You Are Here: Tracking Around the Fourth Amendment to Protect Smartphone Geolocation Information with The GPS Act

By P. Kramer Rice*

I. INTRODUCTION................................................................. 18
II. THE SMARTPHONE REVOLUTION AND THE BIRTH OF GEOLOCATION INFORMATION.................................................... 21
   A. Mobile Phones and CSLI.................................................. 21
   B. Smartphones, Geo-apps, and GLI....................................... 22
   C. Law Enforcement’s Interest in Mobile Phone Data............... 23
III. THE FOURTH AMENDMENT, THE ECPA, AND THE GPS ACT...... 24
   A. Fourth Amendment..................................................... 24
   B. ECPA and GPS Act...................................................... 26
      1. ECPA........................................................................ 26
      2. House Bill 1312: The GPS Act....................................... 28
IV. PROVIDING FOURTH AMENDMENT PROTECTION WHERE THE FOURTH AMENDMENT MAY NOT BE IMPlicated: THE GPS ACT AND SMARTPHONES................................................... 29
   A. The GPS Act’s Promise of a Workable Definition, Standard, and Remedy for Smartphones........................................ 29
   B. The Fourth Amendment and the Third-Party Doctrine’s Impact on Smartphones...................................................... 32
V. CONCLUSION ........................................................................ 33

* P. Kramer Rice is a graduate of Notre Dame Law School, with honors, and has been published on issues associated with the Second Amendment as well as federal and state employment law.
I. INTRODUCTION

On June 6, 2013, President Barack Obama publicly acknowledged PRISM, the National Security Administration’s clandestine electronic data surveillance program that collects individuals’ personal information from various electronic platforms, particularly cellular telephones.\(^1\) In response, people across the country decried the program and its interception of phone data as an affront to civil rights, with one academic going as far as to demand a “Digital Bill of Rights.”\(^2\) While a Digital Bill of Rights theoretically would provide substantive protections for the everyday mobile phone user, it could neither be legislatively representative of national conceptions of electronic privacy nor judicially secured in light of the federal government’s compelling interest in national security, even if enacted. Yet, as people clamor for data protection in a data-soaked society, Congress should heed the interests of the electorate. Inasmuch, instead of adopting an ineffective Digital Bill of Rights, Congress could adopt procedural safeguards ensuring that the government cannot obtain everyday data from domestic cell phones

---


Even the most fundamental rights implicit in the concept of ordered liberty can be overcome by a compelling interest narrowly tailored; however, such governmental tailoring still needs to comply with due procedural safeguards. See, e.g., Griswold v. Connecticut, 381 U.S. 479, 501-02 (1965) (citing Papel v. Connecticut, 302 U.S. 319 (1937) (Harlan, J., concurring) (laying out a means-ends fit to judicial review of fundamental liberties)).
without demonstrating heightened cause. Although the once primary function of cellular telephones to make telephone calls is now secondary to ensuring phone owners can stay connected with those beyond whom they simply speak with over the phone, the wealth of collectable data from peoples’ phones may warrant some level of protection.\(^4\)

In a smartphone era, people use their mobile phones for real-time, turn-by-turn directions and to broadcast locations and pictures on social networking accounts, resulting in both personal and locational data which, taken together, can produce an electronic profile of the user.\(^5\) Smartphone owners maximize the utility of their phones by installing applications, colloquially known as “apps,” many of which purposefully draw upon the geolocation privacy and surveillance (“GPS”) technology of smartphones to allow users to stay connected with the world at large by broadcasting their geographical location.\(^6\) While these “geo-apps” are but one of the many applications that blend the old technology of making and receiving phone calls with the ever-increasing and always-expanding use of GPS technology in smartphones, this technology represents a new challenge to Fourth Amendment jurisprudence concerning how the government collects mobile phone location data, traditionally known as cell site location information (“CSLI”), to geographically pinpoint and apprehend suspected lawbreakers, potentially even domestic terrorists.\(^7\)

\(^4\) Haley Plourde-Cole, Note, Back to Katz: Reasonable Expectation of Privacy in the Facebook Age, 38 FORDHAM URB. L.J. 571, 575 (2010) (discussing how cell phones are now “portable computers” capable of connecting to the internet and emailing people).


\(^6\) See infra Part I.B.

\(^7\) See infra Part III.A. Cases involving contemporary issues surrounding GPS technology and cellular phone location data have inconsistently applied prior case
The Fourth Amendment guarantees Americans the right to be free from “unreasonable searches and seizures,” and whether there exists a “reasonable expectation of privacy” is the threshold consideration as to whether such a search in fact occurs. Even though particular circumstances influence conceptions of reasonableness, judges are tied to a collection of Fourth Amendment precedents too technologically outdated to resolve the circumstances concerning contemporary CSLI from smartphones. In order to fill these gaps in the Fourth Amendment and associated precedent, Congress has proposed House Bill 1312, known as the Geolocation Privacy and Surveillance Act (“GPS Act”), as an amendment to the existing and imprecise privacy protections under the Electronic Communications Privacy Act (“ECPA”) and its provisions within the Stored Communications Act (“SCA”). In concert with the proposed privacy provisions of the GPS Act, an amended ECPA would create a more precise statutory framework governing the development of rationales and holdings involving the Fourth Amendment and geographic tracking devices. Compare United States v. Jones, No. 10-1259, slip op. at 9 (Jan. 23, 2012) (applying common law trespass analysis rather than Fourth Amendment reasonable expectation of privacy analysis derived from tracking beeper cases United States v. Knotts and United States v. Karo (in case involving GPS tracking device attached to car), with In re Application of the U.S. for an Order Directing a Provider of Elec. Comm’n Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 312–13 (3d Cir. 2010) (hereinafter In re Order) (analyzing retrieval of cellular location data from mobile phone by considering the Fourth Amendment tracking beeper cases United States v. Knotts and United States v. Karo.

See infra notes 3034. The Fourth Amendment likely would apply to American citizens abroad. See Reid v. Covert, 354 U.S. 1, 6 (1957) (plurality opinion) (“When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provide to protect his life and liberty should not be stripped away just because he happens to be in another land.”).


See infra Part II.B.
modern-day CSLI derived from GPS-equipped smartphones.\footnote{See infra Part III.}

This Note argues that an amended ECPA, through the GPS Act, would be both statutorily poised for judges to analyze with greater faculty the privacy issues associated with governmental requests for domestic GLI derived from smartphones and geo-apps, as well as procedurally demonstrative of Congress’s ability to enact statutes capable of keeping abreast of privacy issues that ever-evolving smartphone technology will always implicate. Part I provides an overview of smartphone technology as it pertains to GPS technology and geo-apps, and how modern-day technology and GLI differ from corresponding technology and CSLI in traditional cell phones. Part II discusses the applicable telephone-based jurisprudence of the Fourth Amendment, the ECPA-SCA treatment of CSLI, and the regulations of GLI in the GPS Act. Part III analyzes how the ECPA, pursuant to the GPS Act, would govern effectively GLI, and how the Fourth Amendment need not be considered in this extensive statutory framework covering smartphones.

II. THE SMARTPHONE REVOLUTION AND THE BIRTH OF GEOLOCATION INFORMATION

A. Mobile Phones and CSLI

To pinpoint a traditional cell phone’s location, one has to rely on the cell phone’s innate cellular technology.\footnote{See generally Susan Freiwald, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact, 70 Md. L. Rev. 681, 702–15 (2011) (detailing technology of cell phones and cell location data generated from that technology).} Cell phones send radio waves to cell towers placed throughout service areas, and as the phone travels within that area the phone constantly communicates with the nearest cell tower to ensure service.\footnote{Id. at 702–03,} The frequency to which this information is refreshed with the nearest tower, or its “periodicity,” determines the quality of any subsequently positioned location.\footnote{Id. at 703.} The cell site data points created during this process occur both voluntarily—when the cell phone is actually used and connects with a cell tower—and involuntarily—through the constant
registration process for ensuring service. The collection of this information is cell site location information, or CSLI, and the substance of the data and the resulting precision can contribute to a comprehensive understanding of the phone user’s movements.

B. Smartphones, Geo-apps, and GLI

Smartphones are quickly replacing traditional cell phones, with many people purchasing smartphones for the purpose of utilizing the GPS technology and geo-apps. Unlike their cell phone predecessors, smartphones come pre-equipped with GPS technology, which is more precise in calculating location than previous calculations of CSLI. In fact, when smartphone users activate their geo-app GPS technology, it has the capacity to pinpoint their real-time location down to the street corner. Moreover, users are increasingly linking this smartphone geo-app information to social media. For example, users of the smartphone application Foursquare affirmatively

---

15. The following forms of data points are created voluntarily when the user receives and/or makes a phone call: “initiation and termination data” at the beginning and ending times of the call, “data from pinging” when the target is called, “duration data” that occurs during rather than at the beginning or ending of the phone call, and other forms of communication instead of voice calls, such as texting. *Id.* at 703-09. Some courts distinguish between making and answering a phone call, finding that making a phone call is affirmative while taking a phone call is not. *Id.* at 705 n.135 (citing United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *89 (N.D. Ga. Apr. 21, 2008). Involuntarily, cell phones repeatedly create “registration data” when in communication with cell towers, regardless of whether the owner is making or receiving a call. *Id.* at 705.

16. See Freiwald, supra note 12, at 715 (suggesting location data, even in basic form, contains rich information permitting law enforcement to understand the private life of the phone owner).

17. See *id.* at 713 (noting GPS technology is standard on smartphones so that phone owners can take advantage of geo-location applications).

18. See United States v. Jones, 132 S.Ct. 945, 963 (Jan. 23, 2012) (Alito, J., concurring) (comparing older phones, where the accuracy of the location information depends on the density of the tower network, to new smartphones, equipped with a GPS device to permit more precise tracking); Freiwald, supra note 12, at 713 (noting that GPS data is the most efficient technique of targeting a location and a person at that location).

19. See Plourde-Cole, supra note 4, at 574-76 (noting that GPS location features are used in a variety of applications, including street directions, mapping, finding restaurants, and locating other smartphone users).

20. See *Jones* 132 S.Ct. at 963 (Alito, J., concurring) (“[P]hone-location-tracking services are offered as ‘social’ tools, allowing consumers to find (or to avoid) others who enroll in these services.”).
broadcast their location by “checking in” at any place or location, sharing their location with family and the social media network.\textsuperscript{21} The result is a collection of information on the location of the smartphone generated from use of the phone’s GPS technology and geo-apps, or geolocation information (“GLI”).\textsuperscript{22} In contrast to the potential involuntary creation of CSLI, smartphone owners acknowledge the existence of and affirmatively create GLI by purchasing, utilizing, and linking smartphone location technology.\textsuperscript{23} Therefore, ignorance as to promises and perils of this technology cannot exist where users encounter associated privacy statements alerting them to the potential, or even likelihood, that such GLI will be created and become shared information.\textsuperscript{24}

\textbf{C. Law Enforcement’s Interest in Mobile Phone Data}

Law enforcement groups have developed a handful of techniques to elicit records of CSLI in an effort to obtain evidence against suspected lawbreakers as well as to thwart future criminal activity, most specifically potential terrorist attacks, by crafting character profiles of suspicious individuals.\textsuperscript{25} Law enforcement

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{21} See id. at 576 (noting other geolocation-inspired social media applications include Google Latitude and Facebook Places.)
\item \textsuperscript{22} See infra Part II.B.2.
\item \textsuperscript{23} See Jones, 132 S.Ct. at 963 (noting how users must “activate the GPS” on smartphones); see Plourde-Cole, supra note 4, at 623-25 (suggesting GPS technology in smartphones and associated applications disseminate information without the permission or knowledge of the user).
\item \textsuperscript{24} See Plourde-Cole, supra note 4, at 612 (noting that in addition to the disclosures contained within the privacy statements, geoapps have privacy settings informing the users about how, and permitting them to, control location information).
\item \textsuperscript{25} Such techniques include calculating cell phone positions from cell tower face data when towers are placed fifty feet apart and triangulating a position mathematically by drawing lines from multiple source points and finding a point of connection somewhere in the middle. Id. at 710, 712. Some, but not all, cell phones include GPS technology to comply with federal emergency laws. See id. at 713 (noting that traditional cell phones may come equipped with GPS technology so that service providers can abide by federal regulations requiring pinpointed locations during emergency phone calls). The sole use of GPS technology on cell phones for emergency purposes, however, is technologically and practically different than its primary use on smartphones. See also Jones, No. 10-1259, slip op. at 2 (U.S. January 23, 2012) (Sotomayor, J., concurring) (suggesting with increased use of smartphones, the Government will be more capable of duplicating GPS monitoring to create personal profiles of suspects through GPS-enabled smartphones).
\end{enumerate}
\end{footnotesize}
repeatedly seeks CSLI in order to obtain evidence against suspected
drug smugglers. For example, in United States v. Forest, federal Drug
Enforcement Agents obtained CSLI from Forest’s cell phone through
the service provider to determine whether he had traversed certain
states in order to conduct drug operations. Law enforcement also
monitors captured GLI to create a character profile of potential
terrorists. The National Security Administration’s (“NSA”)
clandestine surveillance program, PRISM, efficiently captures most
telecommunications data because such data travels through the
United States, affording the country an acute ability to obtain and
track that data by collecting it “direct[ly]” from the servers of
telecommunications companies. The NSA purportedly utilized
PRISM to capture mobile phone data from citizens suspected of
supporting terrorism and these citizens’ suspected accomplices.
Demonstratively, as more criminals, terrorists, and the countries in
which they operate, become more technologically advanced and GLI
is sent more frequently through the United States, the laws associated
with obtaining useful information contained domestically may need
to adapt and balance the need for national security against the need
for civil rights protections.

III. THE FOURTH AMENDMENT, THE ECPA, AND THE GPS ACT

A. Fourth Amendment

The Fourth Amendment affirms, “[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 . . .” A
search occurs for purposes of the Fourth Amendment when the
government violates an individual’s “reasonable expectation of

See, e.g., United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (tracking
cocaine), Kara, 468 U.S. 705 (tracking ether), Knotts, 460 U.S. 278 (tracking
chloroform).

Forest, 355 F.3d at 947.

See Timothy B. Lee, Here’s Everything We Know About PRISM to Date, THE
WASHINGTON POST, June 12, 2013, available at
http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-
everythingweknowaboutprism-todate/.

See id.

U.S. CONST. amend. IV.
privacy. The inquiry into whether a reasonable expectation of privacy has been violated is two-part: first, whether the individual, by his or her conduct, has exhibited an “actual (subjective) expectation of privacy;” and two, whether the individual’s subjective expectation of privacy is objectively reasonable, or “one that society is prepared to recognize as ‘reasonable’… The subjective prong considers whether the individual has shown that he or she seeks to preserve the matter at issue privately, and the second prong considers the circumstances to determine whether the individual’s expectation is objectively justifiable. In order to conduct a search properly under the Fourth Amendment, “[n]o warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” If law enforcement conducts a search improperly, either for failing to obtain a warrant or for inadequately describing the object to be seized, the Fourth Amendment mandates exclusion of that evidence in a judicial proceeding.

While technological advances have affected the manner in which the Fourth Amendment protects against unreasonable searches, the constitutional standards applied to these developments have reaffirmed established precedent. In Smith v. Maryland, the Supreme Court used its two-pronged test to hold that the installation of a pen register, a device that records the numbers dialed from a telephone, did not constitute a Fourth Amendment search, reasoning that Smith knew he had to convey numerical information to the phone company and thus assumed the risk that such information would be handed to

---

33 Id.
34 U.S. CONST., amend. IV.
35 See Forest, 355 F.3d at 950. The Fourth Amendment’s exclusionary rule is implicated, but not applicable, if a court decides that an exception to the rule applies. See, e.g., United States v. Powell, No. 12-cr-20052, 2013 WL 1876761, at *5960 (D. Mich. 2013) (holding good faith exception to warrant applied); United States v. Lee, 862 F. Supp. 2d 560, 571 (D. Ky. 2012) (holding good faith exception did not apply to warrant requirements).
36 See Kyllo v. United States, 533 U.S. 27, 33-34 (2001) (“It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”). Historically, Fourth Amendment violations were based solely upon the common law of trespass; however, this changed with the advent of electronic surveillance. See id. at 31.
the police; therefore, no demonstration of probable cause was necessary.\textsuperscript{37} Similarly, twenty-five years later in \textit{United States v. Forest}, the Sixth Circuit held that the Drug Enforcement Agency had not unlawfully searched Forest by obtaining his CSLI in order to track the whereabouts of his automobile in an alleged drug smuggling operation because he had no reasonable expectation of geolocational privacy when traveling on public highways.\textsuperscript{38}

\textbf{B. ECPA and GPS Act}

\textbf{1. ECPA}\textsuperscript{39}

Due to the growth and development of electronic communication, holes in Fourth Amendment protection for that data, the desire of law enforcement to retrieve that data in investigations, and the push from users to keep such data private, Congress enacted the ECPA, which includes the SCA.\textsuperscript{40} The ECPA and SCA contain specific definitions that implicate smartphones and their associated data. Title I defines tracking devices as “an electronic or mechanical device which permits the tracking of the movement of a person or object.”\textsuperscript{41} Title II contains the SCA, and the SCA controls access to stored communications and transaction records.\textsuperscript{42} The SCA establishes two categories of information that implicate smartphones: contents of wire or electronic communications and subscriber records concerning “electronic communication service.”\textsuperscript{43} An “electronic communication service” includes providers of “wire or electronic communications.”\textsuperscript{44} Wire communication is defined as:

\textsuperscript{37} Smith, 442 U.S. at 743-44. The register was also attached to telephonic equipment at the telephone company, precluding a claim based in trespass. \textit{Id.} at 741.

\textsuperscript{38} Forest, 355 F.3d at 951-52.


\textsuperscript{40} See Malone, supra note 5, at 716 (noting “Congress enacted the SCA to provide statutory protection of personal information where people were demanding it and traditional Fourth Amendment protections were lacking”); Lisa M. Lindemann, \textit{From Cell to Slammer: Flaws in the Hybrid Theory}, 53 \textit{Ariz. L. Rev.} 663, 672 (2011) (“The ECPA is the authoritative statutory law governing electronic surveillance.”)

\textsuperscript{41} 18 U.S.C. § 3117(b) (2012).


\textsuperscript{43} See id. § 2703(a); § 2703(c).

\textsuperscript{44} See In re Application of the U.S. for an Order, 620 F.3d at 310 (emphasis in original) (citing 18 U.S.C. § 2510(15)).
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... furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce[.]\(^5\)

Electronic communication is defined as:

[An]y transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—(A) any wire or oral communication;... (C) any communication from a tracking device (as defined in section 3117 of this title).\(^6\)

As the distinct definitions suggest, tracking devices, wire communications, and electronic communications each possess different access requirements. For tracking devices under Title I and contents of a wire or electronic communication under Title II, law enforcement must demonstrate probable cause to obtain a search warrant to gain access to the information sought.\(^7\) For Title II subscriber records, law enforcement groups seeking certain subscriber records need not obtain a warrant so long as they can obtain a court order upon proving “specific and articulable facts... showing reasonable grounds to believe that... the records or other information sought, are relevant and material to an ongoing criminal investigation.”\(^8\) In comparison with the high standard of probable cause, the “specific and articulable facts” standard is an intermediate standard between an administrative subpoena and a probable cause warrant.\(^9\) Notably, the SCA does not require the exclusion of non-content communications if improperly obtained, which potentially

---

\(^5\) 18 U.S.C. § 2510(1).


\(^7\) See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 752 (S.D.Tex. 2005) [hereinafter In re Pen Register] (Rule 41 of Criminal Procedure).

\(^8\) 18 U.S.C. § 2703(d); see, e.g., In re Application of the U.S. for an Order, 620 F.3d at 310 (finding CSLI is wire communication and thus does not implicate tracking device consideration).

\(^9\) See In re Pen Register, 396 F. Supp. 2d at 752.
implicates subscriber records.\textsuperscript{50}

2. House Bill 1312: The GPS Act\textsuperscript{51}

Originally introduced in the House of Representatives in 2011, the House reintroduced the GPS Act in 2013.\textsuperscript{52} The GPS Act is a proposed amendment to the ECPA and is designed to fill the outdated void of the ECPASCA regarding GPS technology.\textsuperscript{53} The amendment addresses this void by employing the idea of cell site location information in its definition of “Geolocation Information,” or “any information that is not the content of a communication, concerning the location of a wireless communication device or tracking device [as defined in ECPA Title I]” and 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.”\textsuperscript{54} In defining “Geolocation Information Service,” the revised definition of electronic communication service includes the production of GPS information through mobile phones.\textsuperscript{55} The Act generally prohibits the interception of GLI, permitting an investigative law enforcement officer to obtain a warrant for proper interception of GLI only when it can show

\begin{addendum}
\item See also Lindemann, supra note 40, at 687 (noting Pen/Trap Statute nor the SCA required the exclusion of noncontent communications if improperly obtained); See generally 18 U.S.C. §§ 2707-2708 (2012).
\item See id. It has companion legislation in the Online Communications and Geolocation Act and Location Privacy Protection Act. See Online Communications and Geolocation Act, H.R. 983, 113th Cong. (2013) (providing safeguards for online communication such as e-mails); Location Privacy Protection Act, S. 1223, 113th Cong. (2013) (providing safeguards against corporations providing geolocational information to the government).
\item See generally 18 U.S.C. §§ 2701-2712; see also Plourde-Cole, supra note 4, at 589 (noting ECPA does not explicitly refer to cell site or other location information from a cell phone).
\item H.R. 1312 § 2601(3).
\item See id. § 2703(a); id. § 2703(c); see In re Application of the U.S. for an Order, 620 F.3d at 310 (emphasis in original) (citing 18 U.S.C. § 2510(15)); H.R. 1312 § 2601(4) (“The term ‘geolocation service’ means the provision of a global position service or other mapping, locational, or directional information service to the public, or to such a class of users as to be effectively able to the public, by or through the operation of any wireless communication device, including any mobile telephone, global position system receiving device, mobile computer, or other similar or successor device.”).
\end{addendum}
probable cause; there is no lower standard. The remedy for violation of the Act is the exclusion of the misappropriated GLI.

IV. PROVIDING FOURTH AMENDMENT PROTECTION WHERE THE FOURTH AMENDMENT MAY NOT BE IMPLICATED: THE GPS ACT AND SMARTPHONES

A. The GPS Act’s Promise of a Workable Definition, Standard, and Remedy for Smartphones

Since the adoption and application of the ECPA-SCA, courts and commentators have struggled to uniformly apply the provisions to cell phones and their location data, disagreeing as to whether and to what extent stored historical CSLI can turn a mobile phone into a tracking device and whether CSLI is a wire or electronic communication. Under the current ECPA, the distinctions of whether a mobile phone is a tracking device and whether the data emitted is electronic or wire are noteworthy because if a cell phone is a tracking device and the CSLI emitted is electronic communication, the higher probable cause standard applies. Yet, if the CSLI derives from a wire communication, the lower “articulable facts” standard applies even if the mobile phone is a tracking device, as the definition of wire communications does not exclude tracking devices as does the definition of electronic communications. Much of the

---

50 See H.R. 1312 § 2602(h)(2) (“A governmental entity may intercept geolocation information or require the disclosure by a provider of covered services of geolocation information only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure [Rule 41].”).

51 See id. § 2603 (prohibiting use as evidence of wrongfully acquired geolocation information).

52 Prospective CSLI is generally accepted as qualifying a phone as a tracking device. See, e.g., In re Pen Register, 396 F. Supp. 2d at 759 (finding real-time CSLI transforms mobile phone into tracking device and thus is not electronic communication). Compare Freiwald, supra note 12, at 738-39 (suggesting historical CSLI can give intricate insight into a target’s movements), with In re Application of the U.S. for an Order, 620 F.3d at 312-13 (finding that historical CSLI does not necessarily transform a mobile phone into a tracking device), and Malone, supra note 5, at 727 (suggesting historical CSLI does not qualify a cell phone as a tracking device because it has not been installed). See infra Part III.A.

53 See, e.g., In re Application of the U.S. for an Order, 620 F.3d at 310 (analyzing the applicable standard based on classification under the ECPA and SCA).

54 See supra Part II.B.1. But see In re Pen Register, 396 F. Supp. 2d at 759 (noting although the definition of “wire communication” does not contain a tracking device
confusion surrounding whether a mobile phone can be a tracking device emitting either electronic or wire communications is directly attributable to the lack of any mention of mobile phones or CSLI in the ECPA or SCA.\textsuperscript{61}

The GPS Act, as an amendment to the ECPA, solves these definitional issues by clearly governing mobile phones producing CSLI.\textsuperscript{62} The GPS Act succinctly controls all wireless communication devices producing GLI.\textsuperscript{63} The definition of wireless communication devices explicitly includes mobile phones and the idea of cell site location information—pinpointing location of users—is employed in the Act’s definition of GLI.\textsuperscript{64} Yet, unlike the confusion with CSLI under the ECPA and SCA, GLI does not distinguish between types of data.\textsuperscript{65} Accordingly, smartphones are wireless communication devices, separate from tracking devices, and the CSLI need not be classified as being wire or electronic communication because it now is GLI, covered irrespective of its stored nature, under the GPS Act. Notably, even if a mobile phone were classified as a tracking device, because GLI is not distinguishable as wire or electronic, and tracking devices can emit GLI, a smartphone is still covered.\textsuperscript{66}

With coverage assured, the GPS Act further accomplishes clarity by lessening the importance of such prior distinctions because of the universal standard and remedy it borrows from Fourth Amendment precedent. Requests for GLI must satisfy the probable cause standard, and in the event GLI is improperly intercepted without a warrant, the remedy is exclusion of the evidence.\textsuperscript{67} So, for example, where the SCA

---

\textsuperscript{61} See Plourde-Cole, supra note 4, at 589, 605 (noting ECPA does not define the standard for either cellular tower location data or GPS information from a cell phone, or even refer to cell site or other location information from a cell phone).

\textsuperscript{62} See generally H.R. 1312 §§ 2601-2605.

\textsuperscript{63} Id.

\textsuperscript{64} See id. § 2601(10) (defining wireless communication device as “any device that enables access to, or use of, an electronic communication system or service, remote computing service, or geolocation service, if that device utilizes a radio or other wireless connection to access such system or service”); id. § 2601(4) (stating wireless communication device includes mobile telephone).

\textsuperscript{65} The SCA is limited to stored historical communication, hence its title. See 18 U.S.C. §§ 2701-2712. The GPS Act is not limited in this way. See H.R. 1312 §§ 2601-2605.

\textsuperscript{66} See H.R. 1312 § 2601(3).

\textsuperscript{67} See H.R. 1312 § 2602(h)(2) (warrant); H.R. 1312 § 2603 (prohibition of use as evidence of acquired geolocation information).
could feasibly cover tracking device CSLI as wire communications to be attained at the lower “specific and articulable facts” standard, under the Act, requests for GLI, either from a wireless communication or tracking device, must satisfy the higher probable cause standard.78 Through the GPS Act, Congress has effectively elevated mobile phone CSLI, defined as smartphone GLI, to the probable cause standard, circumventing the lesser SCA standard that otherwise could have applied, and has invoked the Fourth Amendment exclusionary rule, which is not available under the SCA.79 In doing so, the GPS Act affords aggrieved parties the luxury of not needing to mount a constitutional argument to have the data excluded from evidence and a stronger sanction in the event such evidence is so obtained.

While the proposed framework does not amend the pre-existing statutory language as much as it adds an additional layer, such additions provide clarity to a much needed area for judges, law enforcement, and citizens alike. Judges and law enforcement groups no longer need to wade into the technological waters in which they are untrained to swim by trying to classify and re-classify smartphones and derived location data because the GPS Act does it for them. Instead of having judicial splits as to the proper standard applicable to CSLI, the GPS Act allows courts and police to know the exact standard they must meet in order to obtain an individual’s smartphone data—probable cause.70 Such development will also lead to a calming of the masses who increasingly feel that their civil rights are being violated, especially those calling for a Digital Bill of Rights, because cellular geolocational information can no longer be obtained without a heightened need.

78 See In re Application of the U.S. for an Order, 620 F.3d at 311 (expressing concern but not taking a position on whether a request for GPS data is appropriate under the lower SCA standard when mobile phone is classified as tracking device).

79 See 18 U.S.C. §§ 2703(d), 2707-2708; In re Application of the U.S. for an Order, 620 F.3d at 310; In re Pen Register, 396 F. Supp. 2d at 752; see also Lindemann, supra note 40, at 687 (noting Pen/Trap Statute and the SCA required the exclusion of non-content communications if improperly obtained).

70 Compare In re Application of the United States for Historical Cell Site Data, 747 F.Supp.2d 827, 837 (S.D. Tex. 2010) (requiring probable cause for historical CSLI), with People v. Hall, 14 Misc.3d 245, 257 (N.Y. Sup. Ct. 2006) (holding that cell technology at issue was not a tracking device and that the lower SCA standard applied).
B. The Fourth Amendment and the Third-Party Doctrine’s Impact on Smartphones

The GPS Act’s inclusion of Fourth Amendment standards and protections in the ECPA is particularly potent. If an aggrieved party were to put forth a Fourth Amendment claim for improper retrieval of GLI from his or her smartphone and geo-apps, the Fourth Amendment likely would not apply in light of the Third-Party Doctrine.71 The Third-Party Doctrine holds that the Fourth Amendment “does not prohibit the obtaining of information revealed to third parties and conveyed . . . 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.”72 While the result is the same when the Third-Party Doctrine is invoked—that the Fourth Amendment does not apply—courts have rationalized the doctrine under a failure to satisfy the objectivity prong of the two-pronged test, that the individual’s expectation of privacy is one that society is prepared to recognize as reasonable.73 Other courts, with support from academics, have based the doctrine upon consent: when an individual knowingly discloses information to a third party, he or she consents to another person having control over it.74 Accepting either rationale of the Third-Party Doctrine, a strong minority of courts have applied it

---

71 See Plourde-Cole, supra note 4, at 575 (arguing “Third[-]Party Doctrine,” in addition to numerous federal statutes, governs cell phone information). See generally Kerr, supra note 5, at 56466 (providing a general catalogue of the cases invoking the Third-Party Doctrine). The courts have never formally emblazoned the Third-Party Doctrine; however, courts routinely apply the rationale as such without giving it a formal name. See id.

72 Kerr, supra note 5, at 563 (emphasis added) (citation omitted); see Malone, supra note 5, at 739-40 (“Courts often hold that the determining factor for whether the Third[-]Party Doctrine applies is whether the information is ‘voluntarily’ conveyed to the third party.”).

73 See, e.g., Smith v. United States, 442 U.S. at 743 (citations omitted) (precluding Fourth Amendment protection to telephone numbers conveyed to telephone company); see also id. at 744-45 (“This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”); see, infra note 73 and accompanying text (Dye, Benford, Suarez-Blanco cases).

74 See, e.g., Kerr, supra note 5, at 58889 (defining consent and suggesting Third-Party Doctrine should be considered a consent-based doctrine rather than one based on reasonability); Kran v. United States, 468 U.S. at 711 (holding no Fourth Amendment interest where consent to install tracking beeper validated its presence).
2013] 

YOU ARE HERE

33

specifically in CSLI cases. Based on either of these rationales and viewed in light of the nature of relaying geospatial location to third parties willfully and openly after having purchased, used, and read the privacy statements of a smartphone and any geo-apps, the Third-Party Doctrine would likely preclude Fourth Amendment protection. Thus, the GPS Act provides protections where the Fourth Amendment otherwise would not apply.

V. CONCLUSION

As smartphones, GPS technology, and geo-apps build upon and blend with the standard cell phone technology of receiving and making phone calls, the reasonable expectation of privacy will correspondingly grow to incorporate greater perceived notions of privacy. As judges have attempted to blend, with various results, technologically-outmoded ECPA and Fourth Amendment precedent to new mobile technology, there is trepidation that this type of jurisprudential process risks uncontrolled growth, the result of which would lead to an overwhelming number of unnecessary constitutional claims. While the GPS Act, rather than a Digital Bill of Rights, offers an opportunity to clarify much of the current confusion regarding smartphone technology, it also stands as a prominent example of how Congress can actively formulate immediate and contemporaneous responses to the never-ending evolution of smartphone technology and provide for heightened, Fourth Amendment-like protections where necessary, even where the Fourth Amendment would otherwise likely not be implicated. Indeed, like Congress, states may even take note and develop heightened protections that go beyond accord with those set by Congress or the Constitution.

Adoption of

75 See, e.g., United States v. Dye, No. 1:10-CR-221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011) (“The defendant also seeks to suppress his cell phone records, which were obtained via subpoena. However, there is no reasonable expectation of privacy in cell phone records[]or in cellsite location information”); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *2 (N.D. Ind. Mar. 26, 2010) (“[D]efendant has no legitimate expectation of privacy in records held by a third party cell phone company . . . [but] Fourth Amendment concerns might be raised if cellsite data were used to track the present movements of individuals in private locations.”); United States v. Suarez-Blanca, , 2008 WL 4200156 at *9 (N.D. Ga. Apr. 21, 2008) (rejecting Fourth Amendment claims where tracking device only reveals communications with towers rather than movement inside private location).

76 For example, in Florida, all parties must consent to a recording or disclosure of the contents of a wire, oral or electronic communication; the act of recording,
the GPS Act, as its name suggests, has the potential for guiding the way not just in judicial reasoning and clarity in the current smartphone world, but also in laying a procedural path for Congress to follow in passing future legislation when individuals and society demand protection against those developments in mobile technology that threaten their privacy.

disclosing, or attempting to disclose without consent of all parties may result in felony charges. See FLA. STAT. ANN. § 934.05 (West 2012).