The Heritage Foundation

LEGAL MEMORANDUM

No. 118 | FEBRUARY 28, 2014

Protecting Americans' Privacy: Why the Electronic Communications Privacy Act Should Be Amended

Evan Bernick

Abstract

The development of new technologies has brought the Fourth Amendment front and center in the public discourse. By requesting or compelling cell phone companies to provide subscriber information, law enforcement agencies can pinpoint the locations of the cell sites from which subscribers have made calls and, therefore, where the subscribers can be found. Americans do not want the government to be able to track them without specific, articulable suspicions and without oversight. Americans need not choose between Fourth Amendment precedent and protecting important privacy interests. Congress should consider revising the Electronic Communications Privacy Act to address the privacy concerns raised by ever-evolving tracking technology. The tools are ready at hand.

The development of new technologies has brought the Fourth Amendment front and center in the public discourse. By requesting or compelling cell phone companies to provide subscriber information, law enforcement agencies can pinpoint the locations of the cell sites from which subscribers have made calls and, therefore, where the subscribers can be found.

Recently, the U.S. Court of Appeals for the Fifth Circuit addressed whether a subscriber has a "reasonable expectation" of privacy in that information. In answering that question in the negative, the court relied on the "third party doctrine," according to which information that is voluntarily shared with another is not protected from disclosure to the government by that third party even if one expects that it will be kept private. The New Jersey Supreme Court also

This paper, in its entirety, can be found at **http://report.heritage.org/lm118**

Produced by the Edwin Meese III Center for Legal and Judicial Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Key Points

- The development of new technologies has brought the Fourth Amendment front and center in the public discourse.
- By requesting or compelling cell phone companies to provide subscriber information, law enforcement agencies can pinpoint the locations of the cell sites from which subscribers have made calls and, therefore, where the subscribers can be found.
- Americans do not want the government to be able to track them without specific, articulable suspicions, and without oversight.
- Americans need not choose between Fourth Amendment precedent and protecting important privacy interests.
- Fifth Circuit and New Jersey Supreme Court decisions point to the desirability of a statutory solution to the problem of cell-site location monitoring.
- Congress should therefore consider revising the Electronic Communications Privacy Act to address the privacy concerns raised by ever-evolving tracking technology.

addressed whether the same information is protected by the New Jersey Constitution and, in the course of answering that question in the affirmative, took a different approach to the question of what expectations of privacy are reasonable.[1]

The Fifth Circuit's holding that historical cell-site information is not protected by the Fourth Amendment is consistent with U.S. Supreme Court precedent, but it also leaves the government with a great deal of freedom to acquire personal information about individuals. The New Jersey Supreme Court's holding to the contrary binds only state actors enforcing state law and does not provide a workable alternative to the "third party doctrine" that the U.S. Supreme Court has applied in Fourth Amendment cases. Refining the Electronic Communications Privacy Act (ECPA) is the best option for those who desire to limit the federal government's ability to track their whereabouts through their cell phones.

Summary of Relevant Electronic Privacy Decisions

In re Application of the United States of America for Historical Cell Site Data. In this case, the Fifth Circuit evaluated three government requests relevant to separate criminal investigations.[2] The government asked a U.S. magistrate judge to issue an order under 18 U.S.C. § 2703(d) of the Stored Communications Act to compel the cell phone providers for particular phones to produce 60 days' worth of historical cell-site data—specifically, data concerning the antenna tower and sector to which the phones sent their signals.[3]

In order to secure such an order, the government must set forth "specific and articulable facts that there are reasonable grounds to believe [that the records] sought, are relevant and material to an ongoing criminal investigation." This is a lower standard than probable cause, which is necessary to secure a search warrant. The magistrate judge ruled that compelled warrantless disclosure of such data violated the Fourth Amendment, and the district court agreed with the magistrate's decision.

The court of appeals, however, reversed these decisions, emphasizing that the government had acquired the information after it had been "voluntarily" communicated to a third party, the phone companies.[4] Where "a third party, of its own accord, and for its own purposes"[5] collects and stores information, the court reasoned, "[that information] can be used for any purpose,"[6] including to assist law enforcement. Since the phone companies had "created the business record[s] to memorialize [their] business transaction(s) with the target(s)," the court ruled that the targets could not object to the companies' sharing those records with the government.[7]

In reaching its decision, the court navigated its way through a thicket of case law on the "third party doctrine" from the Supreme Court and from other federal circuit courts of appeal. The Fifth Circuit analogized the facts of the case at bar to those in *United States v. Miller*, in which the Supreme Court rejected a bank depositor's Fourth Amendment challenge to a subpoena for bank records because, "as the bank was a party to the transactions, the records belonged to the bank."[8] The court also distinguished the instant matter from *United States v. Warshak*, in which the Sixth Circuit had ruled that the government could not compel an Internet service provider to turn over the contents of a subscriber's e-mails without a warrant, reasoning that phone companies produce phone records for their own business purposes, whereas Internet service providers act as an intermediary for communication of records between two parties.[9]

1. This paper is solely concerned with targeted cell phone data collection for domestic law enforcement purposes. This paper does not address bulk collection by the government of metadata for foreign intelligence purposes
2. In re Application of the United States of America for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
3. *Id.* at 602.
4. *Id.* at 612.
5. *Id.* at 610.
6. *Id.* at 611.
7. *Id.*
8. United States v. Miller, 425 U.S. 435, 440–41 (1976).
9. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

The court then considered and rejected the argument that the subscribers to phone companies do not voluntarily communicate cell-site location information. The court assumed that cell service subscribers know that cell phones must send a signal to a nearby cell tower, that they are out of range if they cannot pick up a signal, and that calls may not go through if many customers in the area attempt to make calls at the same time.[10] The court further surmised that the cell service providers' contractual terms of service and privacy policies expressly inform subscribers that providers use location information to route phone calls, that providers collect this information, and that providers will turn this information over to the government if served with a court order.[11] Finally, the court pointed out that subscribers are free not to carry phones or use any particular provider.[12] Under these circumstances, the court concluded that an individual's choice to use a cell phone and thus share his or her location is just that: a choice.

In reaching its conclusion, the Fifth Circuit drew upon the Supreme Court's leading case on telephone record collection. In *Smith v. Maryland*, the Court upheld the warrantless use of pen register devices that capture the phone numbers of outgoing calls. The Court reasoned that telephone users "realize they must convey phone numbers to the telephone company" and recognized that "the phone company has facilities for making permanent records of the numbers they dialed."[13] The Court also pointed out that "most phone books tell subscribers ... that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.'"[14] The Fifth Circuit found that the facts before it were sufficiently similar to those of *Smith* to support the same outcome.

State v. Earls. Here, the New Jersey Supreme Court examined a series of information requests that state police officers had made of T–Mobile.[15] The police sought to determine a suspect's location on the night of a burglary by tracking a stolen cell phone the police believed the suspect had been using.

Chief Justice Stuart Rabner, writing for the majority, began by announcing that under settled New Jersey law, "individuals do not lose their right to privacy simply because they have to give information to a third-party provider, like a phone company or bank, to get service."[16] The court went on to determine that individuals do not voluntarily convey cell-site information to phone companies, because the "price of not using a cell phone" is too high to be avoided and "cell phone users have no choice but to reveal certain information to their cellular provider."[17] The court, drawing upon New Jersey case law, held that even if they did choose to reveal that information, individuals are "entitled to assume that the telephone numbers they dial in the privacy of their home will be recorded solely for the telephone company's business purposes."[18] While the court conceded that individuals "may be generally aware that their phones can be tracked," it denied that most individuals "realize the extent of modern tracking capabilities."[19]

Throughout, the court emphasized the precision of today's cell-site location tracking technology. Justice Rabner explained that "cell phones can be pinpointed ... to within feet" and that such information can be used to "provide an intimate picture of one's daily life."[20] Owing to this precision, cell-site location information can, among other things, "reveal not just where people go—which doctors, religious services, and stores they visit—but also the people

10. *Id.* at 613.
11. *Id.*
12. *Id.* at 614.
13. Smith v. Maryland, 442 U.S. 735, 742–43 (1979).
14. *Id.* at 743.
15. State v. Earls, 470 A.3d 630 (N.J. 2013).
16. *Id.* at 632.
17. *Id.* at 641.
18. *Id.* at 642 (quoting State v. Hunt, 450 A.2d 952, 956 (N.J. 1982)).
19. *Id.* at 588.
20. *Id.* at 586.

and groups they choose to affiliate with and when they actually do so."[21] The court found that such precise tracking distinguished cell-site location information from "toll billing, bank, or internet subscriber records."[22]

For support, the court drew upon Justice Samuel Alito's and Justice Sonia Sotomayor's concurrences in *United States v. Jones*,[23] in which the U.S. Supreme Court considered whether the police needed to secure a warrant to engage in 28 days of GPS monitoring of a suspect. The *Earls* majority relied on Justice Alito for the proposition that "longer term"[24] monitoring impinges on privacy expectations and cited Justice Sotomayor's description of the "wealth of detail" that long-term monitoring of public movements can disclose.[25]

Analysis of Electronic Communications Privacy Decisions

The Fifth Circuit's opinion in *Historical Cell Site Data* is consistent with the Supreme Court's Fourth Amendment jurisprudence. Close attention to the Court's precedent reveals that *Smith* and *Miller* cannot be cast aside as aberrations. In a line of decisions involving confidential informants that predate *Smith* by decades, the Court consistently held that one who shares information with a third party cannot rely on the Fourth Amendment for protection against disclosure.[26] For example, in *Hoffa v. United States*, the Court denied a claim that an informant's failure to disclose his identity violated the petitioner's Fourth Amendment rights: "The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak."[27]

But recent technological developments expose privacy interests in ways that the justices who forged the Court's Fourth Amendment jurisprudence could never have anticipated. The Fifth Circuit acknowledged that the cell-site location data can be used to narrow someone's location to a fairly small area, potentially a home, but pointed out that the pen registers in *Smith* did the same: "If a person makes a call from his home landline, he must be located in his home at the landline's receiver."[28] The pen registers in *Smith*, however, did not enable police to follow individuals from location to location, which could reveal more sensitive information.

In her *Jones* concurrence, Justice Sotomayor explained that modern location tracking technology can ensure that "movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[29] To be sure, the government might be able to obtain much the same information through real-time physical surveillance, but modern tracking technology makes that acquisition far easier and less costly with less risk of detection.

The reasoning of the New Jersey Supreme Court in *Earls* is strikingly similar to that of the District of Columbia Court of Appeals in *United States v.*

21. *Id.*
22. *Id.*
23. United States v. Jones, 132 S. Ct. 945 (2012). The court conceded that applying the *Jones* majority's reasoning would have led to a different conclusion. *Earls*, 470 A.3d at 644.
24. *Earls*, 214 N.J. at 583 (citing *Jones*, 132 S. Ct. at 964 (Alito, J., concurring)).
25. *Id.* (citing *Jones*, 132 S. Ct. at 925 (Sotomayor, J., concurring)).
26. *See, e.g.*, On Lee v. United States, 343 U.S. 747 (1952) (an individual "talking confidentially and indiscreetly with one he trusted" cannot claim that his conversation is protected by the Fourth Amendment if it is recorded and turned over to the police); Hoffa v. United States, 385 U.S. 206, 302 (1966) (the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"). *See also* United States v. White, 401 U.S. 745, 749–52 (1971) (holding that *On Lee* and *Hoffa* survived *Katz* because *Katz* "involved no revelation to the Government by a party to conversations with the defendant" and reiterating that those who share information with third parties "must realize and risk that [their] companions may be reporting to the police").
27. *Hoffa*, 385 U.S. at 303 (citing Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting)).
28. *Historical Cell Site Data*, 724 F.3d at 609.
29. *Jones,* 132 S. Ct. at 925 (Sotomayor, J., concurring).

Maynard,[30] the same case that the Supreme Court later decided under the caption of *U.S. v. Jones*. In *Maynard,* Judge Douglas Ginsburg explained that at a certain point, location tracking could produce so much information that it amounts to a search requiring the issuance of a warrant. The D.C. Circuit in *Maynard* held that 28 days of GPS tracking constituted a "search" because such surveillance "reveals the habits and patterns that mark the distinction between a day in the life and the way of life," among them "whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, [and/or] an associate of particular individuals or political groups."[31]

In *Jones,* both Justice Sotomayor and Justice Alito accepted this "Mosaic Theory," determining that long-term monitoring was categorically distinguishable from short-term monitoring because of the *extent* of the information that could be acquired through aggregation. *Earls,* too, focuses on the extent of the information that is revealed through aggregated cell-site location data.

Can a workable alternative approach to the reasonable-expectation-of-privacy calculus be gleaned from these cases to replace the third-party doctrine?

Mosaic Theory Not a Practical Alternative to the Third Party Doctrine

At the very least, any alternative to the third party doctrine must enable both law enforcement authorities and private citizens to determine *ex ante* whether there is a reasonable expectation of privacy in the information that law enforcement seeks to collect. One of the virtues of the third party doctrine is its clarity: The Fourth Amendment never protects information disclosed to third parties. The only ambiguity lies in whether one can reasonably expect that the information has been disclosed, and the leading cases have required only a general awareness of the possibility of disclosure to a third party before finding that such disclosure can reasonably be expected.

The same cannot be said for the reasonable expectations analysis in *Earls.* The court acknowledged that it was not able to "draw a fine line" to "calculate a person's legitimate expectation of privacy with mathematical certainty."[32] The court, however, did not draw any useful line at all. Rather, it conceded that individuals are "generally aware that their phones can be tracked" but then asserted that "no one buys a cell phone to share detailed information about their whereabouts" and that "most people do not realize the extent of modern tracking capabilities."[33]

These assertions raise more questions than they answer:

- At what point is information sufficiently "detailed" that a warrant must be secured?
- If individuals are "generally aware that their phones can be tracked," how can the court claim that they can reasonably expect privacy in the information that can be gleaned through tracking?
- How can law enforcement officials determine *ex ante* the tracking capabilities with which "most people" are familiar?
- Must the police (or the prosecutor's office, the governor's office, etc.) publish a notice in advance (in a newspaper, on the Internet, on highway billboards, etc.) to ensure that no criminals will be surprised to learn that (and therefore will be unable to object to the fact that) law enforcement authorities are able to derive information about them either through new surveillance technology or through the innovative use of existing technology?
- Is that conduct that we want law enforcement authorities to pursue?

30. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* U.S. v. Jones, 132 S. Ct. 945 (2012). *See also* Commonwealth v. Augustine, No. SJC-11482 (Mass. Feb. 18, 2014) (concluding that Article 14 of the Massachusetts Declaration of Rights, which protects against unreasonable searches and seizures, required a warrant for cell-site records covering a two-week period because this time period "was more than sufficient to intrude upon the defendant's expectation of privacy safeguarded by Article 14").
31. *Id.* at 562.
32. *Earls*, 214 N.J. at 587.
33. *Id.* at 588.

The deficiencies of *Earls* are intrinsic to the Mosaic Theory. Judge Ginsburg's conclusion that 28 days of tracking triggered Fourth Amendment protection does not provide any reliable metric by which law enforcement or citizens could determine whether, say, seven days would. Justices Sotomayor and Alito had different views about what the standard should be—whether courts should look to whether individuals can reasonably expect law enforcement to monitor them extensively *in most cases* or whether they can reasonably expect such extensive monitoring *at all*.[34]

The Mosaic Theory provides more Fourth Amendment protection than the third party doctrine, but it does not offer courts or law enforcement authorities an objective means by which to distinguish conduct that amounts to a search from conduct that does not.

Amending the Electronic Communications Privacy Act

The Fifth Circuit's decision is faithful to precedent predating *Smith* and provides a usable rule that is lacking from proposed alternatives. What, then, are cell subscribers who are concerned about protecting their location information to do?

The Fifth Circuit indicated that subscribers have options: "The recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections."[35] Justice Alito expressly endorsed the political option in his *Jones* concurrence, arguing that the legislature is better suited to addressing privacy concerns precipitated by technological advances than are the courts: "A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and safety in a comprehensive way."[36]

The Electronic Communications Privacy Act, which was enacted in 1986 to reform federal privacy law in light of new communications technologies, seems at first blush to provide strong privacy protections for stored data.[37] The ECPA enables the government to compel electronic communications providers that store customer data to produce said data under certain conditions. Specifically, Section 2703(c)(1) provides that:

> [Law enforcement authorities may] require a provider of electronic communication service ... to disclose a record or other information pertaining to a subscriber to or customer of such service [if, pursuant to Section 2703(d), officers submit] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Section 2703(d) mirrors the "reasonable suspicion" standard set forth in *Terry v. Ohio*.[38] Under *Terry*, brief investigatory stops may be conducted by law enforcement, even in the absence of probable cause, if reasonable suspicion exists, based on "specific and articulable facts" and not an "unparticularized suspicion or 'hunch,'" that the person has committed, is committing, or is about to commit a crime.[39]

Information that can be gleaned from cell-site location tracking can be used to track individuals' locations with greater precision than is possible

34. Compare *Jones*, 132 S. Ct. at 955–6 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on") *with id*. at 964 (Alito, J., concurring) ("the use of longer term GPS monitoring in investigations of *most* offenses impinges on expectations of privacy") (emphasis added).

35. *Historical Cell Cite Data*, 724 F.3d at 615.

36. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

37. The ECPA comprises three titles. Title I is codified at 28 U.S.C. §§ 2510–22 and protects oral communications. Title II deals with access to stored communications and transaction records and is codified at 18 U.S.C. § 2701 *et seq.* Title III, codified at 18 U.S.C. §§ 3121–27, concerns the use of pen register and/or trap and trace devices to record dialing, routing, addressing, and signaling information used in the process of transmitting wire or electronic communication.

38. Terry v. Ohio, 392 U.S. 1 (1968) Courts have interpreted it accordingly. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1202 ("the 'specific and articulable facts' standard derives from the Supreme Court's decision in *Terry*").

39. *Terry*, 392 U.S. at 27.

with pen registers, potentially revealing more information about their personal lives. Accordingly, it make sense for judges to scrutinize requests for Section 2703(d) independently pursuant to the *Terry* standard, even though pen register requests are not subjected to any independent judicial review.[40]

Courts have assumed, however, that Section 2703(d)'s standard need not be satisfied with respect to each individual whose data are collected from a cell tower. That is to say, hundreds of innocent individuals could have their information collected in "cell tower dumps" because specific and articulable facts exist showing that there are reasonable grounds for believing that some of the data will be relevant and material to an ongoing criminal investigation—even if a substantial amount will not be.

Revising Section 2703(d) to ensure that the *Terry* standard is applied to every individual whose cell location information is requested would prevent cell-tower dumps without crippling law enforcement's capacity to respond expeditiously to criminal activity. For example, it would not be possible to secure three hours' worth of records from thousands of users of a Verizon cell-tower near a bank simply on the grounds that the bank was robbed during that time interval. Indeed, there would be no "particularized and objective basis" for suspecting any given Verizon user of criminal activity, but if the police suspected that a cell phone number was connected to a recent robbery near a cell tower, they could request that a judge issue an order requiring Verizon to turn over any data in that tower connected with that number.

What, then, of requests for subscriber information that span longer periods of time—days or months rather than hours? It is certainly true that more information about a person would be exposed as the time span over which his or her location was tracked increased. Further, if requests were not time-limited, individuals could be tracked over time periods during which there was no reason to believe they were involved in criminal activity by an official engaged in the "competitive enterprise of ferreting out crime."[41]

The ECPA's limitations on wiretapping provide guidance here. Pursuant to Section 2518(5), real-time wiretaps are capped at 30 days, after which police must seek an extension from a magistrate. Section 2518(1)(f) provides that applications for extensions must both include the information cited in the original applications and state the results already obtained or a reasonable explanation of the failure to obtain the desired results. The Supreme Court has held that the purpose of Section 2518(1)(f) "is to permit the court realistically to appraise the probability that relevant conversations will be overheard in the future."[42] These limitations ensure that citizens need not rely on the good faith of law enforcement: They subject real-time surveillance to oversight by impartial actors.

How, then, should the time span of cell-site location information requests be limited? Given that the Constitution does not fix a limit, it falls to Congress to set a threshold that balances privacy and security preferences in a transparent manner. Furthermore, such a limitation should reflect the public's desires, as opposed to those of unelected judges. A week to 10 days' worth of cell phone use would seem to be a good initial limit.

To borrow from *Maynard,* a week to 10 days' worth of movements discloses a "way of life."[43] An individual's cell phone use during that time period should be sufficient for police to gather a wealth of detail about said individual's movements and, thus, his or her involvement (or lack thereof) in criminal activity. Police should be able to secure extensions when they can demonstrate that relevant information would likely be acquired if the extension were granted. As in the case of wiretap extensions, police should be required to include the information cited in the original application and state either their results or a reasonable explanation of their failure to attain the desired results.

40. *See* 18 U.S.C. § 3123(a) (2000) (investigators need only certify that "the information likely to be obtained … is relevant to an ongoing criminal investigation"). Relevance does not require any independent judicial scrutiny. *See, e.g.*, In re U.S. for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device, 846 F.Supp. 1555, 1559 (M.D. Fla. 1994) (under relevance standard, there is no "independent judicial inquiry into the veracity of the attested facts").
41. Johnson v. United States, 333 U.S. 10, 15 (1948).
42. United States v. Giordano, 416 U.S. 505, 532 (1974).
43. *Maynard*, 615 F. 3d at 562.

Conclusion

The Fifth Circuit and New Jersey Supreme Court decisions point to the desirability of a statutory solution to the problem of cell-site location monitoring. The third-party doctrine is entrenched in the Supreme Court's Fourth Amendment jurisprudence, and the Mosaic Theory is not a workable alternative. Even if cell-site locations are not constitutionally protected, however, Americans do not want the government to be able to track its citizens without specific, articulable suspicions—and not without oversight.

Americans need not choose between Fourth Amendment precedent and protecting important privacy interests. Congress should consider revising the ECPA to address the privacy concerns raised by ever-evolving tracking technology. The tools are ready at hand.

*—**Evan Bernick** is a Visiting Fellow in the Edwin Meese III Center for Legal and Judicial Studies at The Heritage Foundation.*