Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 22 *Volume XXII*
Number 1 *Volume XXII Book 1*

Article 12

2011

Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy

Christian Levis
Fordham University School of Law, clevis1@law.fordham.edu

Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy

Cover Page Footnote
J.D. Candidate, Fordham University School of Law, 2012. Thank you to Professor Sylvain for his guidance and insight. Thank you also to my friends and family for their support.

Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy

Christian Levis*

* J.D. Candidate, Fordham University School of Law, 2012. Thank you to Professor Sylvain for his guidance and insight. Thank you also to my friends and family for their support.

INTRODUCTION

If you happen to use one of the 200 million[1] iPhone, iPad, and iPod touch devices on the planet, Apple knows where you are. Tucked away in a file[2] on every user's device is a regularly updated list of location-based information.[3] Apple claims that it uses that information to improve the response time of software that requires a user's location.[4] But that sensitive information is not kept secret.[5] The list of a user's locations is stored in an unprotected, unencrypted file, open to every application on a user's iOS[6] device.[7]

Apple has since updated its software to reduce the amount of location-based information it stores and to give users more control over how their information is used.[8] While that change is

---

1 *See* Graham Spencer, *Over 200 Million iOS Devices Sold, 25 Million iPads and $2.5 Billion Paid to Developers*, MACSTORIES, http://www.macstories.net/news/over-200-million-ios-devices-sold-25-million-ipads-and-2-5-billion-paid-to-developers/ (last visited Sept. 8, 2011).

2 The file, called consolidated.db, was discovered by two hackers in the Spring of 2011. *See* Nick Bilton, *3G Apple iOS Devices Are Storing Users' Location Data*, N.Y. TIMES (Apr. 20, 2011, 3:04 PM), http://bits.blogs.nytimes.com/2011/04/20/3g-apple-ios-devices-secretly-storing-users-location/ [hereinafter Bilton, *3G Devices*].

3 *See id. See also* Nick Bilton, *Apple Updates Software to Fix Problems With Collecting Location Data*, N.Y. TIMES (May 4, 2011, 3:42 PM), http://bits.blogs.nytimes.com/2011/05/04/apple-ios-software-release-fixes-location-bug/ [hereinafter Bilton, *Apple Updates Software*] (noting that a problem with Apple's mobile devices enabled them to collect customers' locations).

4 *See* Bilton, *Apple Updates Software*, *supra* note 3.

5 *See* Bilton, *3G Devices*, *supra* note 2.

6 iOS is Apple's mobile operating system which runs on the iPhone, iPad and iPod touch. *See iOS 4.3 Software Update*, APPLE, http://www.apple.com/ios/ (last visited Sept. 9, 2011).

7 *See* Bilton, *3G Devices*, *supra* note 2.

8 *See* Bilton, *Apple Updates Software*, *supra* note 3.

beneficial for Apple's users, it was a business decision.[9] Apple was not obligated to change its policy. It was not in violation of any law.[10]

Apple's location-storing episode highlights a gap that exists in current privacy law. The smartphone,[11] a cell phone with PC-like functionality, has made it possible for users to turn their current location into a practical tool.[12] Smartphone applications, called location-based mobile services (LBMS),[13] are designed to facilitate this new functionality. These applications, however, operate in a largely unregulated space. Courts that are forced to deal with mobile privacy issues are left with a statute that was drafted in 1986,[14] years before the Internet took off[15] and the smartphone was first introduced.[16] In many cases, actions that intuitively seem

---

[9] Apple's decision to change how iOS stores user information was part of a public relations campaign to appease users after it was discovered that users' locations were being stored. *See* AppleInsider Staff, *Apple Releases iOS 4.3.3 with Fixes for Location Database Controversy*, APPLEINSIDER (May 4, 2011, 1:25 PM), http://www.appleinsider.com/articles/11/05/04/apple_releases_ios_4_3_3_with_fixes_for_location_database_controversy.html. The proposed changes, along with answers to other questions, were provided in a press release shortly after the consolidated.db file was discovered. *See Apple Q&A On Location Data*, APPLE (Apr. 27, 2011), http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html; Bilton, *3G Devices*, *supra* note 2.

[10] *See* Karen Gullo, *Apple Sued Over User Location Data Storage on IPhones, IPads*, BLOOMBERG (Apr. 25, 2011, 1:52 PM), http://www.bloomberg.com/news/2011-04-25/apple-sued-over-user-location-data-storage-on-iphones-ipads.html.

[11] The smartphone as a class includes iPhones, Blackberries, and other Android OS-enabled devices. Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, 25 FCC Rcd. 11407, 11412 (2010).

There were approximately 78.2 million smartphone devices in the United States as of June 2011. *See 50 Wireless Quick Facts*, CTIA: THE WIRELESS ASS'N (June 2011), http://www.ctia.org/advocacy/research/index.cfm/AID/10378.

[12] This is not to imply that a message will be received or read by the entire Internet. Rather that a public message, like a tweet, is accessible by everyone with an Internet connection.

[13] *See* GSM Ass'n, *Permanent Reference Document SE.23: Location Based Services*, GSM WORLD, 11 (2003), http://www.gsmworld.com/documents/se23.pdf [hereinafter *Location Based Services*].

[14] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[15] For example, current privacy law would apply differently to a phone call transmitted digitally and one transmitted over copper wires. *See infra* Part III.B.

[16] The first smartphone was the IBM Simon, created in 1992. BUSINESS2COMMUNITY, *A Look Back in Time at the First Smartphone Ever*, BUSINESS2COMMUNITY.COM (June

wrong, like Apple's secret storing of a user's location, simply do not fall within the scope of existing privacy law. Furthermore, actions that do come within the language of existing regulations are resolved in ways that do not take into consideration the current state of technology or how it is used by the public.

This Note addresses the need to build a regulatory system that can correctly deal with location-based mobile information. Part I describes the current status of the technology industry and outlines what information software developers can currently access from a user's device. Part II examines the statute regulating this area, the Electronic Communications Privacy Act (ECPA), and points out some of the problems courts face when applying it to cases that deal with information privacy. Part III highlights where the application of this regime produces conflicting results. Lastly, Part IV examines changes to the ECPA that will bring it up to speed with modern uses of technology, and suggests why proposed legislation does not go far enough to make a substantial change.

I. WHAT THEY KNOW ABOUT YOU

LBMSs are third-party applications commonly known as apps. Smartphone users download these apps from the Internet and install them onto their devices.[17] The process is similar to downloading and installing software onto a computer. Once installed, the LBMS purportedly uses a person's current location to perform useful functions[18]—anything from providing directions to

27, 2011), http://www.business2community.com/mobile-apps/a-look-back-in-time-at-the-first-smartphone-ever-040906.

[17] Users can download applications either directly from a third-party's website or from a digital "app store," a specialized application or website that facilitates this type of content delivery. App stores are usually preinstalled by the phone manufacturer on a given device. The largest marketplace for these "apps" is the iTunes app store operated by Apple. *See Apple Introduces the New iPhone 3G*, APPLE (June 9, 2008), http://www.apple.com/pr/library/2008/06/09Apple-Introduces-the-New-iPhone-3G.html. At the time of the writing of this note there are over 300,000 apps available for download onto the iPhone alone. *See* Federico Viticci, *How Many iPhone Apps Are There? 306,554 – And 60,000 iPad Apps*, MACSTORIES.NET (Jan. 18, 2011), http://www.macstories.net/news/how-many-iphone-apps-are-there-306554-and-60000-ipad-apps/.

[18] *See Location Based Services*, *supra* note 13, at 11.

allowing users to share their location with friends. There are thousands of potential uses for a user's location.[19]

Just like any other piece of software, installing an LBMS requires that a user agree to certain conditions.[20] These conditions may be agreed to at the initial installation of the app or later on during its use.[21] The terms a user agrees to control not only the use of the app but also the application's use of the information stored on the device.[22] Once an LBMS makes its way on to a user's device it often has access to a wealth of information beyond what a user provides[23]—particularly with regard to location-based information.

A. Location-Based Information

One class of LBMS facilitates a user's choice to share his current location with others. How each application achieves this goal varies. For example, "check in" applications like foursquare[24] or Gowalla[25] encourage users to share their location with friends by "checking in" at a specific place.[26] This "check-in" often links

---

[19] For example, mobile apps may be used for social networking, booking a vacation, sharing photographs, or many other including ones that are constantly being developed. *See, e.g.*, Doug Gross, *New Wave of Location-Based Apps Mark a 'Paradigm Shift,'* CNN (June 29, 2011), http://articles.cnn.com/2011-07-29/tech/discovery.apps_1_android-free-app-hipstamatic?_s=PM:TECH.

[20] Computer software commonly prompts users upon installation to agree or disagree with certain conditions known as the End User License Agreement. *See, e.g.*, Specht v. Netscape Commc'ns Corp., 150 F. Supp. 2d 585, 587 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d Cir. 2002) (describing an End User License Agreement as "the contract allegedly made by the offeror of the software and the party effecting the download"). On the Android app marketplace, for example, users are prompted prior to downloading and installing an app of the permissions that are required for that app to run. If a user does not agree to the conditions, he is not allowed to install the app. *See* Frank McPherson, *Android App Permissions Explained*, SOCIALTIMES (July 29, 2010, 9:42 PM), http://socialtimes.com/android-app-permissions-explained_b47761.

[21] *See infra* Part I.C.

[22] *See Application Licensing*, ANDROID DEVELOPERS, http://developer.android.com/guide/publishing/licensing.html (last visited Sept.12, 2011).

[23] *See* Bilton, *3G Devices*, *supra* note 2 and accompanying text.

[24] *See* FOURSQUARE, www.foursquare.com (last visited Sept. 12, 2011).

[25] *See* GOWALLA, www.gowalla.com (last visited Sept. 12, 2011).

[26] Shane Snow, *Foursquare vs. Gowalla: Location-Based Throwdown*, MASHABLE (Dec. 25, 2009), http://mashable.com/2009/12/25/foursquare-gowalla/.

to other social networks[27] and rewards a user for his continued participation.[28] This reward practice is utilized by start-up companies and by subdivisions of larger, well-established, social networks, like Facebook.[29] The rewards encourage users to share their location with their friends more frequently, thereby using the app, the company's product, more frequently.

Apps that do not use a "check in" model automatically broadcast a user's location to others within the application.[30] Google Latitude[31] ("Latitude"), for example, is primarily an extension of the mapping program Google Maps.[32] Latitude allows users to share their current location with existing contacts.[33] Unlike the "check in" model which broadcasts a message to a user's existing network, Latitude displays a user's location on a

---

[27] Linking to social networks drastically increases the overall effect of each individual check in by spreading that information to a larger number of users. The average user on Facebook has 130 friends. *See Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Dec. 3, 2010); *cf. Primates on Facebook: Even Online the Neocortex is the Limit*, ECONOMIST (Feb. 26, 2009) http://www.economist.com/node/13176775?story_id=13176775 (noting that while the average Facebook user has 120 friends, the maximum number is set by biological factors). *But see* Cameron Marlow, *Maintained Relationships on Facebook*, OVERSTATED (Mar. 9, 2009), http://overstated.net/2009/03/09/maintained-relationships-on-facebook.

[28] On foursquare, the user who "checks in" at any given location the most is deemed the "mayor" of that location. *What is a Foursquare "Mayor"?*, FOURSQUARE, http://support.foursquare.com/entries/188303-what-is-a-foursquare-mayor (last visited Sept. 11, 2011). Many businesses offer special deals or savings to the mayor of that location. *See* Robert Gembarski, *FourSquare: Unlock Check-In Specials*, BRANDING PERSONALITY (Sept. 7, 2011), http://www.brandingpersonality.com/foursquare-unlock-check-in-specials/. Furthermore, users who hold ten mayorships at once receive a "badge" on their profiles that designates them as a "Super Mayor." *The Full List of Foursquare Badges*, 4SQUAREBADGES.COM, http://www.4squarebadges.com/foursquare-badge-list/ (last visited Sept. 11, 2011).

[29] *See* Josh Constine, *Facebook Testing Places Check-In Incentive Deals and Rewards*, INSIDE FACEBOOK (Oct. 28, 2010), http://www.insidefacebook.com/2010/10/28/places-check-in-deals-rewards/.

[30] *See* Jennifer Van Grove, *iPhone App Uses Background Location for Automatic Checkins on Foursquare*, MASHABLE (Aug. 25, 2010), http://mashable.com/2010/08/25/checkmate-for-foursquare/.

[31] *See Google Latitude*, GOOGLE MOBILE, http://www.google.com/mobile/latitude/ (last visited Dec. 3, 2010).

[32] *See generally Google Maps*, GOOGLE, http://maps.google.com (last visited Sept. 13, 2011).

[33] *See Google Latitude*, *supra* note 31.

map to friends they select from their existing contact list.[34] Other mobile apps mimic this mapping function and combine it with additional features. Apps like Friends Around,[35] for example, use a hybrid model that combines reward-based "check ins" with Latitude-like visualization.[36]

B. Determining A User's Location

No matter which model an app uses, a LBMS can determine a user's current location in four ways: (1) using Global Positioning Service ("GPS");[37] (2) using the user's unique Cell-ID;[38] (3) tracking the user's Internet connection if he has access to Wi-Fi;[39] and (4) allowing the user to specify his current location.[40] Since the fourth option is user-controlled, only releasing location information specified by the user, this note will focus exclusively on the first three methods.[41]

1. GPS

GPS is the most accurate way to determine a user's location.[42] GPS locates each user through a process called trilateration,[43] which uses twenty-seven satellites in orbit above the Earth to plot

---

[34] *Id.*

[35] *See* FRIENDS AROUND, http://friendsaround.com/ (last visited Oct. 31, 2010).

[36] *See Zila Networks Raises the Social Standard with 'Friends Around Me' Mobile Application for the iPhone*, PRWEB (Apr. 14, 2010), http://www.prweb.com/releases/Friends-Around-Me/mobile-social-network/prweb3868854.htm.

[37] *See Obtaining User Location*, ANDROID DEVELOPERS, http://developer.android.com/guide/topics/location/obtaining-user-location.html (last visited Oct. 31, 2011).

[38] Shu Wang, Jungwon Min & Byung K. Yi, *Location Based Services for Mobiles: Technologies and Standards*, LG ELECTRONICS MOBILECOMM, 21 (2008), http://blue-penguin.org/cache/location-based-services-for-mobiles.pdf.

[39] *See Obtaining User Location*, *supra* note 37.

[40] *See* Sarah Perez, *Google Latitude iPhone App Revealed: Should You Use It?*, READWRITEWEB (Dec. 8, 2010, 8:07 AM), http://www.readwriteweb.com/archives/google_latitude_iphone_app_spotted.php.

[41] Keep in mind that a location based mobile service has access to whichever of these methods is available on a given device. When one is unavailable, another may be used. *See Obtaining User Location*, *supra* note 37; *see also Location and my Privacy FAQ*, WINDOWS PHONE, http://www.microsoft.com/windowsphone/en-us/howto/wp7/web/location-and-my-privacy.aspx (last visited Oct. 31, 2011).

[42] *See Obtaining User Location*, *supra* note 37.

[43] *See* Tracy V. Wilson, *How GPS Phones Work*, HOWSTUFFWORKS, http://electronics.howstuffworks.com/gps-phone.htm (last visited Oct. 31, 2011).

the intersection of at least three spheres drawn around the user and three satellites to determine his exact position on the ground.[44] Although extremely accurate, GPS suffers from several limitations. First, it is slow, and can sometimes take minutes to return a result.[45] Second, it is processor-intensive and will quickly drain a phone's battery.[46] Third, it is most effective when the user is outdoors.[47] Because of these limitations, GPS is not always the most practical way to determine a user's location.[48]

2. The Cell-ID Method

The Cell-ID[49] method is less accurate than GPS, but more versatile.[50] This process uses a carrier's cell network, not satellites, to determine a user's location.[51] Conceptually, the Cell-ID method is much simpler than GPS. Every cell phone on a given network is assigned a unique identification number.[52] When a user's phone is on, that phone will connect to the nearest cell tower to establish a connection.[53] By searching for a specific ID number it is possible to identify the tower to which a given device is

---

44 *See id.*

45 *See Using Geolocation*, MOZILLA DEVELOPER NETWORK, https://developer.mozilla.org/En/Using_geolocation (last modified Aug. 12, 2011) (explaining that GPS can take a minute or more to fix a user's location, but that less accurate information like his IP address may be returned faster).

46 *See* Adroit Allen, *The Advantages and Disadvantages of a Dedicated GPS vs A Smart Phone GPS*, HUBPAGES, http://adroitalien.hubpages.com/hub/The-Benefits-Of-A-Dedicated-GPS-vs-A-Smart-Phone-GPS 78 (last visited Sept. 11, 2011).

47 *See* Wilson, *supra* note 43 (explaining how GPS locates a cell phone).

48 Apple explained that the inability to reliably track user location is one of the reasons it needed to store user location data. Capturing that information was justified because it improved the performance of certain mobile apps. *See Apple Q&A On Location Data*, *supra* note 9.

49 *See* Wang, *supra* note 38, at 21.

50 *See Adding Location to a Non GPS Phone: Introducing CellID*, MOBIFORGE, http://mobiforge.com/developing/story/adding-location-a-non-gps-phone-introducing-cellid (last visited Sept. 11, 2011).

51 *See id.*

52 *See id.*

53 *See id.*

connected.[54] Because the tower is fixed, the location of the tower will reveal the location of the user.[55]

The Cell-ID method has benefited from the explosion of the cell phone industry.[56] There are now over 251,000 reported cell sites in the United States, compared to the 913 that existed the year before the ECPA was passed.[57] The proliferation of cell sites is directly related to the increase in the number of cell phone users.[58] As the density of cell phone users in an area grows, the only way for a carrier to accommodate the increased number of customers is to divide that area into smaller and smaller sectors.[59] Carriers then ensure that there is enough bandwidth to service the user base in that area by supplying each sector with its own tower.[60] The smaller a sector is or the more towers there are, the more accurately an individual can be located.[61] Currently, carriers commonly use "microcells," towers with a range of forty feet.[62] The Cell-ID method will become even more accurate over time as the range each tower covers decreases.

Cell-ID location has also benefited from the rise of technology, making it possible to locate a user within any given sector, irrespective of the sector's size.[63] A user within range of multiple

---

54 *See id.*

55 Cell phone towers, like Wi-Fi networks, cover a certain distance. If a user is connected to a tower, it is certain then that he is located somewhere within that tower's covered range. *See id.*

56 The number of cell phone towers has tripled over the last decade. *See In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 832 (S.D. Tex. 2010).

57 *See id.*

58 To keep up with the demand for mobile data usage at broadband speeds, more towers need to be installed. *See The FCC Says the U.S. Needs More Cell Phone Towers*, WIRELESS INDUS. NEWS (June 28, 2011), http://www.wirelessindustrynews.org/news-jun-2011/2581-062811-win-news.html; Dawn Kawamoto, *The Incredible, Shrinking Cell Phone Tower: Alcatel-Lucent Offers an Alternative*, DAILYFINANCE (Mar. 22, 2011, 6:00 AM), http://www.dailyfinance.com/2011/03/22/the-incredible-shrinking-cellphone-tower-alcatel-lucent-offers/; *LTE Cell Phone Tower Industry Growth*, DEADZONES.COM (Apr. 7, 2010), http://www.deadzones.com/2010/04/cell-phone-tower-industry-growth. html.

59 *See In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 832.

60 *See id.* (explaining that the rise of 3G technology is also increasing this demand).

61 *See id.* at 833.

62 *See id.*

63 *Id.*

towers can be located using triangulation.[64] The process is similar to the trilateration method used by GPS, but relies on the overlap of signals in space rather than on the ground.[65] By correlating the time and angle at which a phone's signal arrives at multiple base stations, the carrier can determine a user's location within fifty meters or less.[66]

3. Wi-Fi Geolocation

Wi-Fi geolocation has been available since at least 2008[67] and it is becoming even more useful as the number of smartphones increases.[68] Building off of the Google Gears geolocation project, the World Wide Web Consortium[69] ("W3C") released a geolocation application programming interface ("API") in February of 2010.[70]

The Wi-Fi method of geolocation uses various location-based clues to determine the location from which a user is currently accessing the web.[71] These "clues" include information gathered from the media access control ("MAC") address of other available Wi-Fi networks, cell towers, Bluetooth MAC address, radio-frequency identifier ("RFID"), Cell-ID, and GPS signal.[72] By collecting and storing this information, namely the MAC

---

64 *See In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 451 (S.D.N.Y. 2006).

65 *See* Chris Smith, *Cell Phone Triangulation Accuracy Is All Over The Map*, SEARCH ENGINE LAND (Sept. 28, 2008, 4:59 PM), http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790.

66 Emerging versions of this technology promise to be more accurate. *See In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 827, 833 (S.D. Tex. 2010).

67 *See* Charles Wiles, *Introducing the Gears Geolocation API for All Laptop WiFi Users*, GOOGLE CODE BLOG (Oct. 21, 2008), http://googlecode.blogspot.com/2008/10/introducing-gears-geolocation-api-for.html.

68 *See generally* Marguerite Reardon & Tom Krazit, *Google: Oops, We Spied On Your Wi-Fi*, CNET NEWS (May 14, 2010, 2:49 PM), http://news.cnet.com/8301-30686_3-20005051-266.html.

69 *See About W3C*, W3C, http://www.w3.org/Consortium/ (last visited Oct. 31, 2011).

70 *See Geolocation API Specification: Editor's Draft 10 February 2010*, W3C (Feb. 10, 2010), http://dev.w3.org/geo/api/spec-source.html (providing a simple or less technical description of the API); *see also W3C Geolocation API*, WEBSCANNOTES, http://webscannotes.com/?page_id=425 (last visited Oct. 31, 2011).

71 *See W3C Geolocation API*, *supra* note 70.

72 *See id.*

addresses[73] of other Wi-Fi networks, the W3C API can build a profile for each location.[74] As more information is gathered, it is possible to pinpoint a user's location at any given time.[75] While very few mobile browsers currently support the W3C API, the number is rising and will likely continue to increase.

C. Access To Information Stored On Your Device

LBMS do more than collect location-based data. Each app a user chooses to install on his smartphone can access different information stored on that device.[76] This access, however, is never unlimited.[77] The level of access granted to each application is

---

[73] *See* IEEE Computer Soc'y, *802 IEEE Standards For Local and Metropolitan Area Networks: Overview and Architecture*, INST. OF ELEC. AND ELECS. ENG'RS, 20 (2002), http://standards.ieee.org/getieee802/download/802-2001.pdf, ("The concept of universal addressing is based on the idea that all potential members of a network need to have a unique identifier (if they are going to coexist in the network).").

[74] *See Geolocation API Specification: Editor's Draft 10 February 2010, supra* note 70.

[75] *See Wi-Fi Based Real-Time Location Tracking: Solutions and Technology*, CISCO SYSTEMS, 1–4 (2006), http://www.techrepublic.com/whitepapers/wi-fi-based-real-time-location-tracking-solutions-and-technology/283735 (explaining how Wi-Fi geolocation works, specifically that the calculation of a user's location will be more refined if there is more information available).

[76] While no application can access user information automatically, each application has access to the data that it pulls into its "sandbox." *iOS Application Programming Guide: The Application Runtime Environment*, APPLE, http://developer.apple.com/library/ios/#documentation/iphone/conceptual/iphoneosprogrammingguide/RuntimeEnvironment/RuntimeEnvironment.html (last updated Feb. 24, 2011). "The sandbox is a set of fine-grained controls limiting an application's access to files, preferences, network resources, hardware, and so on. Each application has access to the contents of its own sandbox but cannot access other applications' sandboxes." *Id.* The data that makes it into the sandbox is normally defined by user permissions. *See, e.g.*, *id.*; *Security and Permissions*, ANDROID DEVELOPERS, http://developer.android.com/guide/topics/security/security.html (last updated Sept. 13, 2011).

[77] *See, e.g.*, *supra* note 76 ("A central design point of the Android security architecture is that no application, by default, has permission to perform any operations that would adversely impact other applications, the operating system, or the user. This includes reading or writing the user's private data (such as contacts or e-mails), reading or writing another application's files, performing network access, keeping the device awake, etc. An application's process runs in a security sandbox. The sandbox is designed to prevent applications from disrupting each other, except by explicitly declaring the permissions they need for additional capabilities not provided by the basic sandbox. The system handles requests for permissions in various ways, typically by automatically allowing or disallowing based on certificates or by prompting the user. The permissions required by

determined by a set of controls called "permissions."[78] Applications do not have access to any user information by default, and can only access whatever the "permissions" allow them to.[79] These restraints can be defined either at the installation of the application by a traditional "clickwrap" license,[80] or later on throughout the use of the application by user prompts.[81] The type of permission required depends on the information being sought by the application and varies according to the phone's operating system.[82]

Permissions are important because a user-defined permission is evidence that a user consents to the application accessing that data.[83] In an attempt to gain permission most privacy policies

an application are declared statically in that application, so they can be known up-front at install time and will not change after that.").

78 *See id.*

79 *See id.*

80 *See* Feldman v. Google Inc., 513 F. Supp. 2d 229, 236 (E.D. Pa. 2007) ("A clickwrap agreement appears on an internet webpage and requires that a user consent to any terms or conditions by clicking on a dialog box on the screen in order to proceed with the internet transaction."); *see also* Ed Bayley, *The Clicks That Bind: Ways Users "Agree" to Online Terms of Service*, ELEC. FRONTIER FOUND. (Nov. 2009), http://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service.

81 For example, an application that wants to access your GPS data can satisfy the above requirement by: (1) including as part of a general term of service agreement that you allow them to access your location data at all times or; (2) prompting the user with a question, similar to "do you want to allow X to access your location," that governs what the application is allowed to do. Following these procedures, an application can access any of the information it wants on a user's device, contacts, e-mails, etc., as long as it makes sure it secures permission first. *See* Katherine Noyes, *Why Android App Security is Better Than for the iPhone*, PC WORLD BUS. CTR. (Aug. 6, 2010, 4:20 PM), http://www.pcworld.com/businesscenter/article/202758/why_android_app_security_is_better_than_for_the_iphone.html; *see also About Permissions for Third-Party Applications*, BLACKBERRY, http://docs.blackberry.com/en/smartphone_users/deliverables/22178/About_permissions_for_third-party_apps_50_778147_11.jsp (last visited Sept. 29, 2011); *Security and Permissions*, *supra* note 76.

82 *See Security and Permissions*, *supra* note 76; *Security Overview*, APPLE, 47 (June 7, 2011), https://developer.apple.com/library/ios/documentation/Security/Conceptual/Security_Overview/Security_Overview.pdf; *BlackBerry Smartphones: UI Guidelines Version 6.0*, BLACKBERRY (Nov. 22, 2010), http://docs.blackberry.com/en/developers/subcategories/?userType=21&category=Java+Development+Guidelines.

83 *See infra* Part II. Every application gains the consent necessary to access user information in a different way. For example, Google Maps uses a traditional clickwrap structure that requires the user to agree to a list of terms and conditions when the program

inform users about: (1) the type of information collected; and (2) the purpose for collecting that information.[84] Applications tend to define the type of data broadly in an attempt to strike a balance between providing enough information so that application may gain consent to access a user's data[85] and being broad enough to avoid ruling out specific information.[86] Similarly the purpose of the data acquisition is also very broad. For example, a privacy policy may state that user data can be collected for anything related to "improving the content of the Service."[87] As the scope of "improving the content of the Service" is never defined, any usage

is initially launched. Peter S. Vogel, *A Worrisome Truth: Internet Privacy is Impossible*, TECHNEWSWORLD (June 8, 2011, 5:00 AM), http://www.technewsworld.com/story/72610.html. Foursquare, on the other hand, embeds its terms in a privacy policy posted on its website, and not within the app. *See infra* note 84 and accompanying text.

84 *See, e.g.*, *Privacy Policy*, FOURSQUARE, http://foursquare.com/legal/privacy (last updated Jan. 12, 2011) ("Personal Information You Provide to Us: We receive and store any information you enter on our Service or provide to us in any other way. The types of Personal Information collected may include your name, email address, phone number, birthday, Twitter and/or Facebook usernames, use information regarding your use of our Service and browser information. We automatically receive your location when you use the Service. The Personal Information you provide is used for such purposes as allowing you to set up a user account and profile that can be used to interact with other users through the Service, improving the content of the Service, customizing the advertising and content you see, and communicating with you about specials and new features. We may also draw upon this Personal Information in order to adapt the Services of our community to your needs, to research the effectiveness of our network and Services, and to develop new tools for the community.").

85 *See Security and Permissions*, *supra* note 76.

86 *See id.* Looking more closely at the foursquare example, users consent to the collection of information they "enter on our service" along with anything they "provide . . . in *any other way*." *See Privacy Policy*, *supra* note 84. What "other way" someone might provide data to that service is not clear. The privacy policy only states that the application may collect "browser information." *See id*. What exactly is included in "browser information" remains unknown.

87 *See Privacy Policy*, *supra* note 84. Foursquare amended its privacy policy on December 2, 2010 to clarify what it was automatically collecting. However, this does not change value of the above example with regard to other policies. *See id.* ("Information Collected Automatically: When you use the Service, foursquare automatically receives and records information on our server logs from your browser or mobile platform, including your location, IP address, cookie information, and the page you requested. We treat this data as non-Personal Information, except where we are required to do otherwise under applicable law.").

could conceivably fall within that category.[88]

II. THE LEGAL BASIS OF MOBILE PRIVACY REGULATION

Currently there is no statute specifically regulating access to user data.[89] Instead this information is governed by statutes regulating electronic communication[90] such as the ECPA.[91] The ECPA was enacted to extend the protections of the Federal Wiretap Act[92] to electronic communications.[93] It addresses three types of intrusive conduct: the intercepting of live communication, the accessing of stored communications, and the recording of "non-content" information.[94] These three categories are reflected in the three titles of the ECPA: Title I–Interception of Communications and Related Matters, which regulates access to live communications; Title II–Stored Wire and Electronic Communications and Transactional Records Access (herein "SCA"), which deals exclusively with access to communications in storage;[95] and Title III – Pen Registers and Trap and Trace Devices

---

88 Providing information to third-party retailers might make the service better, just as monitoring a user's location to ensure he arrives home safely could as well. As it is currently drafted, the boundaries are unclear.

89 For examples of proposed legislation, see Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011); Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011); Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 5777, 111th Cong. (2010).

90 *See* 18 U.S.C. § 2510(12) (2006) (defining "electronic communication" 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").

91 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.).

92 The Federal Wiretap Act was codified at the same time as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968).

93 S. Rep. No. 99-F541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

94 *See id.* at 3557, 3600.

95 Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2701–12 (2006)).

("the Pen Register Statute"), which sets limitations on the access to non-content information.[96]

Each of the ECPA's three titles has its own standard that controls access to communications within that class. Title I, which modified the Federal Wiretap Act, utilizes the highest standard. It requires that the government obtain a warrant, upon a showing of probable cause that the information to be seized is evidence of a crime.[97] Title II, the SCA, uses a lower standard. Under the SCA, the government need only show "specific and articulable facts" that the stored information sought is "relevant and material to an ongoing criminal investigation."[98] Lastly, if the information sought falls under Title III, the Pen Register Statute, the government may obtain a court order for the installation of a pen register device upon mere "certification" that the information sought is "relevant to an ongoing criminal investigation."[99]

Under this three-tiered structure, how a piece of information is treated depends on how it is classified. The dividing line between Titles I, II and III is designed to mirror the amount of privacy an individual can reasonably expect in communications that fall within each class.[100] Understanding what courts consider a reasonable expectation of privacy is the first step in understanding the ECPA's overall structure.

---

96 Title III of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 3121–27 (2006)).

97 *See In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, & for Geographic Location Info., 497 F. Supp. 2d 301, 304 (D.P.R. 2007); *see also* FED. R. CRIM. P. 41(c)(1) (the traditional warrant requirement).

98 *See* 18 U.S.C. § 2703(d) (2006); *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, & for Geographic Location Info., 497 F. Supp. 2d at 304.

99 18 U.S.C. § 3122(b)(2) (2006).

100 *See* United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *3 (D. Or. Jan. 8, 2010) ("Courts, however, have long held that different communications hardware and technologies carry different reasonable expectations of privacy.").

A. Katz and the Expectation of Privacy in Electronic Communications

Much of our modern conception of privacy is grounded in the Fourth Amendment's mandate that individuals "shall be secure in their person, houses, papers and effects" from unreasonable government intrusion.[101] Though it may sound like a blanket grant of protection, the scope of the Fourth Amendment is actually limited. *Katz v. United States*,[102] a wiretap case, established that people are protected from unwarranted government intrusion only in situations where: (1) they have a subjective expectation of privacy; and (2) that expectation is one society is prepared to recognize as "reasonable."[103] Since only "reasonable" expectations of privacy will be honored, for information to receive protection it must meet this threshold.

Applying the *Katz* test to modern communications is often a multi-step process. Most communications can be broken down into component parts, each of which must be addressed separately within the reasonable expectation of privacy analysis.[104] For example, a landline phone call can be split into two pieces, the number dialed and the conversation that follows. As each of these contains distinct information, the level of privacy an individual can reasonably expect will be different for each component.[105]

In following this method, ECPA treats the phone number and conversation differently. The phone number receives very little protection.[106] The conversation however, is almost sacred.[107] Because the level of privacy one expects in the content of the phone call is much higher, Title I of ECPA requires a warrant before law enforcement can gain access to a phone conversation.[108]

---

101 U.S. CONST. amend. IV.

102 389 U.S. 347 (1967).

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

104 *See* Smith v. Maryland, 442 U.S. 735, 741 (1979).

105 *Id.* at 742.

106 *See id.* (explaining that phone numbers are subject to less protection because "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial.").

107 *Katz*, 389 U.S. at 361 (explaining that an individual is "entitled to assume that his conversation is not being intercepted.").

108 18 U.S.C. § 2516 (2006).

Compared to the mere "certification" law enforcement needs to access a phone number under Title III,[109] the difference is considerable.

In many situations, however, the dividing line is not so clear. The *Katz* test recognizes that not all communications within the same class should be entitled to the same expectation of privacy.[110] Instead, a factual inquiry into the circumstances surrounding how a method of communication is used is often warranted.[111] However, 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.[112] In a mobile app context, this means that once an individual chooses to disclose certain information to an application by accepting a requested permission, he loses whatever expectation of privacy he may have previously had. Once a permission is accepted, it does not matter whether a user believes his information is not public. Even if a subjective expectation of privacy previously existed, that expectation becomes less reasonable once that information is public.[113] In this way privacy after *Katz* takes into consideration the level of access of each piece of information. Courts charged with applying the test must distinguish between situations in which the same method of communication was used differently.[114]

Since a government intrusion must infringe on *both* an individual's subjective expectation of privacy and one society is prepared to recognize as reasonable, how "private" (or public) an individual thinks he has made his activity is not dispositive.[115] The

---

109 *Id.* § 3122(b)(2).

110 *Katz*, 389 U.S. at 351 n.5.

111 *See* United States v. Maynard, 615 F.3d 544, 566 (D.C. Cir. 2010) ("Fourth Amendment cases must be decided on the facts of each case, not by extravagant generalizations." (quoting Dow Chem. Co. v. United States, 476 U.S. 227, 238 n.5 (1986))).

112 *Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

113 *See id.*

114 For example a cell phone conversation that takes place in a closed telephone booth may be treated differently than one that occurs on a crowded city bus. *See id.* at 351.

115 *See* California v. Ciraolo, 476 U.S. 207, 212 (1986) ("[T]he test of legitimacy is not whether the individual chooses to conceal assertedly private activity, but instead whether the government's intrusion infringes upon the personal and societal values protected by

societal expectation also has value.[116] Thus, if society considers something to be private, it is likely that an individual would be justified in expecting privacy in that instance. This concept is critical to a court's understanding of a new technology because there is no established precedent to guide its analysis.

Society's expectation of privacy is higher when dealing with a new technology that is not "generally available to the public."[117] The Supreme Court has addressed a range of new technologies over time, from aerial mapping cameras[118] to thermal imaging devices.[119] In each case, the Court has assessed the reasonableness of an individual's expectation of privacy by looking at how accessible that technology was to the general public.[120] In this context, access to the technology is directly related to the ability to access certain information. Arguably, the more common a technology is, the more likely it is to be used to collect information, and therefore the less reasonable it is for one to expect that his actions will remain hidden.[121]

---

the Fourth Amendment." (quoting Oliver v. United States, 466 U.S. 170 (1984)) (internal quotation marks omitted)).

116 Many cases in which the defendants have done everything possible to conceal their behavior are still decided against an expectation of privacy. *See id.* at 211–13 ("It can reasonably be assumed that the 10-foot fence was placed to conceal the marijuana crop from at least street-level views. . . . Yet a 10-foot fence might not shield these plants from the eyes of a citizen or a policeman perched on top of a truck or two-level bus."); *see also* Dow Chem. Co. v. United States, 476 U.S. 227, 241 (1986) ("Short of erecting a roof over the Midland complex, Dow has, as the Court states, undertaken 'elaborate' precautions to secure the facility from unwelcome intrusions.").

117 *See Dow Chem.*, 476 U.S. at 238.

118 *Id.* at 231.

119 *See* Kyllo v. United States, 533 U.S. 27, 29–30 (2001).

120 *Id.* at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home . . . constitutes a search—at least where (as here) the technology in question is not in general public use."); *see also Dow Chem.*, 476 U.S. at 231 ("The photographs at issue in this case are essentially like those commonly used in mapmaking. Any person with an airplane and an aerial camera could readily duplicate them."); *Ciraolo*, 476 U.S. at 215 ("In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.").

121 *See Kyllo*, 533 U.S. at 34 ("[T]he technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private."). *But see Dow Chem.* 476 U.S. at 238 ("[S]urveillance of private property by using highly sophisticated surveillance equipment

This analysis also cuts the other way. Revealing something to the public ordinarily subjects it to a lower expectation of privacy. However, when technology is involved in data collection, one must also examine the method of surveillance under the general accessibility standard.[122] Therefore, in this context, the use of certain technology may create a reasonable expectation of privacy where one previously would not have reasonably expected it.[123]

This "method of surveillance" standard, as applied to modern technology, is derived from *Kyllo v. United States*.[124] In *Kyllo*, law enforcement used a thermal imaging device to observe the relative heat levels inside a house.[125] While the information they collected, thermal radiation, was publicly available, the technology they used was not.[126] Were the traditional *Katz* rational to apply, this public information would not be subject to any reasonable expectation of privacy.[127] The Court, however, focused instead on the technology used to collect that information. It reasoned that even if Kyllo could expect that the heat leaving his house was public, he would not reasonably expect that a thermal imager would be waiting outside.[128]

The import of *Kyllo* is that the use of technology during surveillance may weaken or reverse the effect of public disclosure under the *Katz* analysis. Society may not justifiably impose a lower expectation of privacy on a communication simply because it was made in a public place.[129] The method of surveillance and

not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.").

122 *Kyllo*, 533 U.S. at 33–34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

123 *Dow Chem.*, 476 U.S. at 238 (suggesting that the "use of highly sophisticated surveillance equipment not generally available to the public . . . might be constitutionally proscribed absent a warrant"); *see also Katz*, 389 U.S. at 351 ("But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citing Rios v. United States, 364 U.S. 253 (1960))).

124 533 U.S. at 34.

125 *Id.* at 30.

126 *Id.* at 34.

127 *Id.*

128 *Id.*

129 *Cf. id.*; Katz v. United States, 389 U.S. 347, 352 (1967).

how that public information was collected are equally important.[130] Location is only one factor in the analysis.

This modification to the *Katz* standard is extremely important in the context of mobile privacy. Just as a landline phone call can be divided into two components,[131] mobile communications may be subdivided into smaller parts as well. The data stream from a cell phone may contain many different types of information. It may contain audio from a phone call, e-mail, and data related to a user's current location.[132] Following an application of the hybrid *Katz/Kyllo* test, the reasonable expectation of privacy in each of those communications would be determined separately, by evaluating the general accessibility of the technology required to capture each stream.[133] The technology required to intercept a public phone call, the human ear, is generally accessible to the public. The technology required to intercept an e-mail from a data stream is not. While it may be reasonable that another person within earshot could overhear a conversation taking place, that does not affect an individual's expectation of privacy regarding the e-mail communication his phone is simultaneously receiving.[134]

The three titles of ECPA separate communications not just by the level of privacy an individual can reasonably expect but also by the characteristics of the communication itself.[135] In determining the nature of a given communication there are three remaining

---

130 *Kyllo*, 533 U.S. at 35 n.2 ("The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful.").

131 *See* Smith v. Maryland, 442 U.S. 735, 743 (1979) ("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").

132 *See* Jenna Worthham, *Cell Phones Now Used More for Data Than for Calls*, N.Y. TIMES, May 14, 2010, at B1, *available at* http://www.nytimes.com/2010/05/14/technology/personaltech/14talk.html.

133 *See* United States v. Ahrndt, No. 08-468-KI, 2010 WL 3773994, at *4 (D. Or. Jan. 8, 2010).

134 *See Katz*, 389 U.S. at 352 ("But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen.").

135 *See* 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.).

questions a court must ask: (1) was the communication considered "stored" or "in transmission" when it was intercepted?; (2) does the communication contain "content" or "non-content" information; and (3) is there an exception provided for by the statute?

1. Is it Stored or in Transmission?

The ECPA treats stored electronic communications differently than communications that are in transmission. The statutory language is clear: Title I of the ECPA covers only the *interception* of electronic communications[136] while Title II deals only with *stored* communications.[137] Yet despite this clarity courts are still divided on how this language should apply.

Many courts find that Title I and Title II of the ECPA are mutually exclusive.[138] These courts focus on the distinction between "interception" and "access," and find that it is impossible for an electronic communication to violate both provisions.[139] The rationale is that the ECPA defines the two states of an electronic communication separately, and because the word "transfer" only describes the transmission and not the "electronic storage," the two titles are discrete.[140] A communication therefore must fit into one of the two categories; there is no middle ground.

---

136 *See id.*

137 *See id.*; 18 U.S.C. § 2701(a) (2006) (applying to whoever "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage").

138 *See* Konop v. Hawaiian Airlines, 302 F.3d 868, 890 (9th Cir. 2002) (Reinhardt, J., concurring in part and dissenting in part) (citing United States v. Smith, 155 F.3d 1051, 1058–59 (9th Cir. 1998)); *In re* Double Click Inc. Privacy Litig., 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001); Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000); State Wide Photocopy, Corp. v. Tokai Financial Services, Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995).

139 *See Konop*, 302 F.3d at 876–79.

140 *Id.* at 877 ("Congress' use of the word 'transfer' in the definition of 'electronic communication,' and its omission in that definition of the phrase 'any electronic storage of such communication' . . . reflects that Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage'" (internal citations omitted)); Wesley Coll. v. Pitts, 974 F. Supp. 375, 386 (D. Del. 1997) ("[B]y including the electronic storage of wire communications within the definition of such communications but declining to do the same for electronic communications—Congress sufficiently evinced its intent to make acquisitions of electronic

Similarly, these courts also apply a narrow definition of "interception"[141] and find that the Federal Wiretap Act covers only electronic communications that are acquired contemporaneously with their transmission.[142] Once an electronic communication passes into storage, even temporarily, it switches over to Title II. Because a stored communication can no longer be "intercepted" it is governed by the requirements of the SCA.

At least one court, the Seventh Circuit, has rejected this interpretation of the statute.[143] In *United States v. Szymuszkiewicz*, the Seventh Circuit examined the relationship between the Wiretap Act and SCA as they apply to the interception of e-mails.[144] The case arose from a situation in which office politics had gone too far. Mr. Szymuszkiewicz feared that he was going to lose his job.[145] To obtain more information, he sneaked on to his boss's computer and configured Microsoft Outlook to forward him copies of all the messages his boss received.[146]

Szymuszkiewicz was charged under the Wiretap Act for illegally intercepting his boss's e-mails.[147] Szymuszkiewicz contested the charge as a matter of timing, arguing that

communications unlawful under [the Wiretap Act] only if they occur contemporaneously with their transmissions."); United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) ("[I]ntercepting an electronic communication . . . means acquiring the *transfer* of data. . . . [T]he definitions thus imply . . . that the acquisition of the data be simultaneous with the original transmission of the data."). *See also* United States v. Smith, 155 F.3d 1051, 1057 (9th Cir. 1998) (finding that a narrow definition of intercept is appropriate in the context of electronic communications).

141 *See* Steve Jackson Games Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–62 (5th Cir. 1994) (defining the term "intercept" to mean an acquisition contemporaneous with transmission).

142 *See Konop*, 302 F.3d at 878 ("In cases concerning 'electronic communications'—the definition of which specifically includes 'transfers' and specifically excludes 'storage'—the 'narrow' definition of 'intercept' fits like a glove; it is natural to except non-contemporaneous retrievals from the scope of the Wiretap Act." (quoting United States v. Smith, 155 F.3d 1051, 1057 (9th Cir. 1998))).

143 *See generally* United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010).

144 *Id.* at 703.

145 *Id.*

146 *Id.*

147 *See* United States v. Szymuszkiewicz, No. 07-CR-171, 2009 WL 1873657, at *1 (E.D. Wis. June 30, 2009) (Szymuszkiewicz was charged with three counts of intercepting an electronic communication in violation of 18 U.S.C. § 2511(1)(a)).

interception must be defined narrowly to mean "contemporaneous with transmission."[148] According to Szymuszkiewicz, alleging a violation of the Wiretap Act was inappropriate because his boss's computer did not forward the e-mails until *after* they were received.[149] Under this narrow reading of the statute, his e-mail surveillance efforts did not violate the SCA because, as he argued, if the e-mail was forwarded after it was stored on the host computer then it could not be intercepted.[150]

The court rejected this interpretation for two reasons. First, the plain language of the statute provides no timing requirement for interception.[151] This argument is similar to the one advanced in Judge Reinhardt's opinion in *Konop v. Hawaiian Airlines Inc.*,[152] a case that also interprets Internet privacy. Judge Reinhardt, concurring in part and dissenting in part, pointed out that the ECPA defines "intercept" as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic . . . device."[153] Courts that apply a narrow definition of "intercept" appear to ignore this language and define interception differently.[154]

---

148 *Id.* at *7.

149 *Szymuszkiewicz*, 622 F.3d at 703.

150 The idea that interception must be contemporaneous with transmission is derived from an earlier case, United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976). *See* Konop v. Hawaiian Airlines, 302 F.3d 868, 877 (9th Cir. 2002) (Reinhardt, J., concurring in part and dissenting in part). *Turk* interpreted an earlier version of the Wiretap Act, before the amendments made by ECPA included electronic communications. *Id.* Because the statute has since been revised, the language the *Turk* court relied on no longer exists thus overruling the requirement that interception be contemporaneous with transmission. *Id.*

151 Szymuszkiewicz, 622 F.3d at 706 ("There is no timing requirement in the Wiretap Act, and judges ought not add to statutory definitions." (citing Lockhart v. United States, 546 U.S. 142, 146 (2005))).

152 *Konop*, 302 F.3d at 887 (Reinhardt, J., concurring in part and dissenting in part).

153 *Id.* at 876 *(*quoting 18 U.S.C. § 2510(4) (2006) (internal quotation marks omitted)).

154 *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994).

> Prior to the 1986 amendment by the ECPA, the Wiretap Act defined 'intercept' as the 'aural acquisition' of the contents of wire or oral communications through the use of a device. 18 U.S.C. § 2510(4) (1968). The ECPA amended this definition to include the 'aural *or other* acquisition of the contents of . . . wire, *electronic*, or oral communications. . . .' 18 U.S.C. § 2510(4) (1986) (emphasis added for new terms). The significance of the addition of the words 'or

The court's second reason for rejecting Szymuszkiewicz's argument focused on the differences between the transmission of electronic and wire communications. Wire communications, like telephones, use circuit switching technology.[155] Circuit switching creates a single electronic pathway or circuit between the devices involved in a call.[156] Alternatively, electronic communications use "packet switching" to send data.[157] "Packet switching" breaks a message down into small packets of data.[158] These packets contain not only information about the content of the message, but also routing information, like an address, that tells the packet where it has to go.[159] Each packet travels independently.[160] The network then arranges and resends the packets as necessary so that at least one copy of each packet (there may be many) reaches its final destination.[161] Once all of the packets for a given message are received, a computer then uses a specific protocol[162] to reassemble the packets and create the entire message.[163]

The *Szymuszkiewicz* court reasoned that because of these technological differences, it would be impossible to apply a timing

> other' in the 1986 amendment to the definition of 'intercept' becomes clear when the definitions of 'aural' and 'electronic communication' are examined; electronic communications (which include the non-voice portions of wire communications), as defined by the Act, cannot be acquired aurally.

Id.

155 *See Szymuszkiewicz*, 622 F.3d at 704.

156 *See id.*

157 *See id.*

158 *See* Lee Copeland, *Quick Study: Packet-Switched vs. Circuit Switched Networks*, COMPUTERWORLD (Mar. 20, 2000), http://www.computerworld.com/s/article/41904/Packet_Switched_vs._Circuit_Switched_Networks; *see also Paul Baran and the Origins of the Internet*, RAND CORPORATION, http://www.rand.org/about/history/baran.list.html (last modified Mar. 28, 2011).

159 *See* Copeland, *supra* note 158.

160 *See id.*

161 *See id.*

162 A "protocol" is a standard language by which computers communicate with one another. For instance, there are three e-mail protocols that govern how an e-mail message can be transmitted and received—POP, IMAP, and SMTP. *See* Vic Laurie, *Computer Protocols: TCP, IP, UDP, POP, SMTP, HTTP, FTP and More*, COMPUTER EDUC., http://vlaurie.com/computers2/Articles/protocol.htm (last updated July 13, 2011, 5:17 PM).

163 *See* Copeland, *supra* note 158.

requirement to information sent over a packet switched network.[164] Interception could never take place contemporaneously with transmission because there is no continuous connection between the two ends of an electronic communication.[165] Following a narrow definition of "interception" in the context of electronic communications therefore would produce conflicting and inconsistent results.[166]

To further highlight this argument, the court focused on Voice Over Internet Protocol ("VoIP") services that allow users to make telephone calls over the Internet.[167] These services deliver phone calls through packet switched networks rather than the traditional circuit switched telephone lines.[168] A reading of the Wiretap Act that protects against interception only if it is contemporaneous with transmission ignores VoIP phone calls and criminalizes only those made through traditional circuit switching channels.[169] Given that the Wiretap Act protects the content of a phone call,[170] this surely would be an unintended result. If the statute protects the content of a phone call, then when that call was intercepted should be irrelevant.[171]

---

164 *See* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (2010).

165 *Id.* at 705 ("Szymuszkiewicz's understanding of 'interception' as 'catching a thing in flight' is sensible enough for football, but for email there is no single 'thing' that flies straight from sender to recipient. When sender and recipient are connected by a single circuit, and the spy puts a 'tap' in between, the football analogy makes some sense . . . For e-mail, however, there are no dedicated circuits. There are only packets, segments of a message that take different routes at different times.").

166 *Id.* at 705 ("The difference between circuit-switch and packet-switch transmission methods thus is irrelevant under § 2510." (citing 18 U.S.C. §2510(4) which defines "interception" as "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of *any* electronic . . . device." (emphasis added))).

167 *See id.* at 706.

168 *See generally In re* IP-Enabled Services, 19 F.C.C.R. 4863, 4869 (2004) (reviewing Internet telephony in comparison to traditional landline technology).

169 *See Szymuszkiewicz*, 622 F.3d at 706.

170 *See id.* at 706; *see also* Briggs v. Am. Air Filter Co., 630 F.2d 414 (5th Cir. 1980); Ali v. Douglas Cable Communc'n, 929 F. Supp. 1362 (D. Kan. 1996); United States. v. Borch, 695 F. Supp. 898 (E.D. Mich. 1988).

171 *See Szymuszkiewicz*, 622 F.3d at 706.

> Many phone calls today are made by digitizing speech and transferring the result by packet switching. Transmission by packet switching allows for multiple simultaneous messages over a single circuit and so is cheaper than circuit switching. The adoption of

The court extended its reasoning to the e-mail transmissions.[172] If the Wiretap Act would prevent someone from intercepting a call made using VoIP, then it should also prevent someone from intercepting an e-mail. Since both use the same protocol to transmit information, any requirement that e-mails be intercepted as they were being sent would be equally inappropriate.[173] A different interpretation of the statute would create a conflict and allow e-mails to be read in some situations but not in others.

Addressing Szymuszkiewicz's argument that he had been charged under the wrong statute, the court also held that both the Wiretap Act and the SCA could apply to a single communication and that nothing prohibits both sections from applying at the same time.[174] "Overlapping criminal statutes are nothing new," and the court held that it is appropriate to allow overlapping set of statutes in a civil context as well.[175]

The SCA does not explicitly repeal any part of the Wiretap Act, and the court held that each statute is therefore "fully enforceable according to its own terms."[176] This reasoning recognizes and accounts for the differences between electronic and

> packet switching is not limited to 'voice over IP' services such as Vonage or Skype. The fourth-generation protocol for mobile phones, being introduced this year in the United States, is one part of an effort to transmit all voice communications by IP ('Internet Protocol', a packet-switched method) before many more years have passed. *See* 3rd Generation Partnership Project, *All–IP Network (AIPN) Feasibility Study*, Technical Report no. 22.978 rel. 8 (Dec. 2008). The 'interception' of a communication sent in packets must be done by programming a computer to copy the contents it sends along (and reassemble them later), which was exactly what Szymuszkiewicz told Infusino's computer to do with her incoming emails. In saying that the Wiretap Act's definitions treat the acquisition of emails as an interception, we ensure that the Act applies to packet-switched phone calls too.

Id.

172 *Id.* at 705.

173 *Id.* at 706.

174 *Id.* at 705 ("We agree with *Councilman's* conclusion on that subject (as well as its conclusion that the Stored Communications Act does not repeal any part of the Wiretap Act by implication; each statute is fully enforceable according to its own terms).").

175 *Id.* at 706.

176 *Id.* at 705.

traditional communications, and in so doing removes the conflict that arises when a narrow definition of interception is used. Under the Seventh Circuit's reasoning, both parts of the ECPA may apply to electronic communications while communications that employ traditional circuit switching technology need not look further than the Wiretap Act.

2. Is it Content or Not?

Whether a communication contains content information plays a dual role in an ECPA analysis. On one hand, classifying something as non-content data can result in bypassing all privacy protections.[177] On the other hand, classifying something as non-content data can simply move the information to falling under Title III of the ECPA.[178] While the standard is a low one under Title III, requiring only "certification" that the information sought is part of an ongoing investigation, those seeking to access information under this title must still obtain a court order.[179] Non-content information may be outside the realm of reasonable expectations of privacy as defined by *Katz*, but it still falls within the protective language of the ECPA.

---

[177] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that there was no reasonable expectation of privacy in phone numbers dialed); United States v. Miller, 425 U.S. 435, 440 (1976) (holding that when revealing his affairs to another, the depositor assumes the risk that business records kept by a bank will be turned over to the government); Couch v. United States, 409 U.S. 322, 335–36 (1973) (holding that no reasonable expectation of privacy existed in records that were turned over to an accountant for tax preparation). *But see* Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that the content of a conversation between petitioner and a government informant was not protected by the Fourth Amendment).

[178] *See* 18 U.S.C. § 3127(3) (2006) ("the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication"); *Id.* § 3127(4) ("the term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication").

[179] *See id.* § 3122(b)(2) ("a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.").

Courts have only recently applied Title III to location-based information. In the past, the Pen Register Statute only controlled access to phone numbers.[180] However, in 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act)[181] expanded the statutory definition of a pen register device.[182] This new definition made it possible to record non-content information sent as part of an electronic or wire communication.[183] Law enforcement took advantage of this change and, following the PATRIOT Act's amendment of ECPA, began trying to obtain location-based information via pen register devices.[184] By classifying location-based information as falling under Title III, law enforcement is able to avoid the higher standards imposed by both Title I and Title II.

There was, however, one significant roadblock to this analysis. The Communications Assistance for Law Enforcement Act ("CALEA") expressly limited law enforcement access to location-based information.[185] The statute was designed to ensure that as telecommunications networks evolved, law enforcement would continue to have access to the information necessary to do its job.[186] Telecommunications companies needed to maintain their networks in such a way that it was possible to access "call-identifying information," along with "electronic messaging" and "information services" used for sharing among computer devices.[187] This requirement that information systems remain accessible to law enforcement is balanced by the limitations placed

---

180 *See Smith*, 442 U.S. at 736 n.1 ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977))).

181 USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended at 18 U.S.C. § 3121).

182 18 U.S.C. § 3127(3) (2006).

183 *See id.* § 3127.

184 *See supra* notes 108–09 and accompanying text.

185 *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 47 U.S.C.).

186 H.R. REP. NO. 103-827 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489.

187 *See* 47 U.S.C. §§ 1001-02 (2006).

on the scope of law enforcement access. Recognizing that location-based information is more sensitive than the phone numbers an individual dials, the statute dictates that "information acquired *solely pursuant* to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of the subscriber (except to the extent that location may be determined from the telephone number)."[188]

Several courts have interpreted the phrase "solely pursuant" to mean that the Pen Register Statute may be combined with some additional statutory authority to allow recording beyond what is explicitly listed in the statute.[189] Courts often rely on the SCA for this additional authority.[190] Though it was intended to apply only to stored communications, the SCA authorizes the government to require a provider of electronic communications to disclose "a record or other information pertaining to a subscriber to or customer of such service."[191] This language is very similar to that used by the Supreme Court in addressing non-content information in other customer/subscriber situations.[192] Just like bank records or telephone numbers are non-content subscriber information, cell-

[188] 47 U.S.C. § 1002(a)(2) (2006) (emphasis added).

[189] *See In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Info., 497 F. Supp. 2d. 301, 308 (D.P.R. 2007) ("[N]o such unclarity exists on the face of the statute. In particular, I do not see how the phrase 'solely pursuant' in Section 1002(a)(2) can be read so as *not* to convey the meaning that the Pen Register Statute may be used in combination with some other authority for the purpose the government seeks."); *see also In re:* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 452, nn.11–15 (S.D.N.Y. 2006) (listing all of the cases that have decided for and against this hybrid use of the statute).

[190] *See In re: Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel*., 460 F. Supp. 2d at 452–53.

[191] *See* 18 U.S.C. § 2703(c)(1) (2006).

[192] The language of this section of the statute very closely mirrors the exception for "business records" of other non-content information cases. *See United States v. Miller*, 425 U.S. 435, 440 (1976) ("On their face, the documents subpoenaed here are not respondent's 'private papers.' . . . [R]espondent can assert neither ownership nor possession. Instead, these are the business records of the banks.").

site information may be considered a "record or other information" with regard to the use of a cell phone.[193]

Users automatically disclose their location to the cell phone company every time they turn on their phones.[194] Once a phone connects to a tower the cell phone company knows that user's location.[195] If cell phone companies store this information as traditional phone companies keep records of the phone numbers dialed, then a list of that user's locations falls within the overlap between the two statutes. However, the situation changes when dealing with *prospective,* i.e. real-time, location-based data that is not yet recorded.

Courts that are in favor of treating cell-site information as "stored" data follow the narrow reading of interception that was rejected by the *Szymuszkiewicz* court.[196] These courts treat real-time location-based information as stored data because this information is received by the cell phone service provider and recorded on its system momentarily before it is forwarded to law enforcement officials.[197] As the SCA applies to communications in temporary storage, location-based information falls within its reach.[198]

Courts in opposition to this reading point to several weaknesses. In analyzing the SCA, these courts argue that nothing in the statute contemplates ongoing surveillance in real-time, but rather that the SCA seeks only to control the circumstance under which the government can compel the disclosure of *existing* communications.[199] Unlike the Wiretap Act and the Pen Register

---

193 *See In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., No. 10-MC-897 (NGG), 2011 U.S. Dist. LEXIS 93494, at *18–19 (E.D.N.Y. Aug. 22, 2011).

194 *See supra* Part I.A.

195 *See supra* Part I.B.

196 *See* United States v. Szymuszkiewicz, 622 F.3d 701, 705–07 (7th Cir. 2010).

197 *See In re:* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006).

198 18 U.S.C. § 2510(17)(A) (2006) (defining electronic storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof").

199 *See In re* Application of the U.S. for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. No. [Sealed] & [Sealed], 416 F.

Statute which are expressly designed to allow real-time surveillance, the SCA contains no limitation on the amount of time that law enforcement, pursuant to a court order, can maintain its investigation.[200] Perhaps the SCA's minimal procedural safeguards reveal Congress' intent. If the purpose of the SCA is to allow for real-time surveillance, as permitted under the Wiretap Act and Pen Register Statute, Congress could have included some restriction on duration as it did in the other two sections.

While both sides present good arguments, it is currently unclear where location-based information stands within the Title III framework. This is further complicated by the observation that if the SCA is applicable to location-based information and is sufficient to fill the gap in the Pen Register Statute then it is unclear why location-based information is not governed by the SCA's higher standards of access.

3. Is it an Exception to the ECPA?

Even if a piece of information falls perfectly within the reach of one of the three titles, it may not be protected because it is excepted from the ECPA entirely. There are a handful of exceptions to the statute, available to private parties and the government, that allow for the disclosure of intercepted information.[201]

Some of these exceptions are granted to allow for the day-to-day operation of the telecommunication industry.[202] Keeping in mind that individuals can reasonably expect the content of a phone

Supp. 2d 390, 395 n.7 (D. Md. 2006); *In re* Application of the U.S. For an Order (1) Authorizing The Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294, 313 (E.D.N.Y. 2005); *In re* Application For Pen Register & Trap/Trace Device With Cell Site Location Auth., 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005).

200 *See In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel*., 460 F. Supp. 2d at 459.

201 *See* 18 U.S.C. § 2511(2)(a)(ii).

202 For example, the protections of the ECPA do not apply to the activity of any officer, employee, or agent of a wire or electronic communication service, whose facilities are used in transmitting these communications, from intercepting or disclosing information "in the normal course of his employment while engaged in any activity which is a *necessary incident* to the rendition of his service or to the protection of the rights or property of the provider of that service." *Id.* § 2511(2)(a)(i) (emphasis added).

call to remain private, instances still exist in which the telephone service provider may need to listen in on a user's conversation. For example, a communications service provider may need to perform maintenance or quality control assessments that require listening in on a certain line. Accordingly, the ECPA contains an exception for service provider activity that aims to balance the interest of both the wire communication provider and the paying customer.[203] However this is only a limited exception for service providers, and its aim is to maintain individual privacy in situations not related to the necessary maintenance and upkeep of the communication system.[204] This exception protects phone companies that provide a valuable service from lawsuits related to activity necessary to carry on everyday operations, but allows users to continue making phone calls confident that there is not some idle operator listening in on the line.

Other exceptions are also necessary to protect public information. For example, the ECPA removes from the protections of the Wiretap Act, the SCA, and the Pen Register Statute any electronic communications that are "readily accessible" to the general public.[205] This dovetails with the rationale of *Katz* and the disclosure cases.[206] Once a communication is made public, an individual has no expectation that this communication will remain private.[207] The ECPA recognizes this change in privacy and removes public information from the scope of its protection.[208]

The most important exception to the ECPA, at least for the purposes of this Note, allows for the disclosure of a

---

203 *See id.* § 2511(2)(a).

204 *See id.*

205 *Id.* § 2511(2)(g).

206 *See supra* Part II.

207 *See* United States v. Miller, 425 U.S. 435, 443 (1976).

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.

Id.

208 18 U.S.C. § 2511(2)(g).

communication if one party has consented to it.[209] Mirroring the language used in the disclosure cases,[210] the ECPA removes from the scope of its protection information for which: (1) the observer was a "party" to the communication;[211] and (2) one of the parties has given consent to its interception.[212] This also mirrors the *Katz* analysis in that information disclosed to another party is subject to a lower expectation of privacy given that if a person consents to the interception, whether by inviting a friend over,[213] filling out a form,[214] or consciously providing information in some other way, he cannot then turn around and revoke that disclosure.[215]

The methods of sharing that the exception contemplated, however, are rather traditional. Technology has recently complicated the possible ways that users may voluntarily share their current locations. In applying the existing framework to location-based mobile services, sharing one's information through an app could likely be considered a form of consent. But unlike disclosing a secret to a friend or filling out a survey, in a digital

---

209 *Id.* § 2511(2)(d).

210 *See Miller*, 425 U.S. at 443; *see also* Hoffa v. United States, 385 U.S. 293, 302–03 (1966) (holding that the giving of consent to an informant's presence is valid because the misplaced confidence that one will not reveal wrongdoing does not create a legitimate expectation of privacy under the Fourth Amendment).

211 18 U.S.C. § 2511(2)(d).

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

Id.

212 *Id. See also* 18 U.S.C. § 2701(c) (2006) ("subsection (a) of this section does not apply with respect to conduct authorized . . . (2) by a user of that [wire or electronic communication] service with respect to a communication of or *intended for that user*") (emphasis added).

213 *See Hoffa*, 385 U.S. at 302.

214 *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001).

215 The situation where one enters personal information on a website and clicks submit is less troublesome in this regard. *See id.* at 502 n.8.

world it is not always obvious what the user is consenting to and perhaps more importantly, where that consent begins and ends.

Data collection on the Internet and on a mobile phone may occur without a user ever knowing it.[216] Many websites for example use a small file called a cookie[217] to collect information about those who visit their site.[218] In theory cookies can be helpful. A cookie can "store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner."[219] They can also be harmful, when for example they are used to store and report information from a user's browsing history to a third party.[220] In this and similar situations, a user may believe that the information stored is private.[221]

Complicating the consent analysis is the possibility that in a digital context the user may not know the third party receiving his information exists. This is common in situations that involve mobile and web-based advertising. Usually there are at least three parties to such an information transfer: the user, the website, and an unaffiliated advertising network.[222] The website and the ad network likely have an agreement that allows the ad network to access information about the website's users. The ad network places a cookie on a user's computer when he visits a customer's website. The cookie collects the user's information which is then funneled off to the ad network. In exchange for access to this information, the ad network supplies the website with advertising that is targeted to its users based on the information it collects from the cookies. Because a user is not a party to this agreement, the ad

---

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

217 Cookies are text files that a website sends to a user's computer that allow the website to track his movements. *See* Adam L. Penenberg, *Why Web Surfers Love To Hate Cookies*, SLATE MAG. (Nov. 7, 2005, 4:51 PM), http://www.slate.com/id/2129656/.

218 *See In re DoubleClick*, 154 F. Supp. 2d at 502–03.

219 *Id.*

220 *See id.*

221 The class of users that initiated the suit in *DoubleClick* alleged that the cookies were reporting names, email addresses, home and business addresses, phone numbers, searches performed, and websites visited. *See id.* at 503.

222 *See generally id.* This analysis is modeled on the facts of the *DoubleClick* case.

network is effectively collecting data using a cookie that the website, and not the web user, gave it permission to install.

Under the ECPA it is not clear if authorization is required from the actual end user;[223] the agreement between the website and the ad network may be sufficient for purposes of the exception. In light of the *Katz* privacy test, the ad network's actions are justified by the rationale of the disclosure cases. Once a user discloses information to a third party, his reasonable expectation of privacy decreases.[224] If the user consented to the website's collection of his information, which arguably he did by visiting the site,[225] then the website can authorize the third party ad network to step in.

This disclosure-based rational is mirrored by the ECPA. Under the SCA, because the information collected was intended for the visited website, that website may then authorize whoever it wants to access the data.[226] Similarly because the website was a "party" to the original communication, it is free to intercept data under the Wiretap Act as well.[227] If the website is authorized to intercept the data, arguably it should be allowed to pass that information on to another party.[228]

---

[223] *See* 18 U.S.C. § 2511(2)(d) (2006).

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

Id.

[224] *See* United States v. Miller, 425 U.S. 435, 443 (1976).

[225] *See* Commonwealth v. Proetto, 771 A.2d 823, 829 (Pa. Super. Ct. 2001) ("By the very act of sending a communication over the Internet, the party expressly consents to the recording of the message.").

[226] *See* 18 U.S.C. § 2511(2)(g)(i) (2006).

[227] *See id.* § 2511(2)(d).

[228] In reaching its conclusion, the court seems to ignore where the ad network appears in the transmission. In order to supply content, the ad network must step in at some point between the user requesting the web address and the loading of the page. The ad network therefore likely gets some information about the user from the cookie before the site actually loads. If this is the case, the information was not transferred from the website to the ad network but instead directly from the user's computer. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502 (S.D.N.Y. 2001) ("DoubleClick acts as an

While this exception seems broad, it is not absolute. The Wiretap Act provides a fallback provision that will invalidate the consent and therefore the exception if the information is intercepted "for the purpose of committing any criminal or tortious act."[229] However, this is a very difficult standard to meet. The web user must show intent and demonstrate that the desire to commit a tortious act was the primary motivation or at least a determinative factor in the ad network's actions.[230] It is not enough to simply prove that the defendant committed a tort or crime—in this case a privacy violation.[231] Instead, to obtain relief, a user must prove that the ad network collected his data because it wanted to commit a bad act. Thus, even if the user can prove that he was harmed by the collection of data,[232] that alone is not sufficient for relief under the ECPA.

III. CONFLICTING RESULTS

The ECPA attempts to base the protection it provides on the relative levels of privacy individuals expect for their information.[233] This approach of varied treatment in many ways codifies the *Katz* view of privacy.[234] However, it should not be the sole foundation for defining mobile privacy.

Mobile communications are fundamentally different from the traditional communications *Katz* addressed, both in how they are used and transmitted. In mobile communications oftentimes users are not telling a secret to a friend or filling out a survey—the kind of disclosure *Katz* envisioned—but instead are sending a rich data stream from their mobile device with several different types of information; location-based information is just one category.

intermediary between host Web sites and Web sites seeking to place banner advertisements.").

229 *See* 18 U.S.C. § 2511(2)(d).

230 *See In re DoubleClick*, 154 F. Supp. 2d at 514–15 (quoting United States v. Dale, 991 F.2d 819, 841–42 (D.C. Cir. 1993)).

231 *See id.* at 516.

232 *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490 (2006) (examining the harm that electronic surveillance creates).

233 *See supra* Part II.

234 *See id.*

Rather than address these communications separately, the ECPA treats all digital information sent from a user's mobile device the same.[235] To enable the *Katz* rationale to fit, the ECPA: (1) incorrectly categorizes information as stored or in transmission; (2) incorrectly assumes that location is non-content information; and (3) misapplies the consent exceptions within a mobile context.

A. The ECPA Incorrectly Defines "Stored Communication"

One of the major difficulties courts face when applying the ECPA is distinguishing communications that are stored from those that are in transmission.[236] The statute appears to draw the distinction based on when and where a communication is intercepted.[237] However, actually applying this "stored/in transmission" distinction correctly to digital information proves to be almost impossible.

The stored/in transmission line does not accurately reflect how electronic communications are transmitted.[238] Electronic communications have a dual nature.[239] The packets that carry the communication are stored pieces of data. Yet those packets are also in transmission as they are sent to their final location.[240] The ECPA ignores the fact that electronic communications are really the product of stored bits of information being transferred and then very quickly reassembled to create the final product. Packet-switching is fundamentally different than an analog communication involving live audio like a telephone conversation. In a live conversation the audio is not automatically stored. The information transmitted will be lost (except for in the listeners' memories) unless someone uses a recording device. Electronic communications, like emails, must always be converted into packets before they are sent to their final destination, and therefore must always be stored as data before they are transmitted. Thus one who intercepts an electronic communication would be

235 *See supra* Part II.
236 *See supra* Part II.
237 *See id.*
238 *See* United States v. Szymuszkiewicz, 622 F.3d 701, 704 (7th Cir. 2010).
239 *See id.*
240 *See id.*

intercepting stored information even though he was doing so while it was in transmission.

Because electronic communications involve the transmission of stored information, maintaining the stored/in transmission distinction frustrates the purpose of the ECPA. The Wiretap Act was originally designed to prevent the negative consequences of real-time surveillance.[241] Focusing solely on the status of a communication at the transmission stage ignores the potential harm created by the interception of that message. The *Szymuszkiewicz* court identified this conflict by examining how its decision would impact the classification of VoIP services.[242] VoIP is a new technology that provides an "old" technology function—phone calls. Listening in on phone calls is precisely the kind of harm the Wiretap Act was designed to prevent. If the Wiretap Act only applied in situations where interception was contemporaneous with transmission, a phone call made using VoIP technology would not be protected.[243] Instead, it would be governed by the rules of the SCA and subject to a much lower standard for access along with an unlimited time frame of observation.[244]

The method of transmitting a call, or any other electronic communication, should not affect the level of privacy protection it receives. Maintaining the stored/in transmission distinction ignores the functional similarities between different communications that may logically justify equal protection. For example, VoIP is the functional equivalent of a phone call.[245] There is no dispute that the content of a phone call is protected.[246] It should not be that an individual loses that protection simply by placing a call from something other than a landline. Regardless of

---

241 Solove, *supra* note 232, at 492–93.

242 *See Szymuszkiewicz*, 622 F.3d at 706.

243 *See supra* Part II. It may be possible to argue otherwise if the person using a VoIP service called someone with a traditional landline telephone and that call was tapped from the wire connection and not the VoIP end of the call. However, this argument is precisely the point this note stands against.

244 18 U.S.C. § 2703 (2006).

245 *See Szymuszkiewicz*, 622 F.3d at 706 ("Transmission by packet switching allows for multiple simultaneous messages over a single circuit and so is cheaper than circuit switching.").

246 *See supra* Part II.

how the conversation is transmitted, by copper wire or by packets of information, the resulting service is the same. Because a phone call on either system provides the same service for the user, society would reasonably expect that the privacy afforded to each system be the same. As a result, the harm to society of eavesdropping in either case is also the same. These functional similarities and not the method of transmission should be used to determine the appropriate level of protection.

The stored/in transmission distinction is particularly important to the regulation of location-based mobile services because of the way courts have incorporated location-based data into the Pen Register Statute. This determination is very similar to the VoIP analogy mentioned above. Because location-based data is stored momentarily during the transmission process, it is subject to the lesser protections offered by the SCA.[247] This, read together with the Pen Register Statute, subjects a user's current location, possibly the most sensitive piece of information, to the lowest level of privacy protection.[248]

Just like the VoIP example, for location-based data it should not matter whether there is momentary storage. The focus should instead be on the harm created by the real-time surveillance of a user's location. Arguably, this approach is already built into the ECPA, and both the Wiretap Act and the Pen Register Statute impose time limits and other conditions on situations that involve real-time surveillance.[249] Since the method of transmission, and thus how that data may be intercepted, does not affect or alter the potential societal harm, the technical method of transmission should not affect the amount of protection a communication receives.

---

247 *See supra* Part II.

248 *See supra* Part II.

249 18 U.S.C. § 2518(5) (2006) ("No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days."); *Id.* § 3123(c)(1) ("An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days."). The SCA does not contemplate real time data and therefore does not impose a time limit on government access.

B. The Pen Register Statute Incorrectly Assumes Location is Non-Content Information

While the language of the Pen Register Statute may allow for a hybrid reading in combination with the SCA, that interpretation should not be applied to location-based information. The classification of location-based information as non-content data does not accurately reflect the public's use of that information. The Pen Register Statute, which traditionally governed access to phone numbers,[250] imposes a very low hurdle to access only because the information it was meant to protect is non-content data[251] that was necessarily disclosed to a third party.[252] Location-based user data meets neither of these criteria.

The way the general public currently uses location-based data supports the argument that such data is content. Users who permit location-based services to share their location with others can choose when they will allow that information to be shared. There is no default public setting for one's location, as there is with a phone number or mailing address in a public directory.[253] Except pursuant to a court order, any sharing of information is at the user's discretion. It appears, therefore, that users value location-based information more than they do other public information. Users share such information only at the times and places that they choose to. And furthermore, when the disclosure of a user's location is linked to a social network or media outlet, the sharing of that information creates content for other users.

---

250 *See* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979).

251 *See* 18 U.S.C. § 3121(c) ("A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so *as not to include the contents* of any wire or electronic communications.") (emphasis added).

252 *See* United States v. Miller, 425 U.S. 435, 443 (1976).

253 *See* In the Matter of the Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification Sys. on Tel. Nos. (SEALED) and (sealed) and the Prod. of Real Time Site Info., 402 F. Supp. 2d 597, 599 (D. Md. 2005) ("As the phone changes location, it automatically switches to the cell site that provides the best reception," and therefore there is no default location).

This release of data has a minimum value simply because it is restricted. As far back as 2001, courts recognized a value in this user information.[254] The following explosion of a data-based web economy took this proposition even farther. Not only does data have value for the companies that collect it, but users have also recognized that they control an asset that can be used as currency for exchange.[255] Mobile check-in based applications illustrate this fundamental change in how data is used. Data has in some cases become a form of currency.[256] Users that check-in to places are often given rewards for their information. These rewards range from digital goods, like badges,[257] to coupons,[258] to physical products like a scoop of gelato.[259] The fact that retailers and businesses are willing to exchange physical goods for information suggests that there is real value in this information. This value sets it apart from something like a phone number or address, which in many cases, is freely accessible to anyone with a phone book; no one pays you for information in the phone book.

Applying the *Katz* test in light of how users treat their location-based information supports moving this class of data outside of the Pen Register Statute. Users possess a subjective expectation of privacy in their location. A user's location is private by default, and it remains so until it is shared. This is in complete contrast to a phone number, which users should understand is public by

---

254 *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502 (S.D.N.Y. 2001) ("DoubleClick creates value for its customers in large part by building detailed profiles of Internet users and using them to target clients' advertisements.").

255 *See infra* notes 265–67 and accompanying text.

256 *See In re* DoubleClick, 154 F. Supp. 2d at 502–03 ("When users visit any of these DoubleClick-affiliated Web sites, a 'cookie' is placed on their hard drives.").

257 *See What is Foursquare?*, FOURSQAURE, https://foursquare.com/about (last visited Sept. 13, 2011) ("By 'checking in' via a smartphone app or SMS, users share their location with friends while collecting points and virtual badges."). For a list of badges, see *The Full List of Foursquare Badges*, 4SQUAREBADGES.COM, http://www.4squarebadges.com/foursquare-badge-list/ (last visited Sept. 13, 2011).

258 *See* Jon Fougner, *Introducing Deals*, FACEBOOK (Jan. 31, 2011, 9:58 AM), http://www.facebook.com/blog.php?post=446183422130.

259 This is just one example of a Foursquare promotion. This one was instituted by Whole Foods and it gave away a physical product. *See, e.g.*, Nick Saint, *Whole Foods Pushing Its Foursquare Promotion Hard*, BUS. INSIDER (Aug. 7, 2010, 12:26 PM), http://www.businessinsider.com/wholefoods-is-pushing-its-foursquare-promotion-hard-2010-8.

default.[260] This fundamental difference affects the way in which users value these different types of information. Users recognize that private information, which definitionally is more difficult to obtain, may be assigned a higher value than public information that is available to everyone. That there is a market for location-based information is proof of this value and further demonstrates the fact that users believe that their information is private until they choose to share it. Furthermore, this expectation of privacy is one that society would likely recognize as reasonable. In this instance, smartphone users benefit from the *Kyllo* standard.[261] Location-based information, unless it is shared, is something that cannot be observed without special technology.[262] Because this technology is not generally available to the public, society would recognize an individual's expectation of privacy in his location as reasonable, at least until it is publicly disclosed.

C. The Consent Exceptions to the ECPA Are Too Broad

Data collectors can always acquire consent to collect user information. Within the *Katz* framework, once a user shares his location with a third party or consents to its capture, he loses any expectation of privacy he previously had.[263] Users that choose to share their location with others recognize, or should recognize, that this is the case.[264] The Internet, however, has changed the way data is transmitted between parties. The current concerns regarding consent are not about how information is being used. Instead, the concerns involve the transfer of information to a third

---

[260] *See* Smith v. Maryland, 442 U.S. 735, 743 (1979) (finding that telephone subscribers cannot "harbor any general expectation that the numbers they dial will remain secret").

[261] *See supra* notes 124–29 and accompanying text.

[262] *See, e.g.*, *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010) ("There are two distinct technological approaches for fixing the location of a cell phone: handset-based (GPS) and network-based (cell site).").

[263] *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." (citing Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927))).

[264] For websites like Foursquare that publicly stream check-ins down their homepage, this assertion is more obvious than it is for closed networks like Facebook in which information may be disclosed to only a limited number of individuals. However the effect on privacy is the same.

party, one to whom the user never provided direct consent and the existence of whom the user may not even be aware.

DoubleClick[265] illustrates the potential problems of transferring consent in this situation. In its decision, the court analyzed the use of cookies, in online advertising. It held that for DoubleClick, an online advertising network, to collect information from a user it needed only to obtain permission from the website that user accessed, and not from the user himself.[266] The court's reasoning was similar to that in the disclosure cases.[267] The court reasoned that the information the user disclosed to the website was analogous to information one discloses to another person during a conversation. Just as the other party to the conversation would be free to tell his friends about anything that was said, a website should be free to disclose any information it receives from a user's visit.[268] Because anything a user knowingly discloses to the public, or in this case a website, is no longer subject to a reasonable expectation of privacy, there is no reason that the website should be prevented from disclosing that information.

However, this is an imperfect analogy. Users never utilized DoubleClick's services voluntarily. Instead, DoubleClick collected user data as it was transmitted to the website. DoubleClick sat between the user and the website as a silent middle man. Users who visited the websites associated with DoubleClick did not know that their information was being collected by anyone other than the site they were visiting. They had never actively granted consent to DoubleClick's collecting their data.

This factual difference was insignificant to the *DoubleClick* court.[269] The court reasoned that because the user had granted permission to the website to collect its information, that website was then free to transfer whatever it collected to a third party. The court explained that if the information being supplied to the website could be freely transferred once the website possessed it,

---

265 *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

266 *Id.* at 510.

267 *See id.* at 510–11.

268 *Id.* at 511.

269 *Id.* at 514.

then the website should be allowed to skip a step and authorize DoubleClick to intercept the transfer and collect the data necessary to supply advertisements.[270] Functionally the end result is the same—DoubleClick gets the user data it needs—but the legal implications are very different.

The court's approval of the DoubleClick model substantially alters how consent functions on the Internet. Traditionally, under the Fourth Amendment, only information that a user knowingly discloses to the public is no longer subject to a reasonable expectation of privacy. After *DoubleClick*, a knowing exchange of information is no longer necessary; the intended recipient of a user's data can grant consent to others to collect that information. This nuance restricts a user's ability to choose the websites with which he wishes to share information.

IV. SOLUTIONS

Courts that are forced to interpret the ECPA are left with a difficult task. They must balance individual privacy with the freedom to use emerging technologies. Fortunately, this conflict can be resolved. Correcting each of the flaws enumerated above will provide substantial progress by creating an ECPA that more accurately reflects the modern use of technology. Some of these solutions are already being implemented. H.R. 5777[271] for instance shows that Congress is starting to recognize the problems that currently surround data collection. However, there is more that can and should be done.

A. Redefine Stored Communication

Congress should modify the ECPA to eliminate the distinction between communications that are stored or in transmission when

---

[270] *Id.*

[271] *See* Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 5777, 111th Cong. (2010). In July 2010, Representative Bobby L. Rush (D. Ill.) introduced legislation "[t]o foster transparency about the commercial use of personal information, provide consumers with meaningful choice about the collection, use, and disclosure of such information, and for other purposes." *Id.*

they are intercepted. Not only is the distinction illogical but it is also unnecessary. As it is now drafted, the plain language of the statute supports the *Szymuszkiewicz* court's reading of mutual inclusion.[272] The term "intercept" is defined as any "acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device."[273] As the court in *Szymuszkiewicz* noted, there is no timing requirement written in the statute.[274] The courts applying the narrow reading of "interception" are using an outdated definition that does not make sense in a modern context.[275] Congress should remove this alternative interpretation so that there is a clear standard to follow.

Clarity is most easily achieved by modifying the ECPA such that (1) the Wiretap Act covers *all* situations where a communication is "intercepted" by an unintended party and (2) Title II, the SCA, specifically only applies to situations where individuals *access* computers or databases they were not supposed to.[276] While this may have been Congress's original intent, the current language is unclear. This change would take the focus off of the status of a communication when it was intercepted, and put it more appropriately on the actual harm that resulted. Congress may have a legitimate reason for keeping the two classes of communication separate; for instance, hacking to retrieve a stored record is a different type of intrusion than real-time monitoring is, and they cause different harms. But, a reformed ECPA need not sacrifice policing one for the sake of the other.

This proposal, based on the *Szymuszkiewicz* court's suggestion that the two titles be allowed to overlap[277] is beneficial because it

---

272 *See* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010).

273 18 U.S.C. § 2510(4) (2006).

274 *See Szymuszkiewicz*, 622 F.3d at 705–06.

275 *See* Konop v. Hawaiian Airlines Inc., 302 F.3d 868, 887 (9th Cir. 2002) (Reinhardt, J., concurring in part, dissenting in part) (noting that courts that follow the narrow definition of "intercept" that requires it be contemporaneous with transmission generally look to a particular case, *United States v. Turk*, which interpreted a different version of the statute, one that existed before the amendments were made to the ECPA to include electronic communications).

276 *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001) ("Title II . . . aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications.").

277 *See Szymuszkiewicz*, 622 F.3d at 705.

helps ensure that the ECPA is flexible enough to accommodate future events. The problem with a mutually exclusive reading, classifying a given communication as either stored or in transmission, is that it ignores the possibility of a situation in which a violation of both titles occurs at the same time. The *Szymuszkiewicz* court illustrates a simple example, the VoIP phone call. For these, the Wiretap Act affords one level of protection while the SCA affords another.[278] A VoIP call, by the nature of its transmission is stored at the time it is transmitted.[279] Allowing instead for a reading that takes advantage of both provisions would bring the statute more in line with how technology currently functions, and produce more consistent results.

New technologies will continue to blur the line between storage and interception. The fingerprinting of digital devices, a rapidly growing business, is one such example.[280] Under the existing statute, it is not clear whether the collection of unique, device-identifying data stored within a computer or mobile phone's memory qualifies as accessing a stored communication or interception of a transmitted piece of data intended for another source. Nothing says it cannot be both. As suggested, a standard that distinguishes between interception and access as classes of intrusion rather than the status of a communication at the time it is intercepted has a better chance of adequately addressing the further harm.

B. Close The Doughnut Hole In The Pen Register Statute

The Pen Register Statute should not apply to location-based information because the extremely low standard of access it provides does not reflect the legitimate expectation of privacy an individual has in his location. Location-based information is different than the types of non-content information the Pen Register Statute was intended to control.[281] The recording of

---

[278] *Id.* at 706.

[279] *Id.*

[280] *See* Julia Angwin & Jennifer Valentino-Devries, *Race is on to "Fingerprint" Phones, PC's*, WALL ST. J., Dec. 1, 2010, at A1, *available at* http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html.

[281] *See Supra* Part II.

location-based information is much more intrusive compared to monitoring the phone numbers an individual dials.[282] Knowing which phone numbers an individual dialed might tell law enforcement who an individual chose to contact, but it will not reveal where he was, or what he was doing when he placed the call.

Cell phone users recognize this distinction and treat the two kinds of information differently. Even assuming that the Supreme Court's position in *Smith v. Maryland*[283] is correct and users do not expect any privacy in the phone numbers they dial, the same assumption cannot be made for location-based information.[284] As already discussed, location-based information is more likely to be viewed as content by the user, and therefore he will also attach an expectation of privacy to that information. Thus, whether it be a check-in on Foursquare or a tagged photograph on Facebook, this content information falls outside the scope of the Pen Register Statute, upon a plain reading of its terms, and courts should not apply additional statutory authority to make it fit.[285]

There are two possible solutions that will close this doughnut hole in the statute. First, Congress could completely remove the "solely pursuant" language and thereby limit the Pen Register Statute to its terms. Alternatively, Congress could specify which statutes it would allow to be used in conjunction with the Pen Register Statute, rather than letting the courts or law enforcement pick and choose the additional statutory authority. Closing the loophole entirely by restricting the Pen Register Statute to its terms is the better option in terms of protecting user privacy. It would bring the statute closer to its original function and allow law enforcement easy access to a certain, limited class of data, data in

---

[282] *See Supra* Part III.B.

[283] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (explaining that phone numbers are subject to less protection because "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial.").

[284] The uproar that occurred when users realized that Apple was storing their location strongly suggests that users do not believe that they have no expectation of privacy in their current location. *See supra* note 9.

[285] *See supra* Part III.B.

which users already have no reasonable expectation of privacy.[286] While it is possible that fixing the stored/in transmission distinction would correct this problem on its own, removing the loophole by moving protection of location-based data from the SCA and to the Wiretap Act is the surest way to ensure consistent results.

C. Require Actual Consent To Each Use

This is one area in which Congress has recognized a problem and taken action. H.R. 5777, introduced into the House on July 19, 2010, requires companies to disclose their purposes for collecting user data[287] and to obtain user consent for the specific access they are seeking.[288] This bill addresses the "transferred consent" problem that was present in the *DoubleClick* case,[289] and attempts to solve the problem by enforcing a standard of disclosure about what is being collected.

However, such a requirement does not address the loopholes that exist in the current regulation.[290] Furthermore, corporations have already found a way to work around the H.R. 5777 requirements—they classify additional information collected as non-content data.[291] This technique stems from the existing statutory language of the Pen Register Statute and follows the rationales of *Smith*[292] and *Miller*.[293] If the information collected by

---

[286] Congress initially drafted the SCA to address only stored communications that were not generally available to the public. *See* S. Rep. No. 99-541, Section 201 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589.

[287] *See* Building Effective Strategies to Promote Responsibility, *supra* note 271.

[288] *See id.* ("In General- Except as provided in subsections (e) and (f) and section 106, it shall be unlawful for a covered entity to collect or use covered information about an individual without the consent of that individual, as set forth in this section.").

[289] *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[290] Building Effective Strategies to Promote Responsibility, *supra* note 271 (explicitly not overruling the ECPA).

[291] *See Foursquare Labs, Inc., Privacy Policy*, FOURSQUARE, http://foursquare.com /legal/privacy (last updated Jan. 12, 2011) ("Information Collected Automatically: When you use the Service, foursquare automatically receives and records information on our server logs from your browser or mobile platform, including your location, IP address, cookie information, and the page you requested. We treat this data as *non-Personal Information*, except where we are required to do otherwise under applicable law." (emphasis added)).

[292] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979).

location-based mobile services is non-content, or is "non-personal"[294] information, then an individual likely has no reasonable expectation of privacy in that data. Once it is disclosed to the location-based mobile service, non-content information would be treated like a business record.[295] As such, these records can then be freely disclosed.[296]

H.R. 5777 does not sufficiently solve the problem of transferred consent. In many ways enforcing a consent requirement hinges on restructuring the ECPA so that a user's location is treated as content information. Content information can be regulated much more heavily than non-content information because individuals have a legitimate expectation that the content of their messages will remain private unless they choose to disclose it.[297] The ECPA provides a clear example of how this distinction currently applies to law enforcement. The Wiretap Act regulates access to content and the Pen Register Statute regulates access to phone numbers, and they create two noticeably different standards.[298]

The distinction between content and non-content information is essential to regulating private businesses as well because it firmly establishes how information should be treated. Content information is more sensitive than non-content information. This difference is recognized by the ECPA, which subjects the two classes of information to separate standards.[299] It is reasonable to ask that companies that collect content data acquire consent to do so, and thereby abide by the ECPA's structure. Because users have the right to assume that their information will not be

---

293 *See* United States v. Miller, 425 U.S. 435, 440 (1976) ("[R]espondent can assert neither ownership nor possession. Instead, these are the business records of the banks.").

294 *See id.*

295 *See id.*

296 *See id*. at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." (citing United States v. White, 401 U.S. 745, 751–52 (1971))).

297 *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

298 *See supra* Part II.

299 *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

disclosed unless they choose to disclose it,[300] users may be willing to consent to giving these companies content information only if certain conditions are met.[301] However, if a user's location is treated as non-content information, then it falls into the same category as a telephone number. With no reasonable expectation of privacy in this non-content information,[302] location-based mobile services do not need to ask for consent or notify the individual about how they are using that data. This process not only mischaracterizes how users view their location-based information, but more importantly, it also distorts how the location-based mobile services collect and use that information.

D. Treat Location-Based Data More Like Property

Location-based mobile data has many of the same characteristics of property. It is fixed when it is in storage, it has a monetary value, and it is sold and traded on a regular basis.[303] Most importantly for the purposes of this Note, it is used as consideration in exchange for goods and services.[304] Privacy regulation should recognize the market exchange that is already taking place between smartphone users and mobile service providers. This relationship is not the same as the one between an Internet user and the ad network that collects information and uses his information to sell advertising. There, the value of user data is derivative—created by the ad network supplying its service, banner ad placement, to other companies. Location-based mobile data, on the other hand, has actual monetary value.[305] Companies encourage users to share their information in exchange for tangible rewards.[306] Whether this is represented by a discount or by free scoops of ice cream, it is clear that the data collectors are willing to compensate users for their information. This indicates that

---

300 *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

301 For example, for safety reasons a user may not want to expose his location to a mobile service that sells or distributes his information.

302 *See supra* Part II.

303 *See* 63C AM. JUR. 2D *Property* § 1 (2011).

304 *See supra* Part III.B.

305 *See supra* Part III.B.

306 *See id.*

location-based user data should be treated differently, and under a different standard.

Treating data as property in a mobile setting would address the shortcomings of the ECPA.[307] The stored/in transmission issue would disappear. A statute that recognizes mobile data as something that resembles property would determine access to that data based on whether one has a legitimate expectation of privacy at the time it is collected. This new standard would not have to rely on artificial determinations of a communication's status at the time of interception, but rather would focus on the collection of data as a type of a seizure. This would create a standard that courts are familiar with applying and one that will be effective and relevant as long as mobile data has value.

Furthermore, there would not be any confusion about whether the Pen Register Statute applies. Conceivably, the public would object to property being classified as non-content information. Such a characterization would run counter to existing intellectual property norms, specifically copyright, which allow users to own the content of their creations.[308] This is not to suggest that user data should be treated to copyright protection,[309] but only suggests that a recognition that user content is property is not a concept that is alien to our legal system.

Lastly, treating user data as property would make it clear that consent is required for third-party access. This logic is more closely related to preventing a misappropriation of value than it is in trespass.[310] The changes to Foursquare's privacy policy,[311] highlight the need for this value analysis. If user information is capable of being exchanged for something, it should be exchanged at the user's discretion. An outside third party with an interest in

---

307 *See supra* Part III.

308 17 U.S.C. §§ 102, 106 (2006).

309 *See* Feist Publ'ns Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 359–60 (1991) (holding that copyright protection applies only to the portions of data compilations that are original to the author and not to mere facts).

310 *See* Michael A. Carrier, *Against Cyberproperty*, 22 BERKELEY TECH. L.J. 1485, 1486 (2007) (arguing against creating a right to exclude users from making electronic contact to their network as one that exceeds traditional property notions).

311 *See supra* note 87 and accompanying text.

collecting that information for free should not be allowed to decide that it has no value. The value of information should be decided by negotiations between the two parties. Some academics fear that any negotiation process would require a complex market for data exchange.[312] This fear, however, is misplaced as informal negotiations already happen on a daily basis.[313] When users decide that checking-in and sharing their information with Whole Foods is worth the scoop of gelato offered in exchange, they are determining the market value of their data.[314] With the right information available, and H.R. 5777 suggests it will be in the future, users can make more informed choices about what their information is worth and can choose to share it with those companies that they feel adequately represent that value.

A conception of mobile privacy that is built on property rights also correctly accounts for the harm created by the secondary uses of data. Almost ten years ago, *DoubleClick* illustrated the dangers associated with information being sold, collected, and aggregated by one party.[315] Following its billion-dollar acquisition of consumer records, DoubleClick was in position to compile a database that accounted for and tracked approximately 90 percent of the American public.[316] Similar efforts today are even more advanced.[317] Users can be tracked not just by their habits but also by the unique "fingerprint" their device leaves behind wherever they go. Companies need to be forced to disclose what they are collecting information for and where that information is going, beyond their own servers. This argument is again grounded in a property value-based analysis of personal data. Misrepresenting contract terms is prohibited, and it follows that misrepresenting the terms of an information exchange should also be prohibited. Information is a valuable asset and, as with any transaction, the

312 *See* Carrier, *supra* note 310.

313 *See* Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1136 (2000) (arguing that an institutional market infrastructure would not be necessary to make new property rights in personal information work).

314 *See supra* Part III.B.

315 *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 505 (S.D.N.Y. 2001).

316 *Id.*

317 *See* Angwin & Valentino-Devries, *supra* note 216.

risks associated with that transaction change its value. Consumers are unable to accurately value the information they are agreeing to supply when they lack accurate information as to how his information will be used. Perhaps a check-in at Whole Foods is worth more than a scoop of gelato. Without an accurate representation of the risk associated with that disclosure, the consumer is at a much greater risk of making an unfair deal.[318]

CONCLUSION

Changes in how users are sharing data have created a need to update the existing regulations. While proposed legislation currently in committee addresses some of the issues, it does not go far enough to close the current loopholes and mischaracterizations that threaten mobile user privacy. In addition to adopting a new set of standards regulating data collection, flaws in the ECPA need to be addressed. By mirroring how users and the industry value information, the statute could be amended and the current gaps in the regulation could be closed.

[318] H.R. 5777 makes significant progress in this area, particularly through a provision that allows the FTC to enforce fair commercial practices in data collection. *See* Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 5777, 111th Cong. §§ 601–03 (2010).