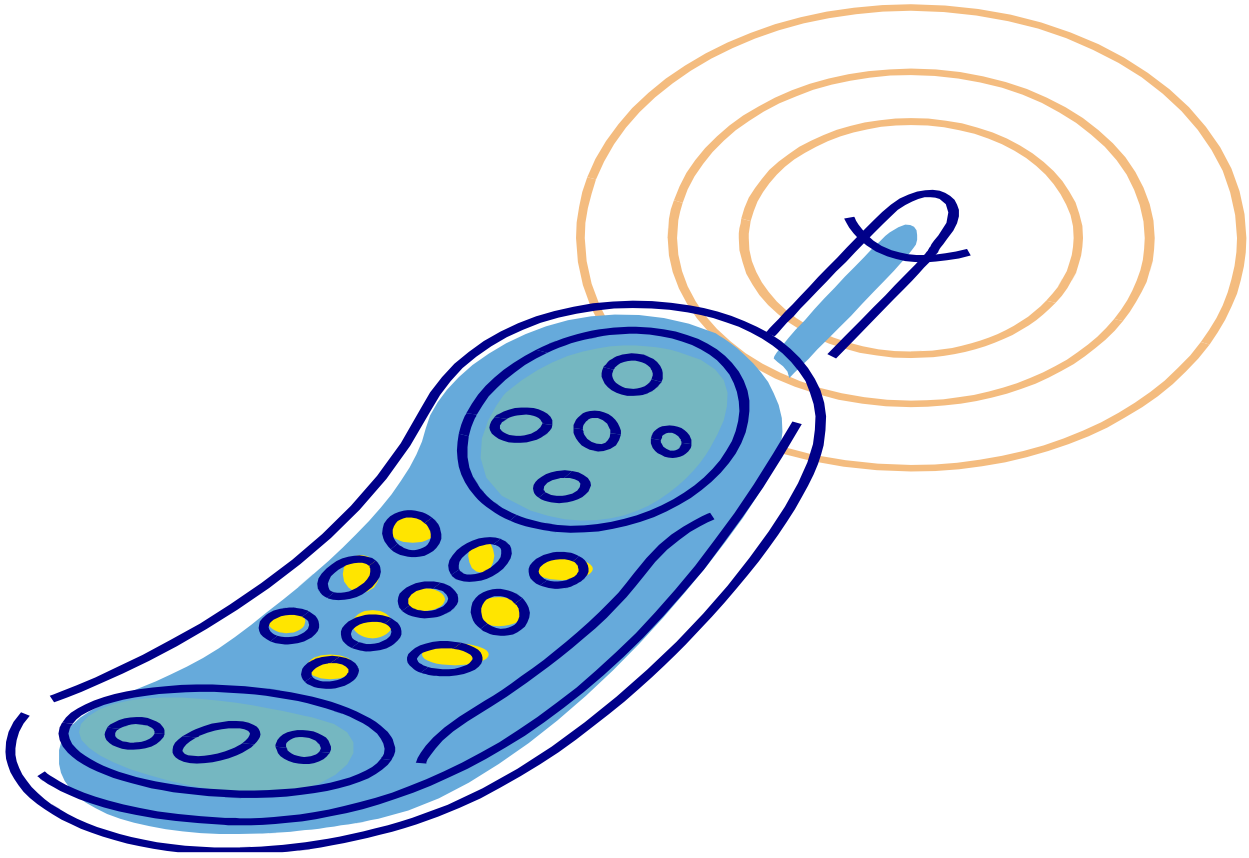
Cell Phone Location Data



Senate Judiciary Committee

2012 Interim

Brief Summary

Cell phone technology, in particular smartphone technology, is developing rapidly and it is now possible to locate cell phones to within a few feet whenever they are turned on. Some believe that cell phone location tracking is more intrusive that GPS tracking of vehicles because users typically carry their cell phones on their person. After the U.S. Supreme Court found that installation of a GPS device constitutes a search, law enforcement appears to be shifting toward cell-site location data that can be obtained without a warrant under federal law.

The seminal question is whether cell phone users have a reasonable expectation of privacy in their historical and current location data collected by their cell phone service providers in the regular course of business. Currently under federal law, law enforcement can gain access to historical cell phone location records with a summons sent to the individual's cell phone service provider. The analysis in Washington will differ because of the greater expectation of privacy provided by Article 1, section 7 of the Washington State Constitution. *Currently, Washington prosecuting attorneys are advising law enforcement to obtain search warrants before requesting cell phone location data from service providers.*

There are three issues upon which future court decisions are likely to turn. First, is a cell phone a communication device or a tracking device? Obviously, they are communications devices, but they are increasingly being used as tracking devices as well. In fact, they are routinely used as tracking devices by law enforcement and emergency personnel to locate missing persons or those requiring assistance; by parents keeping track of their children; and by vendors who want to target potential customers near their establishments.

Second, how accurately can a person's location be tracked? This is a developing technology. If the cell phone user has enabled the internal GPS, the accuracy of the cell phone's location can be established quite accurately. Even if the GPS has not been enabled, the location can increasingly be triangulated using cell towers. This information is often updated as often as every 7 seconds. Recent court decisions appear to be focusing on the accuracy of the location information, the frequency of the information, and the duration of the tracking.

Finally, do customers waive the privacy of their location information when they acquiesce to service agreements that include clauses authorizing the service providers to acquire and record the information? While the agreements typically say that the information is confidential and used only for limited purposes, the federal law currently allows law enforcement to obtain these records without a warrant. Some courts have questioned the scope of this consent and whether it is truly knowingly given.

This is a confusing area of law and the landscape is changing, both in terms of technology and people's expectation of privacy. The federal courts have issued conflicting opinions on these matters and the Washington Supreme Court has yet to weigh in. Washington statutes do not specifically address the issue. There are currently at least two federal cases, addressing the three issues identified above, which are in the process of being appealed to the United States Supreme Court.

Discussion

Cell Phone Technology

The smartphone, a cell phone with PC-like functionality, has made it possible for users to turn their current location into a useful tool for emergency response, traveling, locating services, and obtaining discounts at close by businesses. Smartphone applications, called location-based mobile services (LBMS), are designed to facilitate this functionality. LBMSs are third-party applications commonly known as "apps". Smartphone users download these apps from the Internet and install them onto their devices using a process similar to downloading and installing software onto a computer. Once installed, the app uses a person's current location to perform useful functions for consumers.

Just like any other piece of software, installing an app requires that users agree to certain conditions. 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. Once an app is loaded on to a user's device it often has access to a wealth of information beyond what a user manually provides - particularly with regard to location-based information.

One class of app facilitates a user's choice to share his current location with others. How each application achieves this goal varies. For example, some "check in" applications encourage users to share their location with friends by "checking in" at a specific place. This "check-in" often links to other social networks and rewards users for their continued participation. 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. Unlike the "check in" model which broadcasts a message to a user's existing network, these apps display users' location on a map to friends they select from their existing contact list. Other mobile apps mimic this mapping function and combine it with additional features.

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"); (2) using the user's unique Cell-ID; (3) tracking the user's Internet connection to Wi-Fi; and (4) allowing users to specify their current location. Since the fourth option is user-controlled, only releasing location information specified by the user, this memo will focus exclusively on the first three methods.

GPS is usually the most accurate way to determine a user's location. GPS locates each user through a process called trilateration, which uses twenty-seven satellites to plot the intersection of at least three spheres drawn around the user and the three satellites to determine his exact position on the ground. Even traditional cell phones, without internet capabilities, include GPS technology to comply with federal regulations requiring them to pinpoint locations during emergency calls[1]. Although extremely accurate, GPS has limitations. It is slow, and can sometimes take minutes to return a result; it is processor-intensive and can quickly drain a phone's battery; and it is most effective when the user is outdoors or in open areas.

The Cell-ID method is less accurate than GPS, but more versatile. This process uses a carrier's cell network, not satellites, to determine a user's location. Every cell phone on a given network is assigned a unique identification number. When a user's phone is on, that phone will connect to the nearest cell tower to establish a connection (referred to as "registration"). These registrations may occur as frequently as every 7 seconds, depending upon the provider and signal strength.[2] The more frequent the registrations, the more accurate the cell phone's location can be determined. Registration data is generated

[1] 47 CFR §20.18 (2009).
[2] Thomas Farely & Ken Schmidt, *Cellular Telephone Basics: Registration - Hello World!*, Private Line (January 1, 2006).

whether or not a call is being made[3], but can be disabled (although when disabled, the cell phone cannot be used).[4]

By searching for a specific ID number it is possible to identify the tower to which a given device is connected. There are now over 251,000 reported cell sites in the United States[5]. As the density of cell phone users in an area continues to grow, the only way for a carrier to accommodate the increased number of customers is to divide that area into smaller and smaller sectors. The smaller a sector is or the more towers there are, the more accurately an individual can be located.

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. A user within range of multiple towers can be located using triangulation. The process is similar to the trilateration method used by GPS. 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. Urban areas, generally, have more dense cell tower coverage enabling more accurate location information - approaching the accuracy of GPS location.

Wi-Fi geolocation has been available since at least 2008. The Wi-Fi method of geolocation uses various location-based clues to determine the location from which a user is currently accessing the web. 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. By collecting and storing this information, namely the MAC addresses of other Wi-Fi networks, the W3C API can build a profile for each location. As more information is gathered, it is possible to pinpoint a user's location at any given time. LBMS do more than collect location-based data. Each app that users choose to install on their smartphones can access different information stored on that device. This access, however, is never unlimited. The level of access granted to each application is determined by a set of controls called "permissions." Applications do not have access to any user information by default, and can only access whatever the "permissions" allow them to. These restraints can be defined either at the installation of the application or later on throughout the use of the application by user prompts. The type of permission required depends on the information being sought by the application and varies according to the phone's operating system.

Permissions are important because a user-defined permission is evidence that a user consents to the application accessing that data. In an attempt to gain permission most privacy policies inform users about the type of information collected and the purpose for collecting that information. 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 and being broad enough to avoid ruling out specific information. 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." As the scope of "improving the content of the Service" is never defined, any usage could conceivably fall within that category.

---

[3] Susan Friewald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact,* Maryland Law Review, Vol. 70 (2011).

[4] Wayne Jansen & Rick Ayers, Nat'l Inst. of Standards and Tech., *Guidelines on Cell Phone Forensics: Recommendations of the Nat'l Inst. Of Standards and Tech.,* 63 (2007).

[5] *In re Application of the United States of America for Historical Cell Site Data,* 747 F.Supp.2d 827 (S.D. Texas 2010) (Finding of Fact No. 21.) (holding that the Fourth Amendment demands a higher standard of proof than specific articulable facts); pending appeal to Fifth Circuit United States Court of Appeals (December 12, 2012).

Most location data is obtained from the process of providing wireless voice and data services, or due to users calling 911 or using a location-enabled app on their smartphones. For such information, law enforcement agencies can either request historical data already stored by the provider, or request prospective surveillance that will provide data to the law enforcement agency as soon as the carrier receives it. In either case, the information collection is passive, in that no new data is generated due to the law enforcement surveillance request.

It is also possible, however, for carriers to monitor their customers actively, generating new data specifically in response to a request from law enforcement agencies. In such scenarios, the wireless carriers can covertly "ping" a subscriber's phone in order to locate them when a call is not being made. Such pings can merely reveal the nearest cell site to the subscriber, or more accurate GPS or triangulated data if requested. In addition to the carrier-initiated pings, law enforcement agencies have also performed "low tech" pings by calling a target and hanging up before the phone rings, in order to generate cell site data that can then be requested from the carriers.

United States Constitution: Fourth Amendment

The primary source of privacy in the United States is the Fourth Amendment, which ensures that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...."[6]
In 1928, when police eavesdropped on the telephone conversations of Roy Olmstead and his bootlegging conspirators, the Court refused to label this a violation of the Constitution because the police had not physically trespassed on the defendants' properties in making the wiretaps.[7] The Fourth Amendment protected a person's property interest, the Court held, not abstract things like his own voice. Also, the channel of communication, the telephone wires, extended beyond the defendant's home to the "whole world"—well beyond Olmstead's property interest. Almost 40 years later the Court changed course, radically altering the constitutional contours of protected privacy by determining that "the Fourth Amendment protects people, not places."[8]

In *Katz*, the FBI eavesdropped on Katz's conversation with an electronic device after he had closed himself inside of a telephone booth. The Court found that act of closing himself in a booth indicated Katz's desire for privacy, and that the FBI had overstepped its authority when it listened to the contents of his conversation without a warrant.

The Court developed a new standard—the *reasonable expectation of privacy*—to determine whether an act by the government constitutes a search, thereby triggering a Fourth Amendment analysis. If a person has "exhibited a subjective expectation of privacy" and it is one "that society is prepared to recognize as 'reasonable'", then a search has occurred, and the court will determine whether there was a warrant or whether an exception to the warrant requirement applied. If, on the other hand, there was no reasonable expectation of privacy, a warrantless search does not offend the Fourth Amendment.

Although *Katz* established that the contents of a conversation are accorded constitutional protection, the Court did not extend this protection to information generated in making the communication. In *Smith v.*

[6] U.S. Constitution, Amendment IV.

[7] *Olmstead v. United States*, 277 U.S. 438, 478 (1928).

[8] *Katz v. United States*, 389 U.S. 347, 351 (1967).

Maryland[9], the Court held that a person does not have a reasonable expectation of privacy in the telephone numbers he dials. Michael Lee Smith was a thief who robbed a young woman and then harassed her with obscene phone calls. The police used a pen register (without a warrant) to record the numbers dialed from Smith's office. Based on the numbers he dialed, the police determined that Smith was calling the young woman. In concluding that a search had not occurred, the Court reiterated that a person has no legitimate expectation of privacy in information voluntarily given to third parties—in this case, dialed numbers to the phone carrier.

At least some cell phone providers have provisions in their terms and conditions stating that they may disclose location information to governmental agencies without the users consent. Some recent trial court decisions have questioned whether the terms and conditions constitute valid informed consent given the plethora of verbiage in the documents and their small print.

The Sixth Circuit Court of Appeals found that government agents violated a defendant's Fourth Amendment rights when they compelled an internet service provider (ISP) to disclose the content of emails without obtaining a warrant[10]. Maynard had used questionable marketing practices to sell Enzyte and much of the proof was in the 27,000 emails in the possession of the ISP. The case is notable because the information was in possession of a third party. The evidence was ultimately admitted at trial and upheld because the government agents relied in good faith on the provisions of the Stored Communications Act (discussed below). On the other hand, in *United States v. Miller*[11], the U.S. Supreme Court rejected a Fourth Amendment challenge to a third-party subpoena for bank records, reasoning that the bank's records were not the respondent's private papers, but rather the business records of the bank. The court held 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."[12] A number of district courts have rejected Fourth Amendment challenges relying on *Smith* and *Miller*[13], while others have not[14].

In *U.S. V. Jones*[15], the Supreme Court held that the government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search requiring a warrant. The holding was drafted quite narrowly, however, involving the issue of installation. Justice

[9] *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979).
[10] *United States v. Warshak*, 631 F.3d 266 (2010).
[11] 425 U.S. 435 (1976).
[12] Id. At 443; see also,
[13] *United States v. Dye*, WL 159255 (N.D. Ohio, 2011); *United State v. Velasquez*, WL 4286276 (N.D. Cal., 2010); *United States v. Benford*, WL1266507 (N.D. Ind., 2010); *United States v. Suarez-Blanca*, WL 4200156 (N.D. Ga., 2008); *Mitchell v. State*, 25 So.3d 632 (Fla. Dist. Ct. App. 2009).
[14] *In re Application of United States*, 620 F.3d 304 (3rd Cir. 2010) (location information is not voluntarily conveyed, but historical cell-site records obtainable without traditional probable cause determination under § 2703(d)); *In re Application of United States*, ___ F.Supp 2d ___ WL 3678934 (E.D.N.Y. 2011) (warrant required to compel disclosure of cell-site records.)
[15] *United States v. Jones*, 565 U.S. ___ (2012); see also *United States v. Maynard*, 615 F.3d 544 (D.C. Cir., 2010) (defendant has a reasonable expectation of privacy in "the totality and pattern of his movements from place to place to place.").

Scalia was careful to emphasize that "situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[16] The question of electronic surveillance without an accompanying trespass was left for another day. Justice Sotomayor, in a concurring opinion, stated that:

> I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through conventional surveillance techniques.

United States v. Jones, Id. , Justice Sotomayor, concurring.

While granting police wide latitude for searches occurring in public, the Court remains attentive of privacy in the home. In *Karo v. United States*, the Court held that monitoring the presence of an item in a private residence through the use of a beeper violated the Fourth Amendment rights of the residents, absent a valid warrant[17]. Likewise, when police, without a warrant, used thermal imaging on Danny Kyllo's home to determine if he was using high-intensity heat lamps (usually an indication of growing marijuana), the Court again protected the sanctity of the home, holding that information on activities within a home derived through sense enhancing technology outside of it was obtained in violation of the Fourth Amendment[18].

The duration of surveillance has also been a significant factor cited by the courts. For example, in *United States v. Knotts*[19], the U.S. Supreme Court held that a person has no reasonable expectation of privacy in movements from one place to another (a beeper had been placed in a container as it was driven 100 miles over public roads). The *Knotts* court expressly reserved the question over whether a warrant would have been required for a longer period of surveillance[20]. Warrantless access to historical cell site data was denied in *United States v. Maynard*[21] when the tracking was not limited to a single trip, but covered movements 24 hours a day for 28 days. The court found that the whole of a person's movements over the course of a month was not actually exposed to the public because the likelihood a stranger would observe all those movements was not just remote, it was essentially nil. The court concluded that an individual has a legitimate expectation of privacy regarding the "intimate picture of his life" revealed by prolonged surveillance.

The United States Constitution, however, is a floor, not a ceiling. Federal law (and state constitutions and statutes) can provide more protection than the Constitution requires, but no less.

[16] *Id*.
[17] *United States v. Karo*, 468 U.S. 705, 718 (1984) (upholding introduction of evidence found during search that was based in part on impermissible beeper monitoring; warrant was independently sustainable by additional information).
[18] *Kyllo v. United States*, 533 U.S. 27 (2001).
[19] 460 U.S. 276 (1983).
[20] Id. at 283-84.
[21] 615 F.3d 544 (D.C. Cir. 2010).

There are several comprehensive federal statutes (discussed below) that regulate the use of electronic surveillance—in some instances Congress has seen fit to provide more protection than the constitutional floor, while in others it has not.

Washington State Constitutuion: Article 1 Section 7 Right to Privacy

Article I, section 7 of the Constitution of Washington State provides that : "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."[22] *State v. Gunwall* describes six nonexclusive criteria for determining whether, in a given situation, the state constitution extends broader rights to its citizens than does the United States constitution[23]. Those criteria are: (1) the textual language of the state constitution; (2) significant differences in the texts of parallel provisions of the federal and state constitutions; (3) state constitutional and common law history; (4) preexisting state law; (5) differences in structure between the federal and state constitutions; and (6) whether the matter is of particular state interest or local concern.

Once the court has recognized broader rights in a state constitutional provision, a *Gunwall* analysis is not needed[24]. It is now settled that article I, section 7 is more protective than the Fourth Amendment, and a *Gunwall* analysis is no longer necessary[25]. The inquiry under article I, section 7 is broader than under the Fourth Amendment to the United States Constitution, and focuses on "those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass."[26] The state constitutional analysis precludes a purely "protected places" analysis in favor of the protection of a person in his or her private affairs[27]. "This language prohibits not only unreasonable searches, but also provides no quarter for ones which, in the context of the Fourth Amendment, would be deemed reasonable searches and thus constitutional."[28] Article I, section 7 thus creates "an almost absolute bar to warrantless arrests, searches, and seizures, with only limited exceptions .... "[29]

Whether advanced technology leads to diminished subjective expectations of privacy does not resolve whether use of that technology without a warrant violates article I, section 7[30]. In *Jackson*, it was determined that having a GPS device on a car for 2 weeks provided information that couldn't feasibly be attained from simply following the cars around. Also the GPS device was not just a sense augmenter, because it gave information about the history of the cars locations, compared to binoculars which simply enhanced the officer's vision at one instant. The Court also found that the GPS device was an intrusion to private affairs. "In this age vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles. The GPS tracking devices record all of these travels, and thus can provide a

[22] Const. art. I, § 7.
[23] 106 Wash.2d 54, 720 P.2d 808 (1986) (state constitution requires search warrant for pen register.).
[24] *State v. Jackson*, 150 W.2d 251 (2003) (Holding that a warrant is required before attaching a GPS device to a vehicle to track the driver's movements).
[25] *State v. Vrieling*, 144 Wash.2d 489, 495, 28 P.3d 762 (2001) (citing *State v. Gunwall*, 106 Wash.2d 54, 720 P.2d 808 (1986)).
[26] *State v. Myrick*, 102 Wash.2d 506, 511, 688 P.2d 151 (1984).
[27] Id. at 513.
[28] *State v. Valdez*, 167 Wn.2d 761, 772,224 P.3d 751 (2009).
[29] *Id.* (quoting *State v. Ringer*, 100 Wn.2d 686, 690, 674 P.2d 1240 (1983).
[30] *Id.*; *State v. Young*, 123 Wash.2d 173, 181-82, 867 P.2d 593 (1994).

detailed picture of one's life." In this case, a valid warrant authorizing the GPS device had been obtained by law enforcement.

The *Jackson* case involved a GPS device specifically installed on a vehicle by law enforcement to track its movements. When a person owns a smartphone with GPS enabled or through the use of cell-ID location, law enforcement does not need to place a separate device to track the phone, they can obtain tracking information directly from the service provider. The unanswered question in Washington is whether law enforcement should be able to obtain this information without a warrant.

Applicable Federal Law

Currently there is no statute specifically regulating access to user data. Instead this information is governed by statutes regulating electronic communication such as the Electronic Communications Privacy Act (ECPA)[31]. The ECPA was enacted to extend the protections of the Federal Wiretap Act[32] to electronic communications. It addresses three types of conduct: the intercepting of live communication, the accessing of stored communications, and the recording of "non-content" information. 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 ("SCA"), which deals exclusively with access to communications in storage[33]; and Title III - Pen Registers and Trap and Trace Devices ("the Pen Register Statute"), which sets limitations on the access to non-content information[34]. Each ECPA title has its own standard that controls access to communications within that class.

Title I, modifying the Federal Wiretap Act, requires that the government obtain a warrant, upon a showing of probable cause that the information to be seized is evidence of a crime[35]. 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."[36] 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."[37] Under this three-part 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.

Since only "reasonable" expectations of privacy will be honored, for information to receive protection it must meet this threshold. Most communications can be broken down into component parts, each of which must be addressed separately within the reasonable

[31] Electronic Communications Privacy Act of 1986, P.L. 99-508.

[32] 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).*

[33] 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)).

[34] 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)).

[35] 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).

[36] 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., supra* at 304.

[37] 18 U.S.C. § 3122(b)(2) (2006).

expectation of privacy analysis. For example, a landline phone call can be split into two pieces, the number dialed and the following conversation. The ECPA treats the phone number and conversation differently. The phone number receives very little protection. However, 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[38] compared to the lesser "certification" standard that law enforcement needs to access a phone number under Title III[39].

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[40]. 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 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.

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[41]. Society's expectation of privacy may be higher when dealing with a new technology that is not generally available to the public. The Supreme Court has addressed a range of new technologies over time, from aerial mapping cameras to thermal imaging devices. 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.

This analysis also goes 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. This "method of surveillance" standard, as applied to modern technology, is derived from *Kyllo v. United States*[42]. In *Kyllo*, law enforcement used a thermal imaging device to observe the relative heat levels inside a house. While the information they collected, thermal radiation, was publicly available, the technology they used was not. The Court focused 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. The significance of *Kyllo* is that the use of technology during surveillance may weaken or reverse the effect of public disclosure under the *Katz* analysis.

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. In determining the nature of a given communication there are three remaining 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)

[38] 18 U.S.C. § 2516 (2006).
[39] 18 U.S.C. § 3122(b)(2) (2006).
[40] *Katz v. United States,* 389 U.S. 347 (1967) 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.").
[41] See *California v. Ciraolo, 476 U.S. 207, 212 (1986)* ("The 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 the Fourth Amendment." (quoting *Oliver v. United States, 466 U.S. 170 (1984))*.
[42] *Kyllo v. United States,* 533 U.S. 27 (2001).

is there an exception provided for by the statute[43]?

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[44] while Title II deals only with stored communications[45]. Many courts, including the 9th Circuit Court of Appeals, find that Title I and Title II of the ECPA are mutually exclusive[46]. These courts focus on the distinction between "interception" and "access," and find that it is impossible for an electronic communication to violate both provisions. 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. Similarly, these courts also apply a narrow definition of "interception" and find that the Federal Wiretap Act covers only electronic communications that are acquired contemporaneously with their transmission. 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.

The Seventh Circuit Court of Appeals, has rejected this interpretation of the statute[47]. 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. Szymuszkiewicz was charged under the Wiretap Act for illegally intercepting his boss's e-mails. Szymuszkiewicz contested the charge as a matter of timing, arguing that interception must be defined narrowly to mean "contemporaneous with transmission." 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. 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. The court rejected this interpretation for two reasons.

First, the plain language of the statute provides no timing requirement for interception. The court's second reason focused on the differences between the transmission of electronic and wire communications. The court reasoned that because of technological differences, it would be impossible to apply a timing requirement because interception could never take place contemporaneously with transmission because there is no continuous connection between the two ends of an electronic communication. 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.

Classifying something as non-content data can move the information to falling under Title III of

[43] Christian Levis, *Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy,* 22 Fordham Intell. Prop. Media & Ent. L.J. 191(2011).

[44] Electronic Communications Privacy Act of 1986, P.L. 99-508.

[45] 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").

[46] *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).

[47] *United States v. Szymuszkiewicz,* 622 F.3d 701 (7th Cir. 2010).

the ECPA[48]. 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[49]. 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.

Courts have recently applied Title III to location-based information. In the past, the Pen Register Statute only controlled access to phone numbers. However, in 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act)[50] expanded the statutory definition of a pen register device[51]. This new definition made it possible to record non-content information sent as part of an electronic or wire communication. 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.

[48] 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").

[49] 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.").

[50] 18 U.S.C. § 3121.

[51] *1*8 U.S.C. § 3127(3) (2006).

The Communications Assistance for Law Enforcement Act ("CALEA"), however, expressly limits law enforcement access to location-based information[52]. 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)."[53] 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[54]. Some courts have relied on the SCA for this additional authority[55]. Users automatically disclose their location to the cell phone company every time they turn on their phones. Once a phone connects to a tower the cell phone company knows that user's location. 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, 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

[52] 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.).

[53] 47 U.S.C. § 1002(a)(2) (2006).

[54] 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; 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).

[55] See Id., 460 F. Supp. 2d at 452-53.

reading of interception that was rejected by the *Szymuszkiewicz* court. 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[56]. As the SCA applies to communications in temporary storage[57], location-based information falls within its reach.

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. Unlike the Wiretap Act and the Pen Register 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. 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.

It is currently unclear where location-based information falls within Title III. If the SCA applies 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.

[56] 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).
[57] 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").

Even if a piece of information falls perfectly within the reach of one of the three titles, it may not be protected. There are a handful of exceptions to the statute, available to private parties and the government, which allow for the disclosure of intercepted information[58]. Some of these exceptions are granted to allow for the day-to-day operation of the telecommunication industry. Keeping in mind that individuals can reasonably expect the content of a phone 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. This exception protects phone companies, that provide a valuable service, from lawsuits related to activity necessary to carry on everyday operations, while allowing 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[59]. Once a communication is made public, an individual has no expectation that this communication will remain private. The ECPA recognizes this change in privacy and removes public information from the scope of its protection.

The most salient exception to the ECPA, at least for the purposes of this memorandum, allows for the disclosure of a communication if one party has consented to it[60]. The ECPA removes from the scope of its protection information for which: (1) the observer was a "party" to the communication; and (2) one of the parties has given consent to its interception. This mirrors the

[58] 18 U.S.C. § 2511(2)(a)(ii).
[59] Id. § 2511(2)(g).
[60] Id. § 2511(2)(d).

Katz analysis - information disclosed to another party is subject to a lower expectation of privacy after consenting to the interception.

Technology has significantly 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 be considered a form of consent. However, unlike disclosing a secret to a friend or filling out a survey, in a digital world it is not always obvious what the user is consenting to and when that consent begins and ends. Data collection on the Internet and on a mobile phone may occur without a user ever knowing it. Many websites for example use a small file called a "cookie" to collect information about those who visit their site. A cookie can "store information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner." They can also be used to store and report information from a user's browsing history to a third party. In this situation, a user may believe that the information stored is private (when a person stores their password, do they intend to make the password publically available?).

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[61]. The website and the ad network often 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 network is effectively collecting data using a cookie that the website, and not the web user, gave it permission to install. If the user consented to the website's collection of his information, which arguably he did by visiting the site[62], then the website can authorize the third party ad network to use it.

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[63] (for example law enforcement). This exception 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."[64] 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[65]. It is not enough to simply prove that the defendant committed a tort or crime - in this case a privacy violation. To obtain relief, a user must prove that the ad network collected his data because it wanted to commit a bad act.

State Laws and Legislation

A number of states have statutes or have attempted to regulate the disclosure of geolocation information. Washington does not have any specific statutes in regard to law

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

[62] 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.").

[63] 18 U.S.C. § 2511(2)(g)(i) (2006).

[64] See 18 U.S.C. § 2511(2)(d).

[65] 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)).

enforcement access to cell tower or GPS location based upon cellular phone records.

Washington

RCW 9.73.260 governs the installation and use of pen registers[66] and trap and trace devices[67] in Washington[68]. Neither device is capable of recording the contents of a communication[69]. Neither device may be used without a prior court order issued under the procedures identified in the statute[70]. Failure to obtain a court order prior to the installation of the devices is a gross misdemeanor. The exclusionary rule would also apply, precluding the admissibility any obtained information.

The statute excludes "any communication from a tracking device"[71]. Smartphones are primarily communication devices, but have they also effectively become tracking devices? Law enforcement and emergency services use them to locate people in distress. Users often use them as GPS to locate destinations. The twist is that law enforcement does not have to install any equipment to begin tracking anyone, the subjects voluntarily purchase, maintain, and carry the very equipment used to track their own movements.

The Southern District of Texas found unpersuasive the government's stance that the SCA applied to its request for prospective or real-time cell location information[72]. The analysis begins with the definition of tracking device: the government argued that cell location information did not fit the definition of tracking device -"an electronic or mechanical device which permits the tracking of the movement of a person or [object]"- since it did not provide detailed location information[73]. With the advance in cell phone technology, the court found this argument wanting, as tracking was becoming very precise, and further because the definition of tracking device does not differentiate between general and specific vicinity tracking.

Holding that a cell phone falls into the definition of "tracking device," the court then analyzed each major section of ECPA to determine if any of the sections apply to cell location information. The court dismissed this information as obtainable under the Pen Register Statute, noting that Congress explicitly prohibited law enforcement from obtaining any location information under this statute[74]. The court eliminated the SCA based on the definitions used in that act. First, the SCA must apply to an "electronic communication service." "Electronic communication service," in turn, is defined as "any service which provides to users thereof

[66] A pen register is a device that records the numbers dialed from an identified telephone.
[67] A trap and trace device records the number of the telephone that made a call to an identified telephone.
[68] Washington State Privacy Act, Chapter 9.73 RCW.
[69] The interception and recording of private communications is also governed by Chapter 9.73 RCW and also requires court approval under different sections. This memorandum addresses location data, not content.
[70] RCW 9.73.260 (3) to (6); see also *State v., Gunwall,* 106 Wn.2d 54 (1986).
[71] RCW 9.73.260(1)(b)(iii) mirroring the exclusion in the SCA..

[72] *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F.Supp.2d 747 (S.D. Texas 2005) (noting that historical cell location, as compared to prospective information, fits the definition of transactional records covered by the SCA).
[73] *Id.* (citing 18 U.S.C. §3117(b) (2006)).
[74] Id. At 757-58 ("With regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . .such call identifying information **shall not include any information that may disclose the physical location of the subscriber** (except to the extent that the location may be determined from the telephone number).") (emphasis in original) (quoting 47 U.S.C. §1002(a)(2)).

the ability to send or receive wire or electronic communications[75]." This location information cannot be from an electronic communication, the court concluded, as the definition specifically excludes "tracking devices." It also cannot be a "wire communication" because a wire communication involves the "human voice." Based on this logical sequence of interlocking definitions, the court held that the SCA did not apply, and that the traditional warrant would be necessary. This analysis by the Southern District of Texas has been followed in a majority of jurisdictions.

Alabama

In 2012, the Alabama legislature passed HB 81[76]. The federal law standards for access to stored wire and electronic communications and transactional records were adopted. Federal standards were also adopted for authorization disclosure of call-identifying, addressing, routing, or signaling information that may disclose the physical location of a subscriber, customer, or user of a wire or electronic communications service.

California

Existing California law authorizes a court or magistrate to issue a warrant for the search of a place and the seizure of property or things identified in the warrant where there is probable cause to believe that specified grounds exist. It also provides for a warrant procedure for the acquisition of stored communications in the possession of a provider of electronic communication service or a remote computing service.

California is currently considering SB 1434[77]. This bill would prohibit a government entity from obtaining the location information of an electronic device without a warrant issued by a duly authorized magistrate unless certain exceptions apply, including in an emergency or when requested by the owner of the device. The bill would also prohibit the use of information obtained in violation of these provisions from being used in a civil or administrative hearing. The bill would require a provider to prepare and publish a report containing specified information relating to requests for location information on the Internet, in a searchable format, on or before March 1 of each year. Cell phone companies object to the reporting provisions, arguing that it is too burdensome.

Connecticut

In Connecticut, General Code § 16-247u[78] protects telephone records, defined as information retained by a telephone company that relates to a telephone number dialed by a customer or another person using the customer's telephone with such customer's permission, or the incoming number of a call directed to a customer or another person using the customer's telephone with such customer's permission, or other data related to such call typically contained on a customer's telephone bill, including, but not limited to, the time the call started and ended, the duration of the call, the time the call was made and any charges applied. A telephone record does not include information collected and retained by or on behalf of a customer utilizing caller identification or similar technology.

The law prohibits any person from: (1) Knowingly procuring, attempting to procure,

[75] 18 U.S.C. §2510(15).
[76] http://legiscan.com/gaits/text/645149
[77] http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1401-1450/sb_1434_bill_20120409_amended_sen_v98.html
[78] http://www.cga.ct.gov/2011/pub/chap283.htm#Sec16-247u.htm

soliciting or conspiring with another to procure a telephone record of any resident of this state without the authorization of the customer to whom the record pertains, (2) knowingly selling or attempting to sell a telephone record of any resident of this state without the authorization of the customer to whom the record pertains, or (3) receiving a telephone record of any resident of this state with the knowledge such record was been obtained without the authorization of the customer to whom the record pertained or by fraudulent, deceptive or false means. The provisions do not apply to any person acting pursuant to a valid court order, warrant or subpoena and are not construed to prevent any action by a law enforcement agency, or any officer, employee or agent of such agency, to obtain telephone records in connection with the performance of the official duties of the agency.

Georgia

The 2011 Georgia legislature considered the "Interception and Disclosure of Geolocation Information Protection Act of 2011"[79]. It is the most detailed regulation of geolocation information services found, although it failed to pass.

"Geolocation information" was defined , with respect to a person, as any information that is not the content of a communication, concerning the location of a wireless communication device or tracking device that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person. "Geolocation information service" meant the provision of a global positioning service or other mapping, locational, or directional information service to the public, or to such class of users as to be effectively available to the public, by or through the operation of any wireless communication device, including any mobile telephone, global positioning system receiving device, mobile computer, or other similar or successor device.

The bill made it unlawful for any person to: (1) Intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, geolocation information pertaining to another person; (2) Intentionally disclose, or endeavor to disclose, to any other person geolocation information pertaining to another person, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph; (3) Intentionally use, or endeavor to use, any geolocation information, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph; or (4) Intentionally disclose, or endeavor to disclose, to any other person the geolocation information pertaining to another person, while knowing or having reason to know that the information was obtained through the interception of such information in connection with a criminal investigation and with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

The bill provided for a number of exceptions including: (1) when a person has given prior consent to such interception; (2) for a parent or legal guardian of a child, under age 18 intercepting geolocation information pertaining to that child or to give consent for another person to intercept such information; (3) for any investigative or law enforcement officer or other emergency responder to intercept or access geolocation information relating to a person if such information is

[79] http://www.legis.ga.gov/legislation/en-US/Display/20112012/HB/674

used too respond to a request for assistance or in circumstances in which it is reasonable to believe that the life or safety of a person is threatened, to assist that threatened person; (4) pursuant to a warrant; or (5) when any investigative or law enforcement officer, specially designated by the Attorney General or a prosecuting attorney,intercepts geolocation information if such officer reasonably determines that an emergency situation exists that involves the immediate danger of death or serious physical injury to any person, conspiratorial activities threatening national or state security interest; or conspiratorial activities characteristic of organized crime. Criminal and civil penalties were provided for violations.

Illinois

The 2012 Illinois legislature considered SB 3701[80]. It is somewhat unclear regarding whether the proposed legislation would have applied to cell phone tracking. The bill provided that upon the written complaint of a person under oath or affirmation stating facts sufficient to show probable cause to install and use a tracking device, a judge was authorized to issue a search warrant to install and use a tracking device. Tracking device was defined as an electronic or mechanical device permitting the tracking of the movement of a person or object. It appears that cell phones would qualify as tracking devices given language in the bill that required the warrant to install a tracking device or "otherwise enable the means by which the movement of the person or property named in the tracking device search warrant may be tracked."

Maryland

Georgia's legislation may be the most detailed found, but the legislative proposal in Maryland was certainly the most succinct. HB 560(2012)[81] would have amended the search warrant statute to add that "A law enforcement officer must obtain a search warrant under this section before obtaining location information transmitted by a mobile communications device." The bill failed.

Rhode Island

Legislation introduced during the 2011 Rhode Island legislative session appeared to be aimed at internet service providers with information regarding child pornography, enticement, and exploitation[82]. While the legislation specifically excluded telecommunication offered on a common carrier basis, it stated that "telephone records may not be released by an Internet service provider pursuant to an administrative subpoena." To obtain these records (from those providing telephone services over the internet) a warrant would have been required.

The issue of obtaining geolocation data from a telecommunications service provider has not been comprehensively addressed at the state level. Given this vacuum, the federal provisions discussed above are likely the default standard - an administrative subpoena is sufficient. The greater expectation of privacy encompassed by the Washington state Constitution may, however, require a search warrant.

80 http://www.illinoistrack.us/legislation/GA97SB3701

81 http://mlis.state.md.us/2012rs/billfile/hb0460.htm

82 2011 -- H 5093; http://www.rilin.state.ri.us/BillText11/HouseText11/H5093.pdf

Conclusion

Currently under federal law, law enforcement can gain access to historical cell phone location records with a summons sent to the individual's cell phone service provider. While there is disharmony among the federal courts (at least two federal cases are in the process of being appealed to the United States Supreme Court), the specific cell phone location issue has not been litigated by Washington state appellate courts. The analysis in Washington will differ because of the greater expectation of privacy provided by Article 1, section 7 of the Washington State Constitution. Washington statutes do not specifically address the issue. Currently, Washington prosecuting attorneys are advising law enforcement to obtain search warrants before requesting cell phone location data from service providers.

There are three issues upon which future court decisions are likely to turn. First, is a cell phone a communication device or a tracking device? Obviously, they are communications devices, but they are increasingly being used as tracking devices as well. In fact, they are routinely used as tracking devices by law enforcement and emergency personnel to locate missing persons or those requiring assistance; by parents keeping track of their children; and by vendors who want to target potential customers near their establishments.

Second, how accurately can a person's location be tracked? This is a developing technology. If the cell phone user has enabled the internal GPS, the accuracy of the cell phone's location can be established quite accurately. Even if the GPS has not been enabled, the location can increasingly be triangulated using cell towers. This information is often updated as often as every 7 seconds. Recent court decisions appear to be focusing on the accuracy of the location information, the frequency of the information, and the duration of the tracking.

Finally, do customers waive the privacy of their location information when they acquiesce to service agreements that include clauses authorizing the service providers to acquire and record the information? While the agreements typically say that the information is confidential and used only for limited purposes, the federal law currently allows law enforcement to obtain these records without a warrant. Some courts have questioned the scope of this consent and whether it is truly knowingly given.

Comparison of Federal Law and Washington Law

Provision	Federal	Washington
Intercepting Live Communication (words spoken)	Title I - Interception of Communications and Related Matters; Electronic Communications Privacy Act of 1982, P.L. 99-508. Warrant required, issued upon showing of probable cause that the information to be seized is evidence of a crime, the communication is relevant, normal investigative techniques have failed, and location from which communication is made is connected to the crime.	RCW 9.73.030 - two party consent generally required. RCW 9.73.040 - An ex parte order for the interception of any communication or conversation may be issued by any superior court judge in the state upon verified application of either the state attorney general or any county prosecuting attorney setting forth fully facts and circumstances upon which the application is based and stating that: (a) There are reasonable grounds to believe that national security is endangered, that a human life is in danger, that arson is about to be committed, or that a riot is about to be committed, and (b) There are reasonable grounds to believe that evidence will be obtained essential to the protection of national security, the preservation of human life, or the prevention of arson or a riot, and (c) There are no other means readily available for obtaining such information. RCW 9.73.230 - As part of a bona fide criminal investigation, the chief law enforcement officer of a law enforcement agency or designee above the rank of first line supervisor may authorize the interception, transmission, or recording of a conversation or communication by officers under the following circumstances: (a) At least one party to the conversation or communication has consented to the interception, transmission, or recording; (b) Probable cause exists to believe that the conversation or communication involves: (i) The unlawful manufacture, delivery, sale, or possession with intent to manufacture, deliver, or sell, controlled substances, or legend drugs, or imitation controlled substances, or

		(ii) A party engaging in the commercial sexual abuse of a minor, or promoting commercial sexual abuse of a minor, or promoting travel for commercial sexual abuse of a minor; and (c) A written report has been completed as required.
Access to Stored Communication	Title II - Stored Wire and Electronic Communications and Transactional Records Access (SCA); 18 USC 2701-12. 18 USC 2703 - if storage for 180 days or less, warrant required. If stored for more than 180 days, governmental entity may get a warrant, issue an administrative subpoena (after notice to customer), or with a court order after showing "specific and articulable facts" that the stored information is relevant and material to an ongoing criminal investigation (called a "D" order. The order is to the service provider not the customer who then does not necessarily receive notice). NOTE: "In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State."	No Washington provision dealing with stored cell phone location data. Prosecuting attorneys currently recommend that law enforcement seek a warrant based upon probable cause.
Recording Non-Content Information	Title III - Pen Registers and Trap and Trace Devices; 18 USC 3121-27 Court order upon certification that the information is relevant to an ongoing criminal investigation. Court has no power to review once certification is in the proper form. Neither device can be used in a manner so as to constitute a tracking device without showing probable cause.	RCW 9.73.260 governs the installation and use of pen registers and trap and trace devices. Neither device may be used without a prior court order upon certification that the information is relevant to an ongoing criminal investigation. Failure to obtain a court order prior to the installation of the devices is a gross misdemeanor. The exclusionary rule would also apply, precluding the admissibility any obtained information.

The silver platter doctrine holds that, even though it would not be legal for local law enforcement officials to gather evidence in the same manner, evidence gathered by agents of a foreign jurisdiction (tribal, federal, or other state) is admissible in Washington courts if: (1) there was no participation from local officials; (2) the agents of the foreign jurisdiction did not gather the evidence with the intent that it would be offered in state court rather than in their jurisdiction; and (3) the agents of the foreign jurisdiction complied with the laws governing their conduct. *See generally*, *State v. Brown*, 132 Wn.2d 529, 586-87, 940 P.2d 546 (1997), *cert. denied*, 523 U.S. 1007 (1998).

The silver platter doctrine may allow Washington prosecutors and police officers to utilize tape-recorded calls made by a witness in another state pursuant to that state's one-party consent law. *See State v. Fowler*, 157 Wn.2d 387, 139 P.3d 342 (2006) (state allowed to utilize tape-recorded calls made by the defendant's stepdaughter in Oregon under Oregon's one-party consent law to aid in an Oregon investigation related to defendant's alleged Oregon sexual abuse of which Washington officials were unaware).