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 843; *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 756-57.

[149] *E.g.*, United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012); United States v. Graham, 846 F. Supp. 2d 384, 398-400 (D. Md. 2012); United States v. Dye, No. 1:10CR221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011).

[150] *E.g.*, *Madison*, 2012 WL 3095357, at *9; *Graham*, 846 F. Supp. at 398-400; *Dye*, 2011 WL 1595255, at *9.

records."[151] Courts analogize geolocational data to the phone numbers in *Smith*, finding that no substance of a communication is revealed by its routing information.[152] Further, both forms of data seem to fit squarely within ECPA's definition of "non-content records": "telephone or instrument number[s] or other subscriber number[s] or identity[ies], including any temporarily assigned network address[es]."[153] This has not yet been challenged or addressed by the courts.

IV. WHERE ARE WE?

Despite the similarity of the two types of data, IP addresses have been afforded much less protection than mobile positioning data. Both IP addresses and mobile positioning data reveal the same information about users—their locations.[154] And while mobile positioning data is more accurate for this purpose, IP addresses are not far behind and may soon equal the geolocational accuracy of mobile positioning.[155] Both types of data are revealed to third-party service providers in the same way—during the transmission of a communication.[156] Neither type of data is actively revealed by users to their service providers.[157] IP addresses and mobile positioning data reveal the same information about their users, are collected in the same manner, and should be protected equally.

The *Smith* Court, in finding that the defendant's call logs were subject to the third-party doctrine, emphasized that the defendant had *knowingly* conveyed the telephone numbers he dialed to the phone company: "Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[158] That is, telephone subscribers know that the numbers they dial are conveyed to the telephone company—presumably because they receive a detailed call log on their monthly invoice—and consequently

---

[151] *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008); *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 139 (E.D. Va. 2011).

[152] *See, e.g.*, *Forrester*, 512 F.3d at 510; *In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d at 139.

[153] 18 U.S.C.A. § 2703(c)(2)(E) (Westlaw 2013).

[154] *See* discussion *supra* Part II.

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] Smith v. Maryland, 442 U.S. 735, 743 (1979).

lack a subjective expectation of privacy in the information.[159] Internet users, by contrast, do not receive any type of notice that data is logged by a web service, a mobile carrier, or an ISP. For these reasons, users do not "'voluntarily' share [this data] . . . in any meaningful way,"[160] and the *Smith* decision should not control the disclosure of this data.

Applying the third-party doctrine to geolocational data also fails to recognize the intrusive nature of this data in comparison with previous technologies. By its very nature, the information conveyed by IP addresses and mobile positioning data is much richer than the addressing information on an envelope or call logs from an analog telephone. A postal envelope reveals only the location from which a communication was initiated and whom the communicator intended to reach. Indeed, aside from the postmark, a postal envelope may be completely anonymous if the sender declines to include a return address and name on the envelope. An outgoing call log reveals only that an individual was at a specific location at a particular time, and that he or she attempted to communicate with a specific phone number. IP addresses and mobile positioning data, however, reveal much more—a user's precise location or locational movements over a period of time.[161]

Further, applying the third-party doctrine to this data conflates two very different uses of the data. Generally, users may be willing to share information with their service providers for "civil purposes"—marketing and increasing user experience—but it does not follow that, in doing so, users also relinquish their privacy to government searches of this data. In *Smith*, Justice Marshall (joined by Justice Brennan) dissented to recognize this crucial distinction, noting that the argument that "individuals who convey information to third parties have 'assumed the risk' of disclosure to the government" is flawed:[162] "Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[163] Geolocational data is collected by web service providers for marketing purposes and to improve user experience on the

---

[159] *Id.*

[160] *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (quoting Amici Electronic Frontier Foundation, American Civil Liberties Union, and ACLU of Texas' Brief in Opposition to the Government's Request for Review 21, *available at* www.aclutx.org/documents/01142011CellPhone Amicus.pdf).

[161] *See* discussion *supra* Part II.

[162] *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

[163] *Id.*

website.[164] This is a quid pro quo arrangement—users agree to share some personal information with the website, and, in exchange, they are allowed to use the service free of charge, or they receive additional features or services from the website.[165]

As Justice Marshall noted, that a user discloses information to a service provider in the process of completing a communication does not mean that the user should assume that this information may be shared with others.[166] It defies both logic and common sense to argue that Internet users, who share personal information with trusted websites in exchange for free or improved services should assume that this information may be shared with the government in connection with a criminal investigation against them. Justice Sotomayor decried this non-sequitur in her concurring opinion in *United States v. Jones*: "I 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."[167]

Further, Internet users lack meaningful choice in disclosing their IP addresses and mobile positioning data. Justices Marshall and Brennan also pointed to this in their *Smith* dissent, noting that the holding presented an unacceptable ultimatum: individuals must either sacrifice their privacy or forgo use of the telephone altogether.[168] This did not present individuals with any sort of meaningful choice, because, for many Americans, the telephone is a "personal or professional necessity."[169]

The Internet is no exception here, with statistics indicating that 74% of Americans use web services.[170] Online research, marketing, and

---

[164] *See* discussion *supra* Part II; *see also, e.g.*, *Privacy Policy*, GOOGLE, www.google.com/intl/en/policies/privacy/ (last modified July 27, 2012) ("We collect information to provide better services to all of our users . . . ."); *Information We Receive and How It Is Used*, FACEBOOK, www.facebook.com/about/privacy/your-info#howweuse (last visited Apr. 24, 2013) ("[This information] not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.").

[165] *See, e.g.*, *Privacy Policy*, GOOGLE, www.google.com/intl/en/policies/privacy/ (last modified July 27, 2012) ("We collect information to provide better services to all of our users . . . ."); *Information We Receive and How It Is Used*, FACEBOOK, www.facebook.com/about/privacy/your-info#howweuse (last visited Apr. 24, 2013) ("[This information] not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.").

[166] *Smith*, 442 U.S. at 749 (1979) (Marshall, J., dissenting).

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

[168] *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

[169] *Id*. at 750.

[170] Int'l Telecomms. Union, *Global ICT Developments*, www.itu.int/ITU-D/ict/statistics/ (last visited Apr. 26, 2013).

communications are now commonplace, if not mandatory, in nearly every profession. Email and social networking play key roles in Americans' personal lives and communications.[171] Surveys have indicated that, on average, Americans spend more than twelve hours per week online.[172] For many, online communications have all but replaced traditional modes of communication, becoming the primary method of interaction among personal and professional acquaintances. Like the telephone before it, electronic communication has undoubtedly become a "personal [and] professional necessity."[173] It is untenable to require that Americans forgo use of the Internet to protect their privacy. Just as with traditional methods of communication, the "choice" to either use or refrain from using the Internet represents no choice at all. As Justice Sotomayor sharply observed:

> Perhaps . . . some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable" . . . . But whatever the societal expectations, [individuals] can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.[174]

Finally, the question of "content" is becoming increasingly complex. The data and routing information collected from an Internet user differs in spades from telephone user data. Emerging web service trends like location-sharing indicate that users make myriad communications that convey nothing more than their current location. In this context, the content of the communication arguably *is* the geolocational data. With ever-evolving technologies shaping trends in the communications industry, the lines between user data and the content of a communication can be, and often are, blurred. Courts should recognize this distinction when it arises, and ECPA should be amended to clarify its definition of "non-content records" to recognize that IP addresses may sometimes comprise the "content" of a communication.

---

[171] *See* Jessica E. Vascellaro, *Why Email No Longer Rules. . .*, WALL ST. J., Oct. 12, 2009, *available at* online.wsj.com/article/SB10001424052970203803904574431151489408372.html?mod=wsj_share_facebook.

[172] Lauren Indvik, *Americans Now Spend As Much Time Using Internet as TV*, MASHABLE (Dec. 13, 2010), www.mashable.com/2010/12/13/Internet-tv-forrester/.

[173] *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

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

V. PRIVACY POLICIES AND TERMS OF SERVICE DEMONSTRATE TECHNOLOGY PROVIDERS' FRUSTRATION

When a user subscribes to or visits a website or other online service, he or she agrees to the website's privacy policy and terms of service.[175] These policies explain how a website may use data collected about a user, and how that information may be disclosed to others.[176] Most websites indicate in their terms of service that a user's information may be used for purposes of marketing the website itself or may be shared with third-party advertisers.[177] These agreements also often include vague, blanket disclaimers that any and all information gathered by the website may be shared with law enforcement. Typical disclaimers state that information may be shared when "reasonably necessary to comply with a law, regulation or legal request,"[178] or when the website has a "good faith belief that the law requires [them] to do so."[179]

Web service providers have joined privacy scholars in the goal of clarifying and updating ECPA.[180] Service providers want legislative clarification of these standards so that they may increase users' trust in their services and develop proper procedures to deal with government demands for subscriber information.[181] The eagerness of service providers to clarify these standards illustrates that any ambiguity in their policies is a result of ambiguity in the legislation itself.

---

[175] *See* 2 IAN C. BALLON, E-COMMERCE AND INTERNET LAW § 21.03[4] (2012). The question of whether Internet consumers are bound to a website's terms of service and privacy policy by merely using that website, and the attendant question of whether such contracts are conscionable are hotly debated, but beyond the scope of this Comment.

[176] *See, e.g.*, *Privacy Policy*, GOOGLE, www.google.com/intl/en/policies/privacy (last modified July 27, 2012); *Information We Receive About You*, FACEBOOK, www.facebook.com/about/privacy/your-info#howweuse (last visited Apr. 24, 2013).

[177] *See, e.g.*, *Privacy Policy*, GOOGLE, www.google.com/intl/en/policies/privacy (last modified July 27, 2012); *Information We Receive About You*, FACEBOOK, www.facebook.com/about/privacy/your-info#howweuse (last visited Apr. 24, 2013).

[178] *Privacy Policy*, TWITTER, twitter.com/privacy (last visited Apr. 24, 2013).

[179] *Data Use Policy*, FACEBOOK, www.facebook.com/about/privacy/other (last visited Apr. 24, 2013).

[180] *Who We Are*, DIGITAL DUE PROCESS, www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited May 10, 2013) (listing members of the coalition including Apple, Google, Amazon, and Microsoft).

[181] *About the Issue*, DIGITAL DUE PROCESS, www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited May 10, 2013).

CONCLUSION: ECPA HELP US ALL

Courts are understandably loath to delve into these complicated issues.[182] These technologies are complex and ever-evolving, with every advancement in technology creating a new landscape for courts to navigate. Federal courts are divided and admittedly confused on these issues.[183] Last year, Justice Sotomayor acknowledged this very real difficulty and the attendant detriment to society while we wait to figure it out:

> [F]undamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[184]

Proposed legislation has sought one step toward increasing individual privacy by affirmatively protecting user geolocational records derived from mobile positioning technologies.[185] However, despite the similarities in the technologies and privacy concerns, the proposed amendments fail to recognize a privacy interest in IP addresses, leaving the courts to continue to struggle to understand these technologies and the ongoing invasion to individuals' privacy. ECPA should be amended to recognize an equal and adequate privacy interest in all geolocational data, regardless of its underlying technology.

---

[182] United States v. Jones, No. 05-0386 (ESH), 2012 WL 6443136, at *1 (D.D.C. Dec. 14, 2012) (calling the search of defendant's mobile geolocational data a "vexing question of Fourth Amendment jurisprudence").

[183] *Id.* at *3.

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

[185] Location Privacy Protection Act of 2012, S. 1223, 112th Cong. § 3 (died); GPS Act, H.R. 1312, 113th Cong. (2013) (referred to Committee); Online Communications and Geolocation Privacy Act, H.R. 983, 113th Cong. (2013) (referred to Committee); Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. §§ 3, 6 (died; reintroduced as Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (reported by Committee, Apr. 25, 2013), which excludes any amendments related to geolocational protections).