Chapter 17

Location Privacy: Technology and the Law

David A. Munkittrick

Proskauer Rose LLP

§ 17:1 Introduction
§ 17:2 Development and Uses of Location-Tracking Technologies
  § 17:2.1 Overview
  § 17:2.2 Global Positioning Systems
  § 17:2.3 Cell Site Location Information
  § 17:2.4 Indoor Positioning Systems
    [A] Radio Frequency Identification
    [B] Other IPS Technologies
  § 17:2.5 Vehicle Tracking
  § 17:2.6 Unmanned Drones
§ 17:3 Government Collection of Location Information
  § 17:3.1 Location Privacy Under the Fourth Amendment
  § 17:3.2 Government Requests for CSLI
    [A] Federal Statutes
    [B] Case Law
    [C] State Laws
§ 17:4 Private Collection and Use of Location Information
  § 17:4.1 GPS Tracking
  § 17:4.2 Mobile Devices and Applications

* The author would like to thank Kristen Mathews, Maureen Garde, Richard Kasman, and Minnie Balaguer for their assistance in the preparation of this chapter.
§ 17:1 Introduction

A person’s location is valuable information. Location information can be instrumental in solving and preventing crimes, saving a life after an accident, finding the fastest route on a road trip, and finding nearby deals and offers. Indeed, geo-targeted advertising is projected to generate over $100 billion by 2020.\(^1\) Approximately 30% of American adults now use a location-based service through a mobile device,\(^2\) and that number is set to increase.

Yet with the collection of location data and its many benefits come privacy concerns, lawsuits, and legislation. Location data can reveal a person’s habits, religious affiliation, health conditions, sexual preferences, union and other memberships—the list goes on. In short, location data is valuable information that can be misused, and the law of location privacy—still fledgling—endeavors to balance competing interests in the use and protection of location information.

As the march of location technologies and services unfolds, the law of location privacy will continue to evolve. It is a new and developing story, but with classic themes: the balance between individual rights and law enforcement; the balance between consumer protection and free enterprise; and the evolution of long-standing notions of privacy.

§ 17:2 Development and Uses of Location-Tracking Technologies

§ 17:2.1 Overview

Many technologies—old, new, and developing—impact location privacy, and each reaches into an individual’s location in a different way. Application of privacy laws often depends on exactly how information is derived and recorded, so an understanding of the various technologies is essential to application of the law.

---

1. Mikal E. Belicove, Privacy of Location-Based Services on FCC’s Radar (July 5, 2012), www.entrepreneur.com/blog/223940.
2. Id.
Some technologies such as global positioning systems (GPS), tracking beepers, and radio frequency identification (RFID) technologies are specifically designed to track the location of people or objects. Other technologies were not designed to overtly track location, but their operation or use nonetheless generates location data that is used and stored. These technologies include Wi-Fi communications technology, surveillance cameras, and other technologies discussed below.

Many of these technologies are found in mobile devices. The number of wireless devices in use is exploding. As of December 2012, there were 326.4 million subscribers to the wireless network in the United States (whether by cell phone, smartphone, tablet, or other device), up from 255.4 million in December 2007 and 140.8 million in December 2002. As part of the operation of the cellular system, the location of these devices is continually recorded in relation to the over 300,000 cell sites in the United States. Devices that are equipped with GPS receivers can also be tracked using GPS signals.

Mobile devices, and particularly smartphones, have become treasure troves of personal information about their users. Twenty-five percent of Americans do most of their web surfing on smartphones, and in 2011, 27% of all photographs in the United States were taken with a smartphone. Each photograph taken with a smartphone is embedded with metadata, which may include the geographic coordinates of the place it was taken. Many smartphone applications can access that metadata and upload it to their own servers. Thus, it is possible to piece together the location history of the user based solely

---

4. *Id.*
on photographs.\textsuperscript{8} Metadata in pictures can also reveal location of third parties in photos, particularly with the growing use of face recognition software, which allows companies like Facebook to automatically “tag” people in photos.\textsuperscript{9}

\section*{§ 17:2.2 Global Positioning Systems}

Perhaps the best-known location tracking technology is GPS. Before the advent of GPS, the most widely used method of location tracking other than physically following a person was the “beeper.”\textsuperscript{10} A beeper is a radio transmitter, usually battery-operated, that emits a periodic radio signal. The beeper’s location can be monitored from a short distance away by tracking the beeper’s radio signal.\textsuperscript{11} GPS effectively did away with the necessity of staying within a certain distance of a tracking device. The Department of Defense launched the first GPS satellite in 1978,\textsuperscript{12} and civilian use of the system began in 1983.\textsuperscript{13} Today, the GPS satellite system in the United States is controlled by a joint civilian-military board of the U.S. government and is maintained by the U.S. Air Force.\textsuperscript{14}

GPS devices determine location—latitude, longitude, and altitude—by measuring the distance from the GPS device to a set of GPS satellites.\textsuperscript{15} This process of determining location by measuring distances is known as trilateration (in contrast to triangulation, which

\begin{thebibliography}{9}
\bibitem{8} Christy Foley, \textit{Suing Ourselves; How Our Need for Smartphones Allows Apple and Google to Act Like Big Brother}, 23 NYSBA ENT., ARTS & SPORTS L.J. 32, 32 (Summer 2012) (citing Nick Bilton, \textit{Apple Loophole Gives Developers Access to Photos}, N.Y. TIMES BITS BLOG (Feb. 28, 2012), http://bits.blogs.nytimes.com/2012/02/28/tk-ios-gives-developers-access-to-photos-videos-location/). For example, the location of John McAfee, who was on the run after being dubbed a “person of interest” in a neighbor’s death, was inadvertently revealed when \textit{Vice} magazine posted a picture of him without scrubbing the metadata. Jeff Wise, \textit{In Pursuit of McAfee, Media Are Part of Story}, N.Y. TIMES, Dec. 10, 2012, at B1.
\bibitem{10} This type of tracking beeper should be distinguished from pagers, which are designed to send and receive short messages.
\bibitem{13} \textit{Id.}
\bibitem{15} \textit{Id.}
\end{thebibliography}
measures angles to determine location).\textsuperscript{16} Each GPS satellite transmits its location and the current time, so the GPS receiver can measure its distance to each satellite by determining how long it takes the satellite’s signal (traveling the speed of light) to reach the receiver.\textsuperscript{17} With the distance information of at least four satellites, the receiver can calculate its position in three dimensions.\textsuperscript{18}

GPS receivers passively receive and measure signals from satellites; they do not transmit any signals themselves to determine location.\textsuperscript{19} The passive nature of the GPS system allows it to support an unlimited number of users and makes the system relatively impervious to weather conditions.\textsuperscript{20} Depending on the quality of the GPS receiver, accuracy can range from within a few meters to within a centimeter.\textsuperscript{21} But the signal transmitted from GPS satellites is quite weak, about the power equivalent of a 50-watt light bulb.\textsuperscript{22} Consequently, GPS tracking does not function when objects such as buildings or bridges block the signal, and GPS tracking does not function indoors.\textsuperscript{23}

GPS receivers have become smaller and cheaper, to the point that GPS-enabled mobile devices pervade today’s technology-driven world.\textsuperscript{24} In fact, most cell phones in use today in the United States include GPS receiver capability as a result of a 1999 federal regulation intended to improve emergency response to 911 calls.\textsuperscript{25}

\begin{itemize}
\item \textsuperscript{16} Id.
\item \textsuperscript{17} Griffin, supra note 12.
\item \textsuperscript{18} Id.
\item \textsuperscript{19} Id.
\item \textsuperscript{20} Id.
\item \textsuperscript{21} Id.
\item \textsuperscript{22} Griffin, supra note 12.
\item \textsuperscript{25} See 47 C.F.R. § 20.18 [requiring that licensees “achieve 95 percent penetration of location-capable handsets” among subscribers by the end of 2005]; see also David R. Marshall & Craig S. Friedman, Stopping Employees in Their Tracks: GPS Tracking of Employees, MEALEY’S LITIG. REP.: EMP. L., vol. 4 no. 3 (Oct. 2007), at 1–2.
\end{itemize}
GPS has numerous uses. It enables emergency response teams to quickly locate 911 calls; companies to track employees and vehicles to improve efficiency; parents to keep track of their children; private investigators and law enforcement to track subjects; drivers to access real-time turn-by-turn directions; and consumers to receive location-based services on their mobile devices. Of course, GPS devices can also be used for more nefarious purposes by stalkers and criminals.

While GPS devices do not themselves transmit location information to third parties, often GPS devices are linked to third-party computers or servers, particularly in the case of navigation services, vehicle telematics, and location-based applications on mobile devices.

§ 17:2.3 Cell Site Location Information

Even with GPS functionality disabled, a mobile device’s location can be tracked through another location tracking method using cell site location information (CSLI). Two forms of CSLI are generated as part of the operation of the cellular system: historical and prospective. Historical CSLI provides location data about where a phone has been in the past, while access to prospective CSLI allows law enforcement to track the movements of a cell phone in real time.

As long as cell phones and other mobile devices are powered on, the devices are constantly communicating with nearby cell sites. This automatic communication, called “registration,” functions to identify

27. Id. (“GPS trackers are increasingly being cited in cases of criminal stalking and civil violations of privacy.”).
28. “Vehicle telematics” refers to the integrated use of telecommunications and informatics and includes GPS technology integrated with computers and mobile communications technology in cars. For example, “OnStar,” a vehicle telematics system, is a subscription service provided by General Motors that enables in-vehicle security, hands-free calling, turn-by-turn navigation, and remote diagnostics. The system relies on mobile networks for communication and GPS for location information.
the subscriber within the network, validate the account, and determine where to route call traffic.\footnote{In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) [hereinafter S.D. Tex. 2005] [citing U.S. DEP’T JUSTICE, ELECTRONIC SURVEILLANCE MANUAL, at 178–79 n.41 [rev. June 2005], www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf].} Registration cannot be disabled by the user,\footnote{See S.D. Tex. 2010, 747 F. Supp. 2d at 832.} and the registration signal is carried on a channel separate from the channel used to carry calls.\footnote{Kyle Malone, Comment, The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy, 39 PEPPL. L. REV. 701, 707–08 [Mar. 2012] [citing DEBORAH MORLEY & CHARLES S. PARKER, UNDERSTANDING COMPUTERS: TODAY AND TOMORROW 299 (Marie Lee ed., 12th ed. 2008)].} When a subscriber places a call, a signal is transmitted from the phone to the closest cell site, then to the cellular company’s switching office.\footnote{Id. at 833.} The call signal is then transferred to the recipient’s device by landlines, other cellular transmission towers, or a combination of the two.\footnote{S.D. Tex. 2010, 747 F. Supp. 2d at 832–33.}

The location of a mobile device relative to a cell site is calculated based on the data collected and analyzed at the cell site receiving the device’s signals.\footnote{Id.} This data can be translated into location information by a variety of methods. The most basic method uses the location of the cell site communicating with the device at any given time.\footnote{S.D. Tex. 2010, 747 F. Supp. 2d at 832–33.} This method places the device within that cell site’s reception area, and depending on the network, it may be possible to place the phone within one of the three 120-degree arcs surrounding the cell site.\footnote{Id. at 833.} As the number of cell phone users and the demands put on the cellular network grow, carriers divide the coverage area into smaller and smaller sectors ("cells"). This increases the accuracy of location data by cell site location, sometimes to individual floors and rooms within buildings.\footnote{S.D.N.Y. 2006, 460 F. Supp. 2d at 451.} Newer technologies allow more precise positioning of cell phones within a particular cell site sector. By measuring the time and angle at which a device’s signal arrives at multiple cell sites, for example, it is possible to triangulate a phone’s location to within fifty meters or less.\footnote{Id. at 833.}

Location data is collected with each phone call, as well as every seven seconds as the cell phone periodically registers with nearby

\textit{Location Privacy: Technology and the Law} § 17:2.3


34. Id.


36. Id.


38. Id.


41. Id. at 833.
cell sites. One federal district court observed that based on recent studies on cell phone use, even if cell phone location were recorded only at the beginning and end of phone calls and text messages, location data for a typical adult user would reveal between twenty and fifty-five location points each day. Carriers typically create and retain detailed call records that include precise location information, and some carriers store location data even when calls are not being made or received. This means location data may be recorded up to 100 times per day.

Sometimes the data is handled by third parties. Some carriers outsource the task of collecting, analyzing, and storing location information to other companies.

This vast volume of location data is relatively cheap for carriers to store, and it is valuable for network management, marketing, and developing new services—particularly location-based services. Mobile apps can also use a mobile device’s location data. Indeed, unique serial numbers assigned to every smartphone can be combined with location data to allow a third-party mobile application to track a particular consumer’s real-world location. For example, mobile apps provide turn-by-turn directions, location-targeted ads, and predictive modeling. Predictive modeling is the term for new research that suggests cross-referencing location information of one person with that of the person’s friends can enable predictions of the person’s

---

42. Malone, supra note 35, at 708.
44. Id. at 833–34.
future whereabouts. The technology of determining a person’s identity from anonymized location data is also advancing. Researchers at the Massachusetts Institute of Technology, for example, found just four geo-temporal data points were enough to identify a particular mobile phone user.

Location information generated by the cellular network is also a powerful tool for law enforcement. All this location data also has commercial significance. The location-based services industry is growing, and services go beyond traditional navigation to mobile games that create real-life scavenger hunts, retail applications that allow consumers to find the nearest store, applications that address advertisements to a user’s current location, and applications that provide weather and news targeted to a user’s location.

§ 17:2.4 Indoor Positioning Systems

[A] Radio Frequency Identification

Radio frequency identification—a type of indoor positioning system (IPS)—is a technology that consists of a microchip and antenna (an

53. In 2011, carriers responded 1.3 million times to law enforcement requests for cell site data. Maass & Rajagopalan, supra note 51.
RFID tag, which, when stimulated by a remote reader, sends back information via radio waves. However, because radio waves reflect off metallic and ceramic objects, RFID accuracy can be limited to within forty-nine feet. Still, RFID has many commercial applications, including inventory and asset tracking, security and access control (employee identification badges), and transportation payment systems.

RFID technology has also been used to track individuals. RFID technology has shown particular use in hospitals, where it can be used to track doctors, nurses, patients, and medical equipment. RFID systems have also been implemented in schools to track students, though this use has been the subject of at least one lawsuit, discussed below. The Disney World theme parks are also planning an RFID bracelet program—the bracelets would function as a room key, park ticket, PhotoPass card, and optional payment system in Disney parks. They could also track location and help parents locate lost children.

[B] Other IPS Technologies

In addition to using RFID, location can be determined indoors through ultrasound, infrared, or Wi-Fi technologies. Wi-Fi technology can utilize wireless networks that largely already exist in many places, allowing wireless-enabled devices to be tracked within a building simply by installing software. Wi-Fi location technologies can determine location down to where a customer is sitting at a restaurant. Ultrasound-based IPS can at least establish location in a particular room because ultrasound signals, detected by microphones

58. Greenemeier, supra note 23.
59. Id.
60. See David Rosen, Big Brother Invades Our Classrooms, SALON [Oct. 8, 2012], www.salon.com/2012/10/08/big_brother_invades_our_classrooms/.
61. See section 17:4.1, infra.
63. Greenemeier, supra note 23.
65. Greenemeier, supra note 23.
placed in a room, bounce off walls and doors and so are confined to a particular room.\textsuperscript{67}

In addition to its uses in hospitals and schools, IPS technologies may also prove useful in shopping centers for targeted advertising based on consumers’ proximity to particular stores.\textsuperscript{68} It can also be used in “geo-fencing”—creating a defined boundary around a location, such as a restaurant or a store, within which a mobile device will receive messages advertising the location or making an offer.\textsuperscript{69}

\section*{\textbf{\textsuperscript{§} 17:2.5 Vehicle Tracking}}

License plate tracking technology is also proliferating and is moving from law enforcement to civilian uses. Police cars outfitted with special cameras can capture the license plates of every passing car, noting each car’s location.\textsuperscript{70} The amount of data collected is immense—scanners can record up to 3,000 plates per minute.\textsuperscript{71} Law enforcement uses license plate information to locate stolen cars or missing persons, collect unpaid tickets, and identify vehicles of suspected criminals. Some private companies have also utilized the data to repossess cars or detect so-called owner-give-up insurance fraud, where a vehicle’s owner fakes its theft by giving it to a friend and claiming it was stolen.\textsuperscript{72}

\begin{footnotesize}
\begin{enumerate}
\item Greenemeier, \textit{supra} note 23.
\item Anthony, \textit{supra} note 64; \textit{see also} DesMarais, \textit{supra} note 66.
\item Julia Angwin & Jennifer Valentino-Devries, \textit{New Tracking Frontier: Your License Plates}, \textit{WALL ST. J.}, Sept. 29, 2012, at A1. The license-plate databases do not contain the names and addresses of vehicle owners, but that information can often be obtained from separate databases. \textit{Id}.
\end{enumerate}
\end{footnotesize}
A vehicle’s location can also be tracked using electronic toll collection systems like “EZ-Pass.” Similarly, magnetic fare cards like New York City’s “Metrocard”—a method of payment for entry into the subway system—can also record a person’s location, at least at subway turnstiles and toll booths. Like CSLI records, these records are subject to law enforcement and civil subpoenas.  

§ 17:2.6 Unmanned Drones

Much like GPS did in the 1980s, another government technology, unmanned drones, is spreading to civilian use. The technology was first used extensively in the Iraq and Afghanistan wars, and Congress has asked the Federal Aviation Administration [FAA] to create regulations by September 2015 that will facilitate the routine domestic use of unmanned drones. Law enforcement is of course interested in the technology, but so are oil companies (to monitor pipelines), environmentalists (to monitor species in remote locations), universities (for research) and farmers (to detect which fields need watering). Many of these drones could carry powerful surveillance tools, including cameras, infrared sensors, face-recognition technology, and microphones—technologies that could gather information about people outside and indoors.

§ 17:3 Government Collection of Location Information

Until recently, location privacy was exclusively the realm of Fourth Amendment law, protecting individuals from unreasonable intrusions of privacy by law enforcement. This section discusses the development of this Fourth Amendment jurisprudence as well as statutory law governing law enforcement access to location data from telecommunication carriers.

74. Drones are unmanned aerial vehicles, controlled either autonomously by computers or by a person at a remote command console.
77. CRS DRONE REPORT at 10.
§ 17:3.1 Location Privacy Under the Fourth Amendment

The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” and applies to “safeguard the privacy and security of individuals against arbitrary invasions by government officials.” Early Fourth Amendment decisions concerning the use of surveillance technology focused on whether there had been a physical intrusion into a person’s personal effects or home. In *Olmstead v. United States*, for example, the Supreme Court held that wiretapping a defendant’s phone conversations from outside the home did not violate the Fourth Amendment because there was no physical intrusion. In 1967, however, the Court in *Katz v. United States* moved away from the physical intrusion analysis, stating the Fourth Amendment “protects people, not places.” The *Katz* Court was cognizant that privacy expectations shift with advances in technology. After *Katz*, to determine whether the government unreasonably invaded protected privacy interests in a given situation, courts have asked whether an “individual manifested a subjective expectation of privacy in the object of the challenged search,” and whether “society [is] willing to recognize that expectation as reasonable.” Thus, Fourth Amendment decisions can be instructive in the civil context by defining judicially recognized reasonable expectations of privacy in relation to location tracking.

*United States v. Knotts* was one of the first cases to apply the Fourth Amendment to the use of a tracking device. *Knotts* upheld the use of a tracking “beeper” that had been placed in a container of chloroform, suspected to be destined for the manufacture of illegal drugs. The police followed the cars in which the container was placed with a monitor receiving the beeper signals, lost contact once, and found the beeper signal again, stationary at a cabin in Wisconsin. The officers used that information to secure a search warrant for the cabin. They found a drug laboratory in the cabin and the container of chloroform.

---

78. U.S. CONST. amend. IV.
81. See United States v. Knotts, 460 U.S. 276, 281–82 [1983]; but see Silverman v. United States, 365 U.S. 505, 511–12 [1961] (holding the use of a “spike mike” to listen to conversations in the home was an intrusion into the home, constituted a search, and violated the Fourth Amendment).
83. Id. at 351–53.
86. Id. at 278.
outside. The Court decided there was no intrusion into the defendants’ reasonable expectation of privacy because the location of the car containing the container had been voluntarily conveyed to the public—the car was driven on public roads and the container was placed in open fields clearly visible from public spaces.87

One year after *Knotts*, the Court decided a second “beeper” case, *United States v. Karo*, that distinguished the heightened privacy interests in a private residence.88 In *Karo*, the item tracked with a beeper was brought into a private residence, which spurred the Court to hold that the warrantless use of a beeper in that case invaded Karo’s reasonable expectation of privacy.89 DEA agents had learned that the defendants ordered fifty gallons of ether from a government informant, who told the agents that the ether was to be used to extract cocaine from clothing that was imported to the United States. The agents obtained an order authorizing the installation of a beeper in one of the cans of ether and followed the beeper’s signal to a succession of houses. Determining the can of ether was inside one of the houses, the agents obtained a search warrant, found the cocaine, and arrested the defendants.

In holding the search was not valid, the *Karo* Court reasoned,

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or person, for that matter—is in an individual’s home at a particular time.90

However, in her opinion concurring in part and in the judgment, Justice O’Connor wrote, “As a threshold matter it is clear that the mere presence of electronic equipment inside a home, transmitting information to government agents outside, does not, in and of itself, infringe on legitimate expectations of privacy of all who have an expectation of privacy in the home itself.”91

In 2001, the Court applied some of these principles to heat-sensing technology used to detect the heat signature of marijuana-growing lights emanating from the walls and roof of a suspect’s house.92 The Court held that the use of sense-enhancing technology to gather

---

87. *Id.* at 281–82.
89. *Id.* at 718.
91. *Id.* at 722–23 (O’Connor, J., concurring in part and concurring in the judgment).
information about the interior of a home that could not otherwise have been obtained absent physical intrusion into the home requires a warrant “at least where [as here] the technology in question is not in general public use.”

This was the jurisprudential context in which the Supreme Court decided its first GPS case, United States v. Jones. The question in Jones was whether police had violated the Fourth Amendment in placing a GPS tracker on a suspect’s car and tracking the car for twenty-eight days without a warrant. But instead of simply following the “reasonable expectation of privacy” inquiry, Justice Scalia, in his majority opinion, returned to the Olmstead-style physical trespass test, holding that placing the GPS device on the car constituted a physical trespass, so the warrantless search violated the Fourth Amendment. Justice Scalia declined to decide the reasonable expectation of privacy question. However, in Justice Alito’s four-justice concurrence and Justice Sotomayor’s separate concurrence, five justices applied the reasonable expectation of privacy test. Justice Alito argued that the four-week tracking in Jones violated society’s reasonable expectation of privacy, but that a shorter-term tracking might not. Justice Sotomayor went further and noted the privacy implications of location tracking: it could capture “trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.” Such information can create “a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”

Another Fourth Amendment doctrine of particular import to cell carriers and mobile apps is the third-party doctrine, which provides

---

93. Id. at 46.
95. Id. at 950–52.
96. Id. at 954.
99. Id. at 955 [Sotomayor, J., concurring] [quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) [internal quotation marks omitted]].
100. Id. [Sotomayor, J., concurring].
that any information willingly handed over to a third party is not subject to a reasonable expectation of privacy. In *Smith v. Maryland*, this doctrine was applied to phone records to hold that an individual has no reasonable expectation of privacy in phone numbers dialed because the phone numbers are willingly conveyed to a third party—the phone company. In her *Jones* concurrence, Justice Sotomayor also voiced a willingness to abandon the third-party doctrine because it is “ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”

§ 17:3.2 Government Requests for CSLI

[A] Federal Statutes

A patchwork of federal statutory law supplements the Fourth Amendment in the context of law enforcement requests for location data from telecommunication carriers. The central statute in this patchwork is the Electronic Communications Privacy Act (ECPA), enacted in 1986 in part to fill the gap in Fourth Amendment protection left by the third-party doctrine. The ECPA is made up of three titles. Title I amended the 1968 federal wiretap statute to cover electronic communications; Title II created the Stored Communications Act (SCA); and Title III covers pen registers and trap and trace devices.

The SCA protects information held by providers of an “electronic communication service” (ECS) and providers of “remote computing service” (RCS), both defined terms. The statute defines “electronic

101. United States v. Miller, 425 U.S. 435, 443 (1976) (holding there was no legitimate expectation of privacy in bank records because the information was voluntarily handed over to the bank).
104. See chapter 6 of this treatise for a more in-depth discussion of the ECPA.
105. See In re Application of U.S. for an Order Directing a Provider of Elec. Commc’ns Serv. to Disclose Records to Gov’t, 620 F.3d 304, 306 (3d Cir. 2010).
108. 18 U.S.C. §§ 3121–27. Generally, a pen register is a device that records phone numbers called from a particular phone, and a trap and trace device records all incoming telephone numbers to a particular phone. The USA PATRIOT Act of 2001 amended the definition of “pen register” to include devices that record “dialing, routing, addressing, or signaling information,” 18 U.S.C. § 3127[3], and a “trap and trace device” to include devices or processes that capture “the originating number or other dialing, routing, addressing, and signaling information.” 18 U.S.C. § 3127[4].
communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications,” and “remote computing service” as “provision to the public of computer storage or processing services by means of an electronic communications system.” Both these definitions have been found to be problematic. Generally, the SCA limits the circumstances in which the government can compel private communications companies to disclose information about subscribers. It also limits private companies’ ability to voluntarily provide subscriber information to the government. Under the SCA, cell carriers are treated as ECS providers.

The SCA, in 18 U.S.C. § 2703(c), outlines the procedures by which government officials may seek to require ECS and RCS providers to disclose subscriber information such as CSLI. The authority granted by section 2703(c) does not include disclosure of the contents of communications, such as a recording of a phone call or the text of an email. Indeed, the procedures required under the SCA depend on the type of information the government is requesting, demonstrating the differing privacy interests at stake. Subsections 2703(a)–(b) cover requests for the contents of communications, while section 2703(c) governs requests for “a record or other information” pertaining to a subscriber or customer. The government can obtain such “a record or other information” through a traditional warrant, by consent of the subscriber or customer, or through a court order under section 2703(d). A section 2703(d) order requires less than the probable cause required for a traditional warrant; therefore it presents a lower barrier to government access. A section 2703(d) order can issue on a showing of: “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or records or other information sought, are relevant and material to an ongoing criminal investigation.”

---

110. 18 U.S.C. § 2711(2).
112. 18 U.S.C. § 2703 (detailing the evidentiary standard that must be met to obtain certain types of information).
113. The SCA contains a general prohibition against private companies disclosing subscriber information to the government, and then provides exceptions under which disclosure is proper. See 18 U.S.C. § 2702.
114. A traditional warrant requires a probable cause showing. U.S. CONST. amend. IV.
115. 18 U.S.C. § 2703(d); see also, e.g., In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76, 80.
Federal statutes also confer responsibilities on companies to cooperate in and facilitate the interception of communications information. The Communications for Assistance of Law Enforcement Act (CALEA), passed in 1994, requires communications service providers to engineer their services in a way that allows the government to later intercept or access “all wire and electronic communications carried by the carrier within a service area.” At least one federal court has held that this includes CSLI. Law enforcement may access records with proper authority (warrant or court order), and providers are to secure their systems from unauthorized access.

[B] Case Law

In 2005, courts began publishing opinions regarding government access to CSLI. Until 2005, there were no published opinions on the constitutional and statutory implications of government access to CSLI because applications for access to such data were made ex parte and the proceedings were sealed. They routinely remained sealed even after the conclusion of the underlying criminal matters to which they were related. In 2005, however, two magistrate judges published

[D. Mass. 2007] (“Because historical cell site information clearly satisfies each of the three definitional requirements of section 2703(c), a section 2703(d) order requiring the disclosure of historical cell site information may issue on a showing of ‘specific and articulable facts’ and no more.”).


118. U.S. Telecom Ass’n v. FCC, 227 F.3d 450 [D.C. Cir. 2000] (holding that CALEA’s definition of call-identifying information allowed the FCC to require telecommunications carriers to implement technology that would make CSLI available to law enforcement agencies).

119. See 47 U.S.C. § 1004 (“A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer . . . acting in accordance with regulations. . . .”).


121. See Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before
opinions addressing these issues, and numerous other published opinions followed.

One of the first published opinions came from Magistrate Judge James Orenstein of the Eastern District of New York in a decision from 2005.122 In that case, the government sought the disclosure of CSLI for outbound and incoming calls.123 Judge Orenstein focused on 18 U.S.C. § 2703’s provision for the disclosure of “records concerning electronic communication service or remote computing service” upon a showing of “specific and articulable facts showing that there are reasonable grounds to believe that [such information is] relevant and material to an ongoing criminal investigation.”124 After finding the government had met the “specific and articulable facts” standard, the court considered whether the requested CSLI was properly considered records concerning an electronic communication service subject to section 2703(d).125 Judge Orenstein reasoned that the answer would be “yes” under 18 U.S.C. §§ 2711(1) and 2510(12), which provide the applicable definition of “electronic communication,” unless the subject phone is a “tracking device” under 18 U.S.C. § 3117.126 The ECPA specifically excludes data from tracking devices from its definition of “electronic communication,”127 and “tracking device” is defined as “an electronic or mechanical device which permits the tracking of the movement of a person or object.”128 The court found this described the attributes of the subject cell phone, so the CSLI was not an “electronic communication” and therefore not subject to a section 2703(d) order. “The requested information . . . reveals that person’s location at a given time . . . [so] the authorization, if granted, would effectively allow the installation of a tracking device without the showing of probable cause normally required for a warrant.”129 The government’s request was denied.

Judge Stephen Smith of the Southern District of Texas followed Judge Orenstein with a more detailed opinion deeming cell site

123. Id. at 563.
124. Id.
125. Id.
126. Id. at 564.
127. 18 U.S.C. § 2510(12)(C) (“‘[E]lectronic communication’ . . . does not include . . . any communication from a tracking device”).
128. 18 U.S.C. § 3117(b).
location information the equivalent of turning a cell phone into a tracking device and thus requiring a warrant.\textsuperscript{130}

While Congress may not have known back in 1986 that a cell phone would come to be used as a tracking device, the broad language of § 3117(b) certainly left open that possibility, [and] [a]s with a tracking device, this [registration] process is usually surreptitious and unknown to the user.\textsuperscript{131}

The court declined to adopt the government’s argument that there is no reasonable expectation of privacy in cell site location data, noting that “[u]nlike dialed telephone numbers, cell site data is not ‘voluntarily conveyed’ by the user to the phone company. . . . [A] cell phone user may very well have an objectively reasonable expectation of privacy in his call location information.”\textsuperscript{132}

However, case law in this area is still quite new,\textsuperscript{133} and district court decisions are far from uniform in their approach to government requests for cell site information under the SCA. In 2006, for example, Judge Lewis Kaplan of the Southern District of New York published a decision granting a request for prospective cell site information under the Pen Register Statute, 18 U.S.C. § 3121 \textit{et seq}. and the SCA, 18 U.S.C. § 2701 \textit{et seq}. Instead of asking for CSLI that could be used to triangulate the precise location of the phone, the government request in the \textit{S.D.N.Y. 2006} case asked only for information regarding one tower at a time and only information transmitted at the beginning and end of particular calls.\textsuperscript{134} But the court noted that the statutory authorization would also apply to requests for information from multiple towers simultaneously.\textsuperscript{135} “The language of the two statutes,” the court held, “when read together, clearly authorizes such disclosure.”\textsuperscript{136} Judge Kaplan reasoned that registration information sent by cell phones is “signaling information” under the Pen Register Statute.\textsuperscript{137} He found the prior opinions coming to the opposite

\begin{enumerate}
\item \textsuperscript{130} \textit{S.D. Tex. 2005}, 396 F. Supp. 2d at 754 (“The distinction between cell site data and information gathered by a tracking device has practically vanished.”).
\item \textsuperscript{131} \textit{Id}.
\item \textsuperscript{132} \textit{Id.} at 756–57.
\item \textsuperscript{133} In 2005, Judge Orenstein wrote that his “research on this question has failed to reveal any federal case law directly on point.” \textit{E.D.N.Y. 2005}, 384 F. Supp. 2d at 566.
\item \textsuperscript{134} \textit{S.D.N.Y. 2006}, 460 F. Supp. 2d at 461.
\item \textsuperscript{135} \textit{Id}. at 452.
\item \textsuperscript{136} \textit{Id}. at 450.
\item \textsuperscript{137} \textit{Id}. at 455.
\end{enumerate}
conclusion unpersuasive. While CALEA excepts information that may disclose the physical location of the subscriber from government requests “solely” pursuant to a pen register or trap and trace device, location data could be obtained under the Pen Register Statute in combination with some other authority. That additional authority is found in the SCA’s provision allowing “a governmental entity [to] require a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service.” By reading that provision in conjunction with the Pen Register Statute, the exception of tracking devices did not apply.

The Third Circuit was the first appellate court to address the issue of government access to CSLI under the ECPA in a case on appeal from an opinion by Magistrate Judge Lisa Lenihan of the Western District of Pennsylvania. Judge Lenihan’s opinion was joined by all the magistrate judges of the district and denied a government application to compel a cell phone service provider to disclose historical CSLI. However, the Third Circuit rejected the district court’s treatment of cell phones as tracking devices, reasoning that the historical CSLI records sought were actually wire communications and not electronic communications. Section 2703(d) orders apply to records concerning an electronic communication service, which is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” The statutory definition of “wire communication” is “any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception [including the use of such connection in a switching station].” Because cell towers are essentially switching stations for cell phone calls, the Third Circuit held, cell site information qualifies as wire communications. And, the Third Circuit continued, the

140. Id. at 458 [quoting 18 U.S.C. § 2703(c)].
141. Id. at 460.
142. In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to Gov’t, 534 F. Supp. 2d 585 [W.D. Pa. 2008], see also section 17:2.3, supra [comparing historical and prospective CSLI].
143. Third Circuit 2010, 620 F.3d at 310.
144. 18 U.S.C. § 2510(15).
145. 18 U.S.C. § 2510(1).
146. Third Circuit 2010, 620 F.3d at 310.
“tracking device” exception only applies to electronic communications. The magistrate judge’s order was vacated, and the case was remanded.  

While the Third Circuit decided the ECPA does not mandate a probable cause showing for a section 2703(d) court order covering location information, it held the statute gave district courts discretion to require a warrant rather than the lower standard for a section 2703(d) court order. So, in the Third Circuit, if a district court concludes a warrant is required rather than a section 2703(d) order, “an option to be used sparingly,” the district court must “make fact findings and give a full explanation that balances the Government’s need . . . for the information with the privacy interests of cell phone users.”  

The Third Circuit was the first appellate decision on the ability of the government to obtain CSLI under the ECPA, and federal courts remain divided over whether the government must show probable cause to obtain cell site information from service providers. The Sixth Circuit in United States v. Skinner had the opportunity to add its take on statutory interpretation of the ECPA in 2012, but instead avoided the question and held that tracking the location of a cell phone did not violate the Fourth Amendment. “There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone.” The court noted that the fact the tracking was done pursuant to SCA court orders weighed in favor of constitutionality, but was not necessary to the constitutional finding. The court distinguished the Supreme Court GPS decision in Jones as involving physical trespass, whereas there was no physical intrusion in Skinner. As Justice Sotomayor predicted in her Jones concurrence, the “trespassory test” provides little guidance on “cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion of property.”

147. As an alternative ground, the government also argued that citizens have no reasonable expectation of privacy in CSLI because it is voluntarily shared with cellular providers. The court declined to apply the third-party doctrine to CSLI, noting that “a cell phone customer has not ‘voluntarily’ shared his location information with a cellular provider in any meaningful way [because] . . . it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information.” Id. at 317.

148. Id. at 319.

149. See ACLU v. U.S. Dep’t of Justice, 655 F.3d 1, 13 n.20 (D.C. Cir. 2011) (collecting cases).


151. Id. at 777.

152. Id. at 779.

The Fifth Circuit similarly held that court orders authorized by the SCA to compel cell phone service providers to produce historical cell site information are not unconstitutional under the Fourth Amendment.\footnote{In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).} The court found it key that it is the service providers, and not the government, that initially records the data.\footnote{Id. at 610.} Because the information sent by wireless devices to cell towers was required to route phone calls appropriately, the records were a “business record” (and not tracking information) in which cell service subscribers do not have a privacy interest for purposes of the Fourth Amendment.\footnote{Id. at 610–12.} The court was clear, however, that its decision applied only to the question before it: whether the government may constitutionally request historical cell site information for an individual cell service subscriber only at the time calls are made. Questions remain open regarding orders requesting data from all phones that use a particular cell tower, requesting cell site information from the recipient of a call, or requesting location information for the duration of a call or when the phone is idle.\footnote{Id. at 615.}

[C] State Laws

At least eight states have laws that require cell phone providers to cooperate with law enforcement officials. Kansas was the first, in 2009, enacting a law to make it easier for police to track cell phone signals.\footnote{KAN. STAT. ANN. § 22-4615.} The law requires wireless telecommunications carriers to provide call location data to law enforcement upon request, even without a warrant or court order, in emergency situations.\footnote{Id. at 615.} Hawaii, Minnesota, Missouri, Nebraska, New Hampshire, North Dakota, and Tennessee have all passed similar laws.\footnote{HAW. REV. STAT. § 803-42; MINN. STAT. § 237.83 [written request]; MO. REV. STAT. § 392.415; NEB. REV. STAT. §§ 86-803; N.H. REV. STAT. ANN. § 106-H:17; N.D. CENT. CODE § 57-40.6-13; TENN. CODE ANN. § 38-1-602.} By contrast, 18 U.S.C. § 2702 makes such provision of call location data voluntary when relating to an emergency.

Like their federal counterparts, state laws in this area have not been free of legal challenge. In Missouri, a federal lawsuit was filed challenging the state’s law that requires cell phone providers to supply information to police upon request. The plaintiff in the case alleged the Missouri law is unconstitutional under the supremacy clause of the U.S. Constitution because the law conflicts with the federal Stored

154. In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
155. Id. at 610.
156. Id. at 610–12.
157. Id. at 615.
158. KAN. STAT. ANN. § 22-4615.
159. Id.
Communications Act. The state filed a motion to dismiss, arguing sovereign immunity and lack of standing, and the plaintiff voluntarily dismissed the suit.

§ 17:4 Private Collection and Use of Location Information

Though it is somewhat unsettled, the law of government access to location data is the most developed area of location privacy. In the private context, location privacy issues most often arise in employment contexts, in relation to behavioral and location-based advertising, and recently, in relation to mobile devices and applications.

§ 17:4.1 GPS Tracking

As of this writing, in California, Delaware, Michigan, Tennessee, and Texas, placing an electronic tracking device on a vehicle is unlawful without the owner’s consent. Thus, in the employment context in those states, there is no statutory restriction on employers tracking employer-owned vehicles, but employers would need to obtain employee’s consent to track employee-owned vehicles.

There is also a relative dearth of case law on the topic of GPS location tracking. Cases are most likely to occur in the employment context, and decisions are generally permissive. The case law is also mixed between private and public employers—Fourth Amendment standards apply only to the latter. One of the first decisions in this area came in the private context: Elgin v. St. Louis Coca-Cola Bottling Co. In that case, the defendant employer began using GPS to track company-owned vans as part of an investigation into cash shortages from vending machines. The plaintiff was authorized to drive one of the vans during working and non-working hours. When he found out about the tracking, the plaintiff sued, alleging violations of the Missouri Human Rights Act and intrusion upon seclusion as a result of the defendant’s investigation. The court found plaintiff’s employment condition suffered no tangible change, so defendant’s

163. CAL. PENAL CODE § 637.7; DEL. CODE ANN. tit. 11, § 1335[a][8]; MICH. COMP. LAWS SERV. 750.5291; TENN. CODE ANN. § 39-13-601; TEX. PENAL CODE § 16.06.
165. Id. at *2.
166. Id. at *3.
167. Id. at *1.
action did not violate the Missouri Human Rights Act.\(^\text{168}\) Regarding the common law intrusion upon seclusion claim, the court turned to Fourth Amendment jurisprudence to help determine whether the “intrusion would be highly offensive to a reasonable person.”\(^\text{169}\) “Under U.S. Supreme Court precedent, an automobile’s path of travel is, as a matter of law, not secret and private subject matter as necessary for a viable invasion of privacy claim under Missouri law.”\(^\text{170}\) The court awarded summary judgment for the defendant.\(^\text{171}\)

The New Jersey Appellate Division also used federal Fourth Amendment jurisprudence to determine the scope of privacy rights in the private context. In Villanova v. Innovative Investigations, Inc., the plaintiff alleged intentional or negligent invasion of his right of privacy when a private investigator hired by his wife placed a GPS device on his vehicle.\(^\text{172}\) In New Jersey, the tort of invasion of privacy applies to “one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his [or her] private affairs or concerns.”\(^\text{173}\) There was no evidence that the plaintiff drove the vehicle into a private or secluded location that was out of the public view, and the court cited the Knotts holding that “a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his [or her] movements from one place to another.”\(^\text{174}\) Thus, the court held, GPS tracking of plaintiff’s vehicle did not violate his privacy.

In a case applying the Fourth Amendment to a public employer, New York taxi drivers objected to the Taxi Commission’s use of GPS tracking devices on their cabs because the devices would track the drivers’ movements while they were off duty.\(^\text{175}\) The court declined to implement a preliminary injunction, holding the use of GPS tracking likely did not violate the Fourth Amendment because there were adequate safeguards for the security of personal information, the vehicle owners had a strong interest in tracking and protecting the vehicles, and the taxi drivers did not have a legitimate expectation

\(^\text{168}.\) Id. at *7.
\(^\text{169}.\) Id. at *8.
\(^\text{170}.\) Id. at *8–9 (citing United States v. Knotts, 460 U.S. 276, 281 [1983]).
\(^\text{171}.\) Id. at *10.
\(^\text{174}.\) Id. at 651–52, 657 (quoting United States v. Knotts, 460 U.S. 276, 281 [1983]).
of privacy in their movements on public roads. The court also held federal takings claims and New York State constitutional claims were not likely to succeed.

In another case against a public entity, the New York Court of Appeals held that a public employer is not required to obtain a search warrant before installing a GPS device in a public employee’s personal vehicle to investigate misconduct during working hours. The court reasoned that the location of a personal car used by an employee during working hours is no different from a personal photograph on an employee’s desk, and Cunningham’s expectation of privacy in the location of his car, during the hours he claimed to be at work, was diminished by his obligation to report his arrival and departure times to his employer. Still, the court of appeals reversed the lower court’s decision that the warrantless search was reasonable under the circumstances, because the search was not limited to Cunningham’s working hours. Instead, GPS location data was collected and recorded during evening, weekend, and vacation hours. Consequently, the entire GPS search was unreasonable, and the court ruled that the location evidence should have been suppressed from the state’s disciplinary proceeding.

The Supreme Court of Connecticut has also decided a GPS tracking case, though the court did not reach the privacy issues. In Gerardi v. City of Bridgeport, two city fire inspectors brought suit against their employer, the City of Bridgeport and the city’s fire chief, challenging the defendants’ effort to discipline the plaintiffs for improper job performance detected by tracking plaintiffs via GPS without plaintiffs’ knowledge. The issue in the case was whether there was a private right of action under Connecticut’s statute prohibiting an employer from electronically monitoring an employee’s activities without prior notice to the employee. The answer, the court held, was no, so the case was dismissed for failure to exhaust administrative remedies.

GPS tracking of employees arose in the private employer context before the First Circuit in Haggins v. Verizon New England, Inc., but as in Gerardi, the court did not decide the scope of privacy rights,

178. Gerardi v. City of Bridgeport, 985 A.2d 328 (Conn. 2010).
179. Id. at 331–32.
180. Id. at 335.
but rather held the employees’ state law privacy claims were preempted by section 301 of the federal Labor Management Relations Act. Verizon had issued cell phones with GPS capabilities to its employees, who were represented by a union and had a CBA (collective bargaining agreement) with Verizon. The issue of whether the GPS-capable cell phones violated privacy expectations was governed by the CBA’s management rights clause, which incorporated past practices to give content to reasonable privacy expectations. The plaintiff employees’ allegations were under the state constitution and state privacy law and not section 301, so their claims were preempted by federal law and dismissed.

§ 17:4.2 Mobile Devices and Applications

Private location tracking accomplished through mobile devices and smartphones remains the most undeveloped area of location privacy, but legal movement is increasing. As of this writing, there is no legislation specifically directed towards location tracking by mobile applications. The FTC, of course, has jurisdiction to prosecute “unfair or deceptive acts or practices” under section 5 of the FTCA, as discussed in chapter 4 of this treatise, but there are no laws directly applicable to or designed for tracking by mobile applications. Still, the FTC has indicated practices it believes would insulate companies from liability under section 5, and additional legal theories are being tested in the courts.

The FTC categorizes precise geolocation as “sensitive information” that may require additional protection through affirmative express consent.182 Still, “the Commission believes this requirement of affirmative express consent for first-party marketing using sensitive data should be limited.”183 For companies that just incidentally collect and use sensitive information—such as the Amazon.com or Netflix product recommendations based on prior purchases—express affirmative consent may not be required.184 But “where a company’s business model is designed to target consumers based on sensitive data—including . . . geolocation data—the company should seek express

183. FTC STAFF REPORT 2012 at 47 [emphasis in original]; see also FTC PRELIMINARY REPORT 2010, supra note 49, at 61.
For example, the FTC would include mobile operating system providers and mobile app developers in this latter category requiring affirmative express consent.\(^ {185}\) The FTC has also stressed that location information should not be retained longer than necessary because “location information becomes more sensitive if the information is stored over a period of time.”\(^ {187}\)

The FTC is not the only federal agency involved with location privacy. In May 2012, the Federal Communications Commission [FCC] issued a report entitled *Location-Based Services: An Overview of Opportunities and Other Considerations.*\(^ {188}\) Like the FTC, the FCC report encouraged transparent notice of a company’s privacy practices and meaningful consumer choice with respect to collection and use of personal information.\(^ {189}\) The FCC also stressed data security and minimization—the “idea that a company will only retain personal information it actually needs and only for the amount of time that it is needed.”\(^ {190}\) The Department of Commerce [DOC] and the White House have discussed similar privacy ideals in their own reports.\(^ {191}\)

The FTC, FCC, and DOC reports, however, do not carry the force of law, and cases are just beginning to test the applicability of various legal theories to mobile location tracking. For example, in October 2011, consumers filed a putative class complaint in federal court against Accuweather.com, Inc. and HTC America, Inc. alleging that the collection, without consent, of users’ location data via the Accuweather mobile application violated state consumer protection laws.\(^ {192}\) After a motion to dismiss, the court ruled that the plaintiffs had sufficiently plead injury to meet Article III standing: the accepted injuries were overpayment for their phones (because the plaintiffs

\(^ {185}\) Id. at 47.
\(^ {186}\) FTC STAFF REPORT 2013 at 15–16, 23–24.
\(^ {187}\) FTC PRELIMINARY REPORT 2010 at 60, n.121; FTC STAFF REPORT 2012 at 33.
\(^ {189}\) Id. at 19–27.
\(^ {190}\) Id. at 30 [noting that law enforcement interests may support holding data for longer periods of time].
would have paid less if they had known their location was to be collected as alleged] and diminution in value of the phones because of reduced battery life as a result of the collection of location data. However, the alleged misappropriation of the plaintiffs’ location data was not a sufficiently particularized injury to establish standing, so many of the plaintiffs’ location-based claims were dismissed. The case was ultimately settled.

In another case against a mobile application developer, a putative class of plaintiffs sued Path, Inc. alleging that the company’s mobile application uploaded to Path’s servers the class members’ personal information, including location information. Path moved to dismiss, arguing the plaintiff lacked standing and failed to state a claim on which relief could be granted. The court found the alleged harm of diminished mobile device resources (battery life, storage, and bandwidth) was de minimis and could not confer standing; the alleged threat of future harm due to a security risk to plaintiff’s personal information did not constitute an injury-in-fact; but the alleged harm of spending time and money to remove the tracking software (plaintiff alleged it would cost $12,250 to have a trained technician do so) was sufficient to confer standing. The court then found four of plaintiff’s nine causes of action sufficiently stated a claim for relief: claims under California’s Computer Crime Law, claims under California’s Unfair Competition Law, claims of negligence; and claims of unjust enrichment.

As the Accuweather case evidences, standing is a major hurdle for plaintiffs alleging injury from location tracking practices. In In re iPhone Application Litigation, a large putative class action in the Northern District of California against Apple, plaintiffs essentially asserted that applications available for free in Apple’s App Store allowed the disclosure of personal information, including location data, to defendants without plaintiffs’ consent or knowledge and in contravention of Apple’s privacy policy. The case is a consolidated multi-district litigation involving nineteen putative class action lawsuits. The first consolidated complaint was dismissed for lack of standing in an opinion holding that the collection of data does not

194. Id.
197. Id. at *9–24.
199. Id.
constitute a particularized injury in itself. The plaintiffs then filed an amended complaint with thirteen causes of action, including counts under the Stored Communications Act, the Electronic Communications Privacy Act, the Wiretap Act, the California Constitution, the Computer Fraud and Abuse Act, and various consumer protection statutes. This was dismissed at summary judgment on standing grounds for failure to show a causal connection between the alleged injury of overpaying for phones and the alleged misrepresentations regarding privacy and collection of location information.

After a second motion to dismiss, the court noted that violations of the SCA can serve as a concrete injury for Article III standing, and the iPhone plaintiffs alleged a number of additional injuries: the defendants’ actions consumed finite bandwidth and storage space on the devices; the transmission of personal data was done without encryption, exposing plaintiffs to “unreasonable risks” of interception; and as in Accuweather, that plaintiffs would have paid less for the devices if they had known of defendants’ data-collection practices. The court found plaintiffs had sufficiently alleged standing and moved to the sufficiency of plaintiffs’ claims.

The court found the plaintiffs failed to state a claim under the SCA because their mobile devices could not be deemed “facilit[ies] through which an electronic communication service is provided” and because plaintiffs failed to allege that defendants accessed data in “electronic storage” as required by the SCA. Likewise, the plaintiffs failed to state a claim under Title I of the ECPA (the Wiretap Act), which requires interception of the contents of communications. Location data did not constitute content of communications. The plaintiffs’

201. In re iPhone Application Litig., No. 11-MD-02250, Dkt. No. 25 [N.D. Cal. Nov. 22, 2011].
204. Id. The SCA defines “electronic storage” as “(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17). The plaintiffs alleged that iPhones and iPads stored a log of location and other data as often as 100 times a day for up to one year, so the court found it was not temporary or intermediate storage incidental to an electronic transmission.
claims also fell short of constituting a cognizable claim under the Computer Fraud and Abuse Act or the California Constitution. However, the court allowed two state claims to proceed: (1) a claim under California’s Consumer Legal Remedies Act alleging unfair or deceptive acts or practices; and (2) claims under California’s unfair competition statute.

A similar multi-district putative class action is pending against Google, a Google-owned mobile advertising network, and its subsidiary. In that case, plaintiffs used mobile devices with Google’s Android operating system and alleged that the operating system allowed applications to access, without authorization, plaintiffs’ personal information, including location information, and transmit the data to third parties. This practice caused injury, the plaintiffs alleged, by the diminution in value of their personal information (claimed as property) and diminution of battery life. The plaintiffs brought claims under the Computer Fraud and Abuse Act, California’s constitutional right to privacy, California’s Invasion of Privacy Act, California’s Computer Crime Law, consumer protection statutes, negligence, and trespass. After the defendants’ motion to dismiss, the court found plaintiffs’ allegation of diminished battery capacity due to the collection of location information was sufficient for Article III standing. However, the court joined other decisions holding that alleged lost value in private information does not confer standing. The Android Consumer Privacy court proceeded to dismiss plaintiffs’ claims with leave to amend.

In a second putative class action against Apple in the Northern District of California, the named plaintiff is alleging that Apple failed to prevent third-party software applications from uploading user information, including location information, without permission. The plaintiff asserted various consumer protection violations, violation of California’s False Advertising Law, negligence, and unjust

207. Id.
208. In re Google Android Consumer Privacy Litig., 11-MD-02264 [N.D. Cal. 2013].
210. Id.
211. Id.
enrichment. The court dismissed the first complaint with leave to amend, holding the plaintiff lacked standing because the future risk of misappropriation of personal information did not constitute an injury-in-fact, and the plaintiff failed to adequately plead how Apple’s alleged misrepresentations caused her to purchase an Apple device.

The plaintiff’s second amended complaint, however, survived Apple’s motion to dismiss. Pirozzi alleged that Apple’s website in 2011 contained a statement that “apps requesting location information must get your permission first.” She alleges that that was not in fact true, that she read that statement before purchasing her iPhone, and was “misled as to the nature and integrity of Apple’s products.” Pirozzi’s allegation that she overpaid for her iPhone as a result of Apple’s alleged misrepresentation was enough to satisfy the injury, causation, and redressability requirements of Article III standing.

Microsoft is also involved in smartphone privacy litigation and is a defendant in a case alleging that it tracked the location of Windows Phone users after those users expressly denied it permission to do so. The court dismissed four of the plaintiff’s five claims but allowed the SCA claim to continue. The four dismissed claims included a claim under the Wiretap Act, under Washington’s Consumer Protection Act, under Washington’s Privacy Act, and a claim for unjust enrichment. The Wiretap Act claim was dismissed because it requires interception of the contents of a communication, and location data did not constitute the contents of a communication. The Consumer Protection Act and unjust enrichment claims failed because the plaintiff provided no support for the assertion that the alleged tracking diminished the phone’s market value and thus did not meet federal pleading standards. The Washington Privacy Act claim was dismissed because the Privacy Act protects communications between two individuals, not location data collected by a third party.

214. Id.
218. Id.
220. Id.
221. Id. [citing Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007); Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)].
222. Id.
Citing to In re iPhone Application Litigation, Microsoft moved for certification for immediate appeal, arguing there is substantial ground for disagreement with the court’s conclusions that a mobile device can be a “facility” under the SCA and that location data constitutes an “electronic communication” held in “electronic storage” under the SCA.\textsuperscript{223} The court declined to certify an interlocutory appeal, holding that the Ninth Circuit would benefit from a developed factual record when assessing the issues.\textsuperscript{224}

So, there are multiple cases in the federal district courts of the Ninth Circuit, coming to differing conclusions, and setting the stage for at least one appellate decision on the matter.

\textbf{§ 17:4.3 Other Location Technologies}

\textbf{[A] Radio Frequency Identification}

As discussed in chapter 5 of this treatise, fifteen states have passed legislation addressing the use of RFID technology. California, for example, prohibits any unauthorized “skimming” or reading of RFID tags in identification cards.\textsuperscript{225} Nevada prohibits capturing, storing, or reading information from a person’s RFID-enabled identification document for the purpose of knowingly or intentionally committing fraud, identity theft, or any other unlawful act, without that person’s prior knowledge and consent.\textsuperscript{226} Rhode Island prohibits the use of RFID technology for the purpose of tracking the movement or identity of students.\textsuperscript{227} And Washington prohibits, with a few exceptions, scanning an RFID tag by anyone other than the business or agency that issued the tag.\textsuperscript{228}

RFID has also come under judicial scrutiny. A high school student in Texas refused to wear her RFID badge on constitutional grounds, including religious freedom grounds.\textsuperscript{229} The district court denied the student’s motion for a preliminary injunction. The court noted that the RFID badges are designed to improve safety in the school and more accurately track attendance. The preliminary injunction was denied because the court found no likelihood of success on the merits; the student plans an appeal to the Fifth Circuit.

\begin{itemize}
  \item\textsuperscript{223} 2012 U.S. Dist. LEXIS 179197, at *2.
  \item\textsuperscript{224} Id.
  \item\textsuperscript{225} CAL. CIV. CODE §§ 52.7, 1798.79, 1798.795.
  \item\textsuperscript{226} NEV. REV. STAT. §§ 205.461–205.4657.
  \item\textsuperscript{227} R.I. GEN. LAWS § 42-153-1.
  \item\textsuperscript{228} WASH. REV. CODE §§ 19.300.010, .020, .030.
\end{itemize}
Vehicle Tracking

Regarding license plate tracking, only a few states directly regulate the technology. These include New Hampshire, which bans license plate scanners entirely, and Maine, which restricts license plate scanning to government agencies and requires license plate data to be deleted after twenty-one days, unless part of an investigation. Arkansas limits private use of license plate readers, prohibits any sharing of data unless evidence of an offense, and requires captured data that is not part of an ongoing investigation to be deleted within 150 days. Additionally, the Virginia Attorney General issued an advisory opinion concluding that the state’s Government Data Collection and Dissemination Practices Act prohibits state law enforcement from using license plate readers for passive data collection. Instead, license plates can only be used actively—in pursuit of a particularly identified license plate “evaluated and determined to be relevant to criminal activity.” Conversely, the New Jersey Attorney General issued a directive requiring all New Jersey law enforcement agencies to retain license plate reader data for five years and contemplates data-mining and pattern analysis of the captured plate data “to detect suspicious activities.”

§ 17:5 Legislative Outlook

§ 17:5.1 Federal Proposals

Lawmakers have expressed willingness to act in relation to location privacy issues. For example, in 2011, Senator Charles Schumer (D-NY) called for the Federal Trade Commission to investigate OnStar’s revised privacy policy, which would have allowed it to sell GPS-derived and other anonymized data related to its customers. In response to Senator Schumer and public pressure, OnStar later


reversed its decision. In 2012, Senator Schumer again called for an FTC investigation, this time into iPhone and Android privacy policies. The Senator’s expressed concern was that consumers were not aware of the data they were releasing to companies by accepting privacy policies on iPhone and Android devices. To date, the FTC has not taken action on the matter, but as discussed above, private lawsuits like *In re iPhone Application Litigation* addressing mobile privacy are working their way through the courts.

Federal lawmakers have also taken action by proposing legislation. In 2013, The Preserving American Privacy Act was introduced, which if passed would establish due process protections for Americans against government-operated domestic drones. Representative Bobby Rush (D-IL) sponsored the Best Practices Act in February 2011. This act would have defined “sensitive information” to include “precise geolocation information.” In the 112th Congress, a number of bills addressing location privacy were introduced, but none was ultimately passed before the end of the session in January 2013. Senator Al Franken (D-MN) introduced the Location Privacy Protection Act of 2011, which would have required affirmative opt-in consent before a covered entity could collect, receive, record, obtain, or disclose location information collected by an electronic communication device. Senator Richard Blumenthal (D-CT) introduced the Personal Data Protection and Breach Accountability Act of 2011, which would have enhanced criminal and civil penalties for theft of personally identifiable information, including location information. The bill would have required notification and remedies to consumers affected by a data breach. Then-Senator John Kerry (D-MA) and Senator John McCain (R-AZ) collaborated on the Commercial Privacy Bill of Rights Act of 2011, which would have instructed the FTC to create a comprehensive regulatory framework for entities collecting personally

---


236. *Id.*

237. The Preserving American Privacy Act, H.R. 637, 113th Cong. [2013].


239. Location Privacy Protection Act of 2012, S. 1223, 112th Cong. [2012].


241. *Id.*
identifiable information, including location information.\textsuperscript{242} Similar bills were also introduced in the House of Representatives.\textsuperscript{243}

\section*{\textsection{}17:5.2 State Legislation}

State lawmakers are equally busy in the location privacy arena. For example, at least eight states have enacted legislation regarding unmanned drones.\textsuperscript{244} Laws in Florida, Idaho, Illinois, Montana, Oregon, and Tennessee would require law enforcement to obtain a probable cause warrant before using a drone to gather evidence in a criminal investigation. Some state laws also include data retention limits. Illinois has a thirty-day data retention limit when the data is not evidence of a crime or part of an ongoing criminal investigation, and Tennessee has a twenty-four-hour data retention limit for data collected on an individual, home, or other areas that are not the target of the investigation. Law enforcement officials in Montana and Oregon must meet the same probable cause standards applicable to using their own drones in an investigation before acquiring information from a third-party drone. Montana and Oregon also specify that information collected by a drone cannot be used as part of an application for a warrant. In other words, law enforcement drones cannot just troll for evidence of a crime.

Some of these laws apply to private use of drones as well. Idaho, for example, prohibits photography or recording by drones if an individual will profit from the recording or image. Texas prohibits capturing an image of an individual or private property “with the intent to conduct surveillance.” In Oregon, flying a drone less than 400 feet above another’s private property is prohibited if the person has previously flown a drone over the property and been asked not to do it again.

Virginia’s law simply implements a two-year moratorium on drone use to provide time to craft a set of regulations.

\begin{itemize}
\item \textsuperscript{242} Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011).
\end{itemize}