Where Have You Been - Your Phone Knows (and So Might the Police)

W. Jacob Henerey

Follow this and additional works at: https://scholarcommons.sc.edu/sclr

Recommended Citation
Henerey, W. Jacob (2014) "Where Have You Been - Your Phone Knows (and So Might the Police)," South Carolina Law Review: Vol. 65 : Iss. 4 , Article 5.
Available at: https://scholarcommons.sc.edu/sclr/vol65/iss4/5

This Article is brought to you by the Law Reviews and Journals at Scholar Commons. It has been accepted for inclusion in South Carolina Law Review by an authorized editor of Scholar Commons. For more information, please contact dillarda@mailbox.sc.edu.
On February 5, 2011, Aaron Graham and Eric Jordan were arrested in Baltimore after witness descriptions tied them to the robberies of two fast food restaurants. As part of an investigation into area robberies, federal authorities requested a court order requiring Sprint/Nextel to turn over location data from the defendants’ cell phones. The government requested the information “to more conclusively link the defendants with the prior robberies.” Eventually, the government obtained two orders authorizing the release of a combined 221 days of location data from the defendants’ cell phones. The evidence obtained as a result of these orders helped the government secure indictments against the defendants for multiple robberies in the Baltimore area. The district court upheld the government’s method of obtaining the information, notwithstanding the defendants’ claims that it violated their constitutional rights.

The federal government’s practice of spying on the private communications of Americans has been at the forefront of the national debate over privacy in the past year. Anyone with access to a TV, computer, or newspaper is probably aware of the scandal unleashed by National Security Agency (NSA) leaker

2. Id. at 386.
3. Id.
4. See id. at 387.
5. See id. at 386--87.
6. Id. at 404.
Edward Snowden. But while the NSA continues to garner headlines, the use of personal communication data is hardly limited to federal authorities. Increasingly, state and local police departments are turning to cell site location information (CSLI) to track users’ locations. A nationwide survey of police practices conducted by the American Civil Liberties Union (ACLU) revealed just how prevalent the practice is. Over 250 police departments responded to the ACLU’s requests for information on their policies regarding CSLI; all but thirteen admitted to the use of cellular location data. Some of the departments responded that they require warrants supported by probable cause before ordering phone companies to disclose user location data. Those departments, however, appear to be the exception, not the rule. For example, the Wilson County, North Carolina Sheriff’s Office obtained nearly a month’s worth of cellular location data because an officer had “reason to believe” the information

---


9. See, e.g., Eric Lichtblau, Police Are Using Phone Tracking as Routine Tool, N.Y. TIMES, Apr. 1, 2012, at A1, available at http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html (describing the widespread use of CSLI by local police departments). In fact, the practice has become so widespread that some carriers have created catalogs detailing the services they can provide, as well as how much those services cost, with the most invasive services costing up to $2,200. See id.


11. Id. ACLU affiliates submitted requests to the Greenville County Sheriff’s Office, the Myrtle Beach Police Department, and the South Carolina Law Enforcement Division (SLED), but the ACLU has not listed responses to those requests on its website. See Is Your Local Law Enforcement Tracking Your Cell Phone’s Location?, ACLU, https://www.aclu.org/maps/your-local-law-enforcement-tracking-your-cell-phones-location (last visited Mar. 5, 2014).

12. See Cell Phone Location Tracking Public Records Request, supra note 10; see also, e.g., Letter from Jay Hinkel, Deputy City Att’y, City of Wichita, to Doug Bonney, Chief Counsel & Legal Dir., ACLU Legal Dep’t (Aug. 15, 2011), available at https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_wichita.pdf (responding to an ACLU open records request by stating that the City of Wichita obtains cell phone location records only pursuant to affidavits supported by probable cause).

was “relevant and material” to a criminal investigation.\textsuperscript{14} Police in Lincoln, Nebraska, have used a nearly identical standard to obtain not only CSLI, but Global Positioning System (GPS) data as well.\textsuperscript{15}

This raises the following questions: What is CSLI, and why should privacy advocates be concerned about its acquisition by government agencies? At least one federal district court made extensive findings of fact as to the nature of CSLI before refusing to issue an order requiring a cellular company to turn over this information.\textsuperscript{16} The U.S. District Court for the Southern District of Texas found that a cell phone works by using base stations, or “cell sites,” to connect the phone to the telephone network.\textsuperscript{17} Whenever the phone is turned on, it periodically registers with the nearest cell site;\textsuperscript{18} this happens automatically, “without the user’s input or control.”\textsuperscript{19} A cell phone’s location can be determined by using either GPS satellite technology or cell site information.\textsuperscript{20} While the use of GPS satellites allows for greater precision in determining a phone’s location, it is not always a viable option, in part because some cell phones are not equipped with GPS technology.\textsuperscript{21} CSLI, which is more commonly utilized, determines a phone’s location based on the cell sites with which it registers when making or receiving calls, or when moving from one site to another.\textsuperscript{22} As cellular network use has increased, the areas served by a particular cell site—the “cell sector”—have shrunk dramatically.\textsuperscript{23} As a result, the court concluded that “knowing the base station (or sector ID) handling a call is tantamount to knowing the user’s location to within a relatively small geographic area. In urban areas... this area can be small enough to identify individual floors and rooms within buildings.”\textsuperscript{24} The court found that such information could be used to “track the user on a minute by minute basis, compiling a continuous log of his life, awake and asleep.”\textsuperscript{25}


\textsuperscript{17} Id. at 831.

\textsuperscript{18} Id.

\textsuperscript{19} Id.

\textsuperscript{20} Id.

\textsuperscript{21} Id. at 832.

\textsuperscript{22} Id.

\textsuperscript{23} Id.

\textsuperscript{24} Id. at 833.

\textsuperscript{25} Id. at 835; see also State v. Earls, 70 A.3d 630, 632 (N.J. 2013) (“Cell phones register or identify themselves with nearby cell towers every seven seconds. Cell providers collect data from those contacts, which allows carriers to locate cell phones on a real-time basis and to reconstruct a phone’s movement from recorded data.”).
While states have increasingly turned to the use of CSLI, they have also led the way in extending greater privacy protections to this information. This Note discusses these state actions against the backdrop of current federal case law with an eye toward developing a policy in South Carolina that effectively protects individuals’ right to privacy. This Note argues that, as South Carolina’s constitution provides privacy protections beyond those secured by the Fourth Amendment to the U.S. Constitution, courts in South Carolina should require a warrant supported by probable cause before police can obtain CSLI.

Part II provides background information on the current state of privacy law in the United States, as determined by the Supreme Court and federal appellate courts. Part III discusses the actions various states have taken to provide greater privacy protections than those currently afforded under federal Fourth Amendment jurisprudence. Part IV argues that South Carolina should follow the example of those states providing greater privacy protections to their citizens by requiring warrants supported by probable cause whenever the police seek CSLI from a cellular telephone company. Part V concludes by reiterating that South Carolina’s citizens deserve—and their constitution requires—the greater privacy protections discussed throughout this Note.

II. FEDERAL BACKGROUND

A. The Supreme Court

The starting point for any discussion of privacy law is Katz v. United States.26 In Katz, the Supreme Court removed the “place” requirement from Fourth Amendment jurisprudence, holding that “the Fourth Amendment protects people, not places.”27 Justice Harlan’s concurrence established the standard that has since guided the Court when faced with privacy questions.28 According to Justice Harlan, the Fourth Amendment protects a person’s reasonable expectation of privacy, which is “an actual (subjective) expectation of privacy . . . that society is prepared to recognize as ‘reasonable.’”29 Importantly for the purposes of this Note, the Court also recognized that “the protection of a

26. 389 U.S. 347 (1967); see also Smith v. Maryland, 442 U.S. 735, 739 (1979) (“In determining whether a particular form of government-initiated electronic surveillance is a ‘search’ within the meaning of the Fourth Amendment, our lodestar is Katz v. United States.” (footnote omitted)).
person’s *general* right to privacy... is... left largely to the law of the individual States.*

More than a decade later, in *Smith v. Maryland*, the Court applied the reasonable expectation of privacy analysis in the context of phone records. In that case, the police instructed the telephone company to install a pen register to record all of the phone numbers dialed from a robbery suspect’s home. Although the police request was not accompanied by a warrant or court order, police used the information obtained from the pen register to obtain a warrant to search the suspect’s home. The Court expressed “doubt that people in general entertain any actual expectation of privacy in the numbers they dial.” The Court went on to say that, even if the suspect had a subjective expectation of privacy in the numbers dialed from his home, the suspect’s expectation was not reasonable because “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” Accordingly, by placing phone calls, the suspect “voluntarily conveyed numerical information to the telephone company” and “assumed the risk that the company would reveal to police the numbers he dialed.” The Court based its holding on prior decisions, particularly *United States v. Miller*, which espoused a so-called third-party doctrine applicable to business records. In *Miller*, the Court refused to find a Fourth Amendment violation when federal agents obtained bank records without a warrant because the “information [was] voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” Therefore, no constitutional violation occurs when the government acquires “information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”

---

Smith also produced two well-reasoned dissents.\textsuperscript{42} Justice Stewart saw little difference between the phone numbers dialed in that case, which the Court refused to protect, and the phone conversation in Katz, which the Court did protect.\textsuperscript{43} Just like the numbers dialed, the “conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.”\textsuperscript{44} Justice Stewart concluded that, although the information obtained from a pen register is not as revealing as an actual conversation, it is “not without content” and “easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person’s life.”\textsuperscript{45} Likewise, Justice Marshall sharply criticized the Court’s reliance on the purported voluntariness of the disclosure in Smith.\textsuperscript{46} According to Justice Marshall, a person can only assume the risk of conveying information to another party legitimately if the person has a choice regarding whether to convey that information.\textsuperscript{47} Justice Marshall noted that no real choice is involved in deciding whether to use a telephone, which is more properly termed a necessity for most people in modern times.\textsuperscript{48} He further criticized the application of the third-party doctrine, stating that “[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.”\textsuperscript{49} Justice Marshall also reasoned that, under the Court’s assumption of risk analysis, all the police need to do to sidestep the Fourth Amendment is publicly announce their intent to intercept random phone calls and letters, thereby “put[ting] the public on notice of the risks they would thereafter assume in such communications.”\textsuperscript{50} Justice Marshall argued for a more restrictive interpretation of the third-party doctrine, writing that the determination of whether a person has assumed the risk of a third party disclosing information to the government should not be based “on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society.”\textsuperscript{51}

In two cases that serve as an important analog for current location information litigation, the Court made clear that individuals have no reasonable
expectation of privacy in their movements on public roads. In *United States v. Knotts*, the police obtained permission from a chemical company to place a tracking beeper inside a container of chloroform; the chloroform was, in turn, sold to someone suspected of manufacturing illegal drugs. The police used the beeper to maintain visual surveillance of the vehicle transporting the container and, eventually, to obtain a search warrant, which led to the discovery of drug-making equipment. The Court stated that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” According to the Court, it made no difference that the police were aided in their observations of the vehicle’s movements by a tracking device. Therefore, the Court found nothing unconstitutional in the police officers’ use of technology to augment what they could already legally do.

*United States v. Karo* also involved government monitoring of a drug suspect with a tracking beeper hidden in a container of chemicals. In *Karo*, however, the federal agents also used the beeper to reveal information from inside the suspect’s home. According to the Court, the agents crossed a constitutional line when they used the beeper to determine something they could not have visually observed from outside the suspect’s house. The Court stated that using the beeper to verify the container’s location inside the suspect’s home was no different than physically entering the home and visually verifying the container’s location. Therefore, the Court established a distinction between monitoring on open roads and monitoring the inside of a private residence.

---

53. 460 U.S. 276.
54. See id. at 278.
55. See id. at 278–79.
56. Id. at 281.
57. Id. at 282 (“The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of [the suspect’s] automobile to the police receiver, does not alter the situation.”).
58. See id. (“Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.”).
60. Id. at 708.
61. See id. (“[A]gents determined by using the beeper that the ether was still inside the house . . . .”)
62. See id. at 715.
63. See id. at 715, 716 (“Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.”)
64. See id. at 713–14. Compare United States v. Knotts, 460 U.S. 276, 282 (1983) (finding no constitutional violation when the police use technology to augment visual surveillance of movements on public roads), with *Karo*, 468 U.S. at 714 (finding that police use of technology to monitor the inside of a private residence does violate the Constitution).
In *Kyllo v. United States*, the Court considered a different kind of technology used to glean information about the interior of a suspect’s home. *Kyllo* required the Court to determine the constitutionality of federal agents using a thermal imaging device to measure the amount of heat coming from a drug suspect’s home. Agents used the device to gather evidence of the use of heat lamps to grow marijuana plants indoors; this evidence was, in turn, used to obtain a warrant to search the residence. The Court found it dispositive that the imaging device revealed details about the interior of the suspect’s home, which is protected under the Fourth Amendment. Importantly, for purposes of comparison to police tracking movements on public roads, the Court made clear that it was irrelevant whether the information could also have been obtained by some other means; rather, the constitutional violation itself is important.

The Court again took up the issue of police monitoring of an individual’s movements on public roads in *United States v. Jones*. Holding that the government agents committed an unconstitutional search, the majority found dispositive the fact that the agents placed a GPS tracking device on the suspect’s car without a warrant. Although the Court held that the *Katz* reasonable expectation of privacy test was not necessary to decide the case, the Court did not repudiate that standard. In his concurrence, Justice Alito relied on the reasonable expectation of privacy analysis to find that the warrantless GPS surveillance was unconstitutional. Tellingly, Justice Alito noted the ability of law enforcement to use cell phones as tracking devices. He noted that the widespread availability of these devices, combined with the ease with which law enforcement can utilize them, supported reconsideration of privacy expectations. Justice Alito suggested a legislative solution, noting the lack of

---

66. See id. at 29.
67. See id. at 29–30.
68. See id. at 34 (“We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area’, . . . constitutes a search—at least where (as here) the technology in question is not in general public use.”) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).
69. See id. at 35 n.2 (“The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.”).
70. 132 S. Ct. 945 (2012).
71. See id. at 949 (“It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information.”).
72. See id. at 952 (“[T]he *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”).
73. See id. at 964 (Alito, J., concurring) (“[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.”).
74. Id. at 963.
75. Id. at 963–64.
federal and state legislation to regulate the police use of this technology.\textsuperscript{76} Justice Sotomayor also wrote a separate concurrence, agreeing that the police violated the Fourth Amendment by attaching the tracking device onto Jones’s car without a warrant.\textsuperscript{77} However, Justice Sotomayor also agreed with Justice Alito that long-term, warrantless monitoring could, by itself, violate the Fourth Amendment.\textsuperscript{78} Justice Sotomayor suggested reconsidering the third-party doctrine, stating that 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.”\textsuperscript{79} Although the Court did not need to consider the third-party doctrine to decide Jones, Justice Sotomayor noted that such disclosures would only be constitutionally protected “if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.”\textsuperscript{80}

\subsection*{B. Lower Courts}

To date, the Supreme Court has yet to hear a case regarding the police use of CSLI. Lower courts have grappled with this and related issues, however, and have reached different conclusions.\textsuperscript{81} For instance, the Fourth Circuit held that subscriber information—including an individual’s name and address—conveyed to phone companies and Internet Service Providers (ISPs) is not protected by the Fourth Amendment because any expectation of privacy a person may have in such information is unreasonable.\textsuperscript{82} The Fourth Circuit, however, has not yet heard a case dealing with the police use of CSLI.

In contrast, the Third, Fifth, and Sixth Circuits have explicitly ruled on challenges to the police use of CSLI in criminal investigations.\textsuperscript{83} While these circuits have reached different conclusions with respect to the standard the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{76} Id. at 964.
\item \textsuperscript{77} See id. at 954 (Sotomayor, J., concurring) (quoting id. at 950 n.3 (majority opinion)) (“The Government usurped Jones’s property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection.”).
\item \textsuperscript{78} See id. at 955 (quoting id. at 964 (Alito, J., concurring)).
\item \textsuperscript{79} Id. at 957.
\item \textsuperscript{80} Id.
\item \textsuperscript{81} \textit{Compare In re Application of the U.S. for Historical Cell Site Data,} 724 F.3d 600, 615 (5th Cir. 2013) (holding that the lesser standard of “specific and articulable facts” for CSLI data in the Stored Communications Act is not unconstitutional, even though it does not rise to the level of a Fourth Amendment “probable cause” standard), \textit{and United States v. Skinner,} 690 F.3d 772, 775 (6th Cir. 2012) (holding that individuals have no reasonable expectation of privacy in CSLI), \textit{with In re Application of the U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t,} 620 F.3d 304, 319 (3d Cir. 2010) (holding that judges have discretion to require a warrant showing probable cause before issuing orders to disclose CSLI).
\item \textsuperscript{82} United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010).
\item \textsuperscript{83} See \textit{In re Application for Historical Cell Site Data,} 724 F.3d at 605–06 (citing Katz v. United States, 389 U.S. 347, 353 (1967)); Skinner, 690 F.3d at 775–76; \textit{In re Application for an Order Directing Provider of Elec. Commc’n Serv.,} 620 F.3d at 305–06.
\end{itemize}
\end{footnotesize}
government must meet in applications for orders to produce CSLI,\(^{84}\) this
discrepancy is largely the result of differing statutory, rather than constitutional,
interpretations.\(^ {85}\) Furthermore, even the CSLI case from the Third Circuit—
which ostensibly provides more protection for individual privacy—will, in most
cases, not require the government to obtain a warrant based on probable cause.\(^ {86}\)
In the \textit{In re Application for the United States for an Order Directing a
Provider of Electronic Communication Service to Disclose Records to the
Government} case, the Third Circuit compared CSLI to the tracking devices at
issue in \textit{Karo} and \textit{Knotts}.\(^ {87}\) Based on this comparison, as well as the fact that no
evidence showed that the CSLI revealed any information about a user’s location
inside the home, the court held that an order to obtain CSLI did not require
probable cause per se.\(^ {88}\) Instead, the court’s decision turned on the language of
the statute the government used to request the court order: the Stored
Communications Act (SCA).\(^ {89}\) The court noted two methods by which the
government may seek a disclosure of CSLI: through a warrant or an order under
the SCA.\(^ {90}\) Because obtaining a warrant supported by probable cause is one of
those methods, the court held that a judge \textit{could} require a warrant showing
probable cause instead of issuing an order under the SCA.\(^ {91}\) Nonetheless,
despite recognizing that “[a] cell phone customer has not ‘voluntarily’ shared his
location information with a cellular provider in any meaningful way,”\(^ {92}\) the court
concluded that requiring a warrant supported by probable cause “is an option to
be used sparingly.”\(^ {93}\)

\footnotesize{\textsuperscript{84} See \textit{supra} note 81 and accompanying text.  
\textsuperscript{85} See \textit{infra} notes 87–97 and accompanying text.  
\textsuperscript{86} See \textit{In re Application for an Order Directing Provider of Elec. Commc’n Serv.}, 620 F.3d
at 319 (stating that requiring a warrant to obtain CSLI “is an option to be used sparingly” given the
statutory availability of a court order).  
\textsuperscript{87} \textit{Id.} at 312 (quoting United States v. Karo, 468 U.S. 705, 714–715 (1984)) (citing United
States v. Knotts, 460 U.S. 276, 281 (1983)).  
\textsuperscript{88} \textit{Id.} at 312–13.  
\textsuperscript{89} See \textit{id.} at 305–06 (“This appeal gives us our first opportunity to review whether a court
can deny a Government application under [the SCA] after the Government has satisfied its burden
of proof under that provision . . . .”). The SCA provides the means by which the government can
acquire information from electronic communication providers. See \textit{id.} at 306. In addition to listing
the information that can be obtained, the SCA also details the methods that may be used to obtain
that information. See 18 U.S.C. § 2703(a)-(d) (2012). Electronic communication service providers
can be ordered to turn over customer records by a warrant or a court order issued pursuant to the
SCA. See \textit{id.} § 2703(c)(1)(A)-(B). A court order may be issued pursuant to the SCA “if the
governmental entity offers 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.” \textit{Id.} § 2703(d).  
\textsuperscript{90} See \textit{In re Application for an Order Directing Provider of Elec. Commc’n Serv.}, 620 F.3d
at 319.  
\textsuperscript{91} \textit{id.}  
\textsuperscript{92} \textit{Id.} at 317.  
\textsuperscript{93} \textit{Id.} at 319.}
The Fifth Circuit, in contrast, held that cell phone users do voluntarily turn over their location information to service providers when using their cell phones. The court described a person’s decision to obtain and use a cell phone as a voluntary act leading to the voluntary disclosure of location information every time the person uses the phone. Based on this reasoning, the court held that the business records doctrine, as spelled out in *Smith and Miller*, applied to CSLI. Because the Fourth Amendment was therefore inapplicable, the court held that requiring probable cause and refusing an order that met the lesser “reasonable grounds” and “specific and articulable facts” standard outlined in the SCA was not within the judge’s discretion.

The Sixth Circuit, on the other hand, is unique in its view that CSLI is not entitled to constitutional protection under the Fourth Amendment because acquiring it does not constitute a search. In *United States v. Skinner*, the court determined there is no reasonable expectation of privacy in CSLI produced by a “voluntarily procured . . . cell phone.” The court compared the location information a cell phone gives off to the scent a bloodhound might track, concluding that requiring a warrant to follow the former, when one obviously is not necessary to trace the latter, would mean that “technology would help criminals but not the police.” The court saw “no inherent constitutional difference between trailing a defendant and tracking him via such technology [as CSLI and GPS].”

---

94. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 612 (5th Cir. 2013) (“[U]sers know that they convey information about their location to their service providers when they make a call and . . . they voluntarily continue to make such calls.”).

95. *Id.* at 613–14.

96. *See id.* at 615 (“Cell site data are business records and should be analyzed under that line of Supreme Court precedent”); *see also Smith v. Maryland*, 442 U.S. 735, 744 (1979) (stating that there is no reasonable expectation of privacy in phone numbers voluntarily conveyed to the phone company in the ordinary course of its business); *United States v. Miller*, 425 U.S. 435, 442 (1976) (concluding that a person has no reasonable expectation of privacy in financial documents voluntarily given to a bank for use in the ordinary course of the bank’s operations).

97. *In re Application for Historical Cell Site Data*, 724 F.3d at 615; *see also* 28 U.S.C. § 2703(d) (2012).

98. *See United States v. Barajas*, 710 F.3d 1102, 1108 n.2 (10th Cir. 2013).

99. *United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012); *see also id.* at 781 (“Because authorities tracked a known number that was voluntarily used while traveling on public thoroughfares, Skinner did not have a reasonable expectation of privacy in the GPS data and location of his cell phone.” (emphasis added)). The Sixth Circuit distinguished this case from *Jones* by noting that the Supreme Court’s holding in *Jones* was based on a physical trespass, an issue that was absent in *Skinner*. *See id.* at 780 (quoting *United States v. Jones*, 132 S. Ct. 945, 949 (2012)).

100. *Id.* at 777.

101. *Id.* at 778. In *Skinner*, the police acquired both CSLI and real-time GPS information. *See id.* at 776. Privacy advocates and defense lawyers have widely criticized *Skinner*. According to one defense attorney, following *Skinner* could very well lead to the conclusion that the government could track any vehicle, at any time, if it was already equipped with a GPS device. *See Daniel K. Gelf, United States v. Skinner: Using a Cell Phone Is Not a Consent to Search*, THE CHAMPION, Nov. 2012, at 30, 31.

Others have warned that the court’s holding in *Skinner* “could easily undergird a police state where all citizens are subject to electronic surveillance.” Richard Sobel,
While the Fourth Circuit has not heard a case dealing with CSLI, a district court within the circuit has addressed the issue. In United States v. Graham, the U.S. District Court for the District of Maryland noted that this issue was one of first impression in the circuit. In its survey of court opinions, the court noted that most decisions do not implicate the Fourth Amendment’s probable cause requirement; instead, most courts rely on the business records doctrine. Therefore, the court refused to hold that police actions pursuant to the SCA violate a reasonable expectation of privacy.

Regardless of the possibility of an appeal, the Fourth Circuit is unlikely to provide much in the way of privacy protection for CSLI because the defendants, in objecting to the government’s use of their CSLI, did not argue that the SCA’s “reasonable grounds” and “specific and articulable facts” standard was unconstitutional. Instead, the defendants “ma[de] an as-applied challenge” based on “the length of time and extent of the cellular phone monitoring” gathered by the police. Presumably, then, the most that the Fourth Circuit could do on appeal is find that extensive CSLI covering a lengthy period of time can only be obtained with a warrant supported by probable cause. No evidence indicates that the court would hold that such a warrant is always required. Accordingly, individuals in the Fourth Circuit should not rely on that court to provide greater privacy protections.

C. What It Means

Several common strands run through the decisions of the federal courts regarding privacy protections for CSLI. These decisions show a reluctance to


104. Id. at 388.
105. See id. at 389.
108. Id. (“Essentially, the Defendants present[ed] the question of whether twenty-four hour ‘dragnet’ surveillance by emerging technological means infringes on the Fourth Amendment’s guarantee against unreasonable searches and seizures.”).
109. See generally United States v. Hager, 721 F.3d 167, 182 (4th Cir. 2013) (noting that when constitutional challenges to a statute are not raised at the district court level, the decision is subject only to plain error review).
110. See, e.g., United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding that an individual has no reasonable expectation of privacy in subscriber information voluntarily given to phone and Internet companies).
protect information conveyed to a third party, regardless of whether the information is consciously communicated to that third party. The courts’ reluctance is especially troubling in the context of modern technology. For instance, because CSLI is automatically generated whenever a cell phone is turned on, a cell phone user usually does not voluntarily convey this information to anyone—at least not in any meaningful sense of the word.

The courts have also compared CSLI to financial records given to a bank and numbers dialed from a particular phone that are communicated to a phone company. These analogies are faulty, however, because CSLI is generated by a user’s cell phone and communicated without any action from the user.

Police collection of CSLI stands in contrast to a list of numbers dialed from a certain phone, which, by definition, only contains numbers that a user has communicated to the phone company when that user chooses to call a particular person or business. Location information, on the other hand, is constantly generated every few seconds without any input from the phone’s user.

The comparison to a list of phone numbers and financial records is lacking for another reason as well. While phone numbers can be revealing, CSLI threatens to be much more so. As Justice Sotomayor noted, knowing where a person travels can reveal an abundance of intimate details about that person. Such information can reveal personal details that would otherwise be unavailable without constant, around-the-clock visual surveillance. In addition, as the U.S. District Court for the Southern District of Texas recognized, CSLI does not merely reveal information about movements on public streets; it has become refined enough to reveal movements within buildings and even homes, which have historically received the greatest protection from the government’s inquiring eye.

Even though federal courts have been hesitant to recognize a reasonable expectation of privacy in information conveyed to third parties, some signs indicate that this disinclination may be changing. The concurrences in Jones

111. See, e.g., supra notes 92–93 and accompanying text (noting that, despite the lack of voluntary conveyance of information, the information is still shared with a third party).
112. See In re Application of the U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records, 620 F.3d 304, 317 (3d Cir. 2010).
113. See supra note 96 and accompanying text.
114. See supra notes 18–19 and accompanying text.
116. See id. at 956 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)) (noting that new technology allows the police to perform surveillance that would have previously been financially untenable).
117. See supra notes 23–24 and accompanying text.
119. See supra notes 31–41 and accompanying text.
revealed that a majority of the Supreme Court is willing to recognize that long-term, widespread monitoring of a person’s movements violates that person’s reasonable expectations of privacy. 120 While the monitoring in Jones involved a GPS device attached to an individual’s car, 121 the same standard can logically apply to CSLI gathered from an individual’s cellular service provider. As Justice Sotomayor hinted, it borders on the absurd to continue basing privacy jurisprudence on the notion that individuals lose a reasonable expectation of privacy in information they do not keep completely secret. 122 The concurrences of Justices Sotomayor and Alito in Jones demonstrate a positive step toward federal courts reevaluating privacy norms and, perhaps, the federal judiciary’s recognition of changing privacy expectations in the twenty-first century. 123

Hopefully, these concurrences presage a growing awareness by the federal judiciary that when people decide to purchase and use cell phones, they do not also decide to allow the government to track their every movement. 124

Privacy advocates also have reason to be excited about Klayman v. Obama, 125 a recent district court decision regarding the related issue of the NSA’s mass collection of Americans’ telephone metadata. Although the government defended the program by referring to the holding in Smith—that people have no reasonable expectation of privacy in the phone numbers they dial because the numbers are communicated to the phone company, a third party—the U.S. District Court for the District of Columbia disagreed. 126 The court concluded “that [the] plaintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata,” 127 criticizing the indiscriminate collection of Americans’ data as “almost-Orwellian.” 128 The court questioned the continued validity of using Smith to decide issues such as the one before it, noting that “the relevance of [Smith] has been eclipsed by technological advances and a cell phone-centric lifestyle heretofore inconceivable.” 129

120. See supra notes 73–80 and accompanying text.
122. See id. at 957 (Sotomayor, J., concurring).
123. See supra notes 73–80 and accompanying text.
124. See generally Gelb, supra note 101, at 31 (“Cell phones . . . are not purchased with the expectation that the government will have unfettered access in order to mine through the geolocation data created through use of the phone.”).
126. See id. at 30–31 (citing Smith v. Maryland, 442 U.S. 735, 742–44 (1979)).
127. Id. at 39.
128. Id. at 33. But see ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (finding the NSA’s collection of metadata constitutional). In ACLU v. Clapper, the U.S. District Court for the Southern District of New York pointed to the terror attacks of September 11, 2001, to support its conclusion that the massive data collection program is an essential tool in counteracting terrorists’ use of technology to plan and carry out attacks. See id. at 757.
129. Klayman, 957 F. Supp. 2d at 43; see also id. at 37 (“[T]he Smith pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between
While these and other federal decisions indicate growing unease with using twentieth century cases to resolve twenty-first century problems, they also indicate that change is often slow. While some courts—even the Supreme Court—have indicated a willingness to readdress privacy precedent, federal decisions are still dominated by a belief that any information conveyed to another is undeserving of privacy protections. Unless the Supreme Court revisits its holding in Smith, the federal judiciary seems unlikely to provide privacy protection to Americans’ CSLI. As one scholar noted, for the time being, “as a matter of federal law we are solely dependent upon statutory protection for all third party information.”

---


131. See, e.g., Clapper, 959 F. Supp. 2d at 749 (“[A]n individual has no legitimate expectation of privacy in information provided to third parties”); see also Shaun B. Spencer, The Surveillance Society and the Third-Party Privacy Problem, 65 S.C.L. REV. 374, 383–84 (2013) (noting that “one cannot expect privacy in information shared with third parties”). At least one scholar has argued that the third-party doctrine should be limited to information revealed to a third party for use by that third party. See Henderson, supra note 130, at 378 (citing Stephen E. Henderson, Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search, 56 MERCER L. REV. 507, 524–28 (2005) [hereinafter Nothing New Under the Sun?]). For instance, a phone company does not need to know a cell phone user’s location to complete a call, so that information should be protected by a reasonable expectation of privacy. Cf. Nothing New Under the Sun?, supra, at 526 (noting that, even though the contents of a telephone conversation are transmitted via the phone company’s network, users retain a reasonable expectation of privacy in those contents because the phone company need not know them to complete the call). For an argument that a “justifiable reliance” standard would provide greater privacy protections than the reasonable expectation of privacy standard, see Sobel et al., supra note 101, at 23–28 (citations omitted).

132. See, e.g., Sobel et al., supra note 101, at 44 (“Whatever the legislative protections, the Supreme Court needs to articulate a clear restatement that electronic intrusions and the use of sense-enhancing tools constitute searches and require warrants supported by probable cause.”).

133. Henderson, supra note 130, at 413.
III. STATE ACTION

A. Legislative Action: Montana and Maine

Despite the equivocation at the federal level, some states have taken definitive steps to provide greater privacy protections for cell phone users.\textsuperscript{134} For example, Montana and Maine recently enacted laws requiring that police obtain warrants before acquiring CSLI.\textsuperscript{135} In addition, the New Jersey Supreme Court recently held that police in that state also must obtain warrants before acquiring CSLI, noting that the state constitution provides greater protections than those found in the Fourth Amendment.\textsuperscript{136} These states’ actions are a step in the right direction and demarcate a clear path forward that South Carolina can, and should, follow.

Montana was the first state to pass a law requiring that police get a warrant supported by probable cause to obtain CSLI.\textsuperscript{137} The Montana statute includes a blanket prohibition against the government acquiring location information from an electronic device without first obtaining a warrant.\textsuperscript{138} The statute defines an electronic device, in part, as “a device that enables access to or use of an electronic communication service,”\textsuperscript{139} and location information as “information concerning the location of an electronic device that, in whole or in part, is generated or derived from or obtained by the operation of an electronic device.”\textsuperscript{140} The definitions of electronic device and location information clearly


\textsuperscript{136} See Zernike, supra note 135; see also infra Part III.B.

\textsuperscript{137} See Allie Bohm, First in the Nation: Montana Requires a Warrant for Location Tracking, ACLU (June 20, 2013, 10:15 A.M.), https://www.aclu.org/blog/technology-and-liberty-national-security/first-nation-montana-requires-warrant-location; Gallagher, supra note 135.

\textsuperscript{138} See MONT. CODE ANN. § 46-5-110(1)(a) (2013). It is worth noting that the Montana constitution explicitly protects the right to privacy. See MONT. CONST. art. 2, § 10.

\textsuperscript{139} MONT. CODE ANN. § 46-5-110(1)(a).

\textsuperscript{140} Id. § 46-5-110(2)(d).
encompass the CSLI automatically generated by cell phones. The statute then lists exceptions to this general rule that allow police to obtain such information without a warrant in certain circumstances. Under the statute, police do not need a warrant to obtain location information from an electronic device if the owner of the device reports it stolen, if the police are responding to a call by the user of the device requesting emergency services, if the police have the informed consent of the owner or user of the device, or if a possible life-threatening situation exists. The exception for life-threatening situations anticipates a possible objection from law enforcement, as some have justified the police use of location information by pointing to the number of lives saved as a result of its use. This exception is also consistent with existing Supreme Court precedent regarding exceptions to the warrant requirement for exigent circumstances. Violations of the statute result in the exclusion of evidence so obtained, along with a civil fine.

In Maine, a bill requiring that police obtain a warrant before acquiring CSLI overcame opposition from law enforcement, as well as a governor’s veto, to become law. Similar to the Montana statute, the Maine law generally requires a warrant before the government can obtain location information from an individual’s cell phone. Maine’s statute defines an electronic device, in part, as “a device that enables access to, or use of, an electronic communication service” and location information as “information concerning the location of

141. See supra notes 17–25 and accompanying text.
142. See MONT. CODE ANN. § 46-5-110(1)(b).
143. Id. § 46-5-110(1)(b)(i).
144. Id. § 46-5-110(1)(b)(ii).
145. Id. § 46-5-110(1)(b)(iii).
146. Id. § 46-5-110(1)(b)(iv).
147. See Lichtblau, supra note 9, at A20 (reporting that one police department used location information to find a stabbing victim). According to one criminal analyst, the use of CSLI is valuable because “[w]e find people . . . and it saves lives.” Id. (internal quotation marks omitted).
148. See, e.g., Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) (“One exigency obviating the requirement of a warrant is the need to assist persons who are seriously injured or threatened with such injury.”).
149. See MONT. CODE ANN. § 46-5-110(1)(c)–(d). Given that the fine is capped at fifty dollars, enforcement of the statute will most likely depend on the exclusion provision. See id. § 46-5-110(1)(d).
150. See Christopher Cousins, Maine House Backs Bill to Require Warrant for Cellphone Tracking, BANGOR DAILY NEWS (May 29, 2013, 8:38 PM), http://bangordailynews.com/2013/05/29/politics/state-house/main-state-house-bill-to-require-warrant-for-cellphonetrackings/?ref=latest (noting opposition to the bill from law enforcement); Gallagher, supra note 135 (noting that the Maine legislature overrode the governor’s veto of the bill). Maine also passed legislation protecting the contents of electronic communications. See An Act to Protect Cellular Telephone Privacy, ch. 402, 2013 Me. Laws 993 (codified at ME. REV. STAT. ANN. tit. 16, §§ 641–46 (Supp. 2013)).
152. ME. REV. STAT. ANN. tit. 16, § 647(3).
an electronic device, including both the current location and any prior location of the device, that, in whole or in part, is generated, derived from or obtained by the operation of an electronic device."\textsuperscript{153} The definitions of \textit{electronic device} and \textit{location information} closely mirror those found in the Montana law\textsuperscript{154} and clearly encompass cell phones and the location information they automatically generate.\textsuperscript{155} Much like the law in Montana,\textsuperscript{156} however, the Maine law provides exceptions to the warrant requirement.\textsuperscript{157} Specifically, the Maine law allows the police to obtain CSLI without a warrant in response to a request for emergency services,\textsuperscript{158} with the consent of the owner or user of an electronic device,\textsuperscript{159} with the consent of the guardian or next of kin of an owner or user of a device believed to be dead or reported missing,\textsuperscript{160} or when "an emergency involving immediate danger of death or serious physical injury" exists and "a warrant cannot be obtained in time to prevent the identified danger."\textsuperscript{161} The law also requires the government—with some exceptions—to give notice to an individual that the government has acquired location information about that individual from an electronic device.\textsuperscript{162} Within three days of obtaining the location information, the government must inform the individual about the nature of its inquiry; what location information was acquired; and, if the information was acquired from a third party, from whom it was acquired.\textsuperscript{163} This provision is important because an individual would otherwise not likely know that the government has obtained personal CSLI: gathering of such information by the police is "typically done without . . . public awareness."\textsuperscript{164} In fact, "[m]any departments try to keep cell tracking secret" to avoid a "possible backlash from the public."\textsuperscript{165}

B. Judicial Action: New Jersey

New Jersey also recently made headlines by extending privacy protections to CSLI.\textsuperscript{166} The development in New Jersey, however, came not from the legislature, but from the state supreme court.\textsuperscript{167} In \textit{State v. Earls},\textsuperscript{168} the Supreme Court of New Jersey held that individuals have a protected privacy interest in the

\textsuperscript{153} Id. § 647(5).
\textsuperscript{155} See supra notes 17–25 and accompanying text.
\textsuperscript{156} See Mont. Code Ann. § 46-5-110(1)(b).
\textsuperscript{158} Id. § 650(1).
\textsuperscript{159} Id. § 650(2).
\textsuperscript{160} Id. § 650(3).
\textsuperscript{161} Id. § 650(4).
\textsuperscript{162} See id. § 649.
\textsuperscript{163} See id. § 649(1).
\textsuperscript{164} Zernike, supra note 135.
\textsuperscript{165} Lichtblau, supra note 9, at A20.
\textsuperscript{166} See Zernike, supra note 135.
\textsuperscript{167} See id.
\textsuperscript{168} 70 A.3d 630 (N.J. 2013).
location information created by their cell phones. The court’s holding was based on its interpretation of the New Jersey constitution. The language in New Jersey’s analog to the Fourth Amendment is essentially identical to that found in the Federal Constitution. Notwithstanding the similarity of the language, the court noted that “the protections [granted by the Fourth Amendment and the state constitution] against unreasonable searches and seizures are not always coterminous.” Therefore, although a warrant may not be required to obtain location information from a cell phone as a matter of federal constitutional law, the New Jersey Supreme Court was not foreclosed from deciding that a warrant is required as a matter of state constitutional law.

The holding in Earls was supported, in large part, by previous decisions of the New Jersey Supreme Court interpreting the state constitution’s role in resolving privacy issues. In addition to cases interpreting the state constitution, the court also addressed the third-party doctrine as well as the nature of CSLI, considering how these issues relate to reasonable expectations of privacy.

Importantly, the court noted that the third-party doctrine had been effectively rejected in New Jersey. For example, in State v. Reid, the Supreme Court of New Jersey determined that a person has a legitimate privacy interest in subscriber information provided to ISPs. In so concluding, the court acknowledged that it was diverging from “settled federal law that a person has no reasonable expectation of privacy in information exposed to third parties.” Additionally, in State v. McAllister, the court held that “under the New Jersey Constitution, citizens have a reasonable expectation of privacy in bank

169. Id. at 644 (“[T]he New Jersey Constitution protects an individual’s privacy interest in the location of his or her cell phone.”).
170. Id. (“Our ruling today is based solely on the State Constitution.”).
171. See U.S. CONST. amend. IV; N.J. CONST. art. 1, para. 7.
172. Earls, 70 A.3d at 641 (quoting State v. Hunt, 450 A.2d 952, 955 (N.J. 1982)) (internal quotation marks omitted).
173. See id. (noting that, despite the similarities between the two constitutions, Fourth Amendment rights offered under the New Jersey constitution often provide greater protection than the U.S. Constitution); see also id. at 644 (“We recognize that [United States v.] Jones and Smith [v. Maryland], to the extent they apply, would not require a warrant in this case.”).
174. See id. at 641 (“On a number of occasions, this Court has found that the State Constitution provides greater protection against unreasonable searches and seizures than the Fourth Amendment.”).
175. See id. at 641–44 (citations omitted).
176. See id. at 641 (“[A]n individual’s privacy interest under New Jersey law does not turn on whether he or she is required to disclose information to third-party providers to obtain service.”).
177. 945 A.2d 26 (N.J. 2008).
178. Id. at 28. But see United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding that individuals have no reasonable expectation of privacy in subscriber information voluntarily given to phone and Internet companies).
179. Reid, 945 A.2d at 31.
Finally, in a decision finding an expectation of privacy in phone records, the court observed that “[i]t is unrealistic to say that the cloak of privacy has been shed because the telephone company and some of its employees are aware of this information.”

The Supreme Court of New Jersey still relies on reasonable expectations of privacy in determining whether government action constitutes an unreasonable search or seizure. However, because the state supreme court has sometimes disagreed with the U.S. Supreme Court as to what constitutes a reasonable expectation of privacy, and because the state constitution provides greater protections than the Fourth Amendment, the analysis can be very different. As noted above, the fact that one has disclosed something to a third party does not, by itself, destroy that person’s reasonable expectations of privacy under New Jersey law. For instance, in Reid, when the court held that subscriber information provided to ISPs is protected by a reasonable expectation of privacy, the court relied on people’s common sense expectations when using the Internet.

In concluding that individuals have a reasonable expectation of privacy in CSLI, the Supreme Court of New Jersey noted the extent of the information that such data can reveal. The court determined that CSLI can be even more revealing than a person’s phone records or Internet history—turning a cell phone into “a tracking device” that acts “as a substitute for 24/7 surveillance” and “involves a degree of intrusion that a reasonable person would not anticipate.” Importantly, the court also noted that, because CSLI is continuously created, it includes records of a person in both public and private places. Therefore, CSLI “does more than simply augment visual surveillance in public areas.”

Considered in that light, the police use of CSLI is more akin to the type of monitoring deemed unconstitutional in Karo than that upheld in Knotts.

Finally, in highlighting the role that cell phones play in modern society, the court

---

181. Id. at 867. But see United States v. Miller, 425 U.S. 435, 442 (1976) (concluding that a person has no reasonable expectation of privacy in financial documents voluntarily given to a bank).
184. See, e.g., State v. Reid, 945 A.2d 26, 28, 31 (N.J. 2008) (discussing the court’s rejection of the federal third-party doctrine for information provided to ISPs).
185. See Earls, 70 A.3d at 641.
186. See id.
187. See Reid, 945 A.2d at 33 (“[W]hen users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential.”).
188. See Earls, 70 A.3d at 642.
189. Id.
190. See id.
191. Id. at 643.
192. See supra notes 59–64 and accompanying text.
193. See supra notes 53–58 and accompanying text.
stated that the ubiquity of cell phones, combined with the reasons for which they are used, leads to the conclusion that people have a justifiable expectation of privacy in the location information they generate by using their cell phones.194

C. What It Means

While many federal courts remain in strict allegiance to the third-party doctrine, some states have acted in accordance with the Court’s statement in Katz that privacy is an area largely governed by state law.195 Although—even after Jones—federal courts continue to compare modern technological developments such as CSLI to items as mundane as a smell that a dog can trace,196 the above discussion shows that some states have boldly progressed into the twenty-first century. Furthermore, some states have even rejected the third-party doctrine entirely, thus removing a major barrier in the way of protecting CSLI.197

Any attempt to catalog every state’s substantive privacy standards would, of course, be a lengthy process and one beyond the scope of this Note.198 Such a survey would necessarily be complex and incomplete.199 What is important is that states can, and have, provided privacy protections beyond those found in the Fourth Amendment. Further, from a practical perspective, a state decision requiring the police to obtain a warrant supported by probable cause before obtaining CSLI does not amount to a decision condemning the state to rampant criminality.200 Finally, notwithstanding the effectiveness of legislative action to

194. See Earls, 70 A.3d at 643. The court noted that people do not buy cell phones so that the police can track their every movement and, even though many people may know that their phones can be tracked, most people do not know the extent to which they can be tracked—and they certainly do not expect the police to do so. Id.
196. See, e.g., United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012) (comparing use of a pay-as-you-go cell phone to the use of fugitive tracking dogs because “[t]he law cannot be that a criminal is entitled to rely on the expected untrackability of his tools”).
197. See Henderson, supra note 130, at 413 (noting that eleven states reject the third-party doctrine and signs show that ten others may also reject it); see also id. at 425 (“It is encouraging that many states have parted course with the United States Supreme Court with respect to the third-party doctrine, and that others seem inclined to follow.”).
198. See generally id. at 395–412 & nn.117–68 (citations omitted) (examining all fifty states and determining whether they follow the federal third-party doctrine).
199. See id. at 394 (admitting the “uncertainty” and “ambiguity” inherent in such an analysis). For an insightful opinion by a state supreme court justice recognizing the third party doctrine but expressing discomfort at how far it could be extended, see State v. 1993 Chevrolet Pickup, 116 P.3d 800, 806–07 (Mont. 2005) (Nelson, J., concurring). Justice Nelson observed, “I don’t like living in Orwell’s 1984; but I do.” Id. at 807.
200. See supra notes 143–48, 158–61 and accompanying text (listing exceptions to the warrant requirement in certain situations). Cf. Cell Phone Location Tracking Public Records Request, supra note 10 (“If [some] police departments can protect both public safety and privacy by [voluntarily] meeting the warrant and probable cause requirements, then surely other agencies can as well.”).
protect privacy, it is worth noting that given the ever-changing nature of modern technology and the amount of disclosure the use of such technology entails, a judicial decision extending privacy protection to CSLI is preferable.

IV. A WAY FORWARD FOR SOUTH CAROLINA

South Carolina’s constitution, statutes, and case law clearly support the proposition that South Carolina courts should provide individuals greater privacy protections than those provided by federal courts. This, in turn, supports the conclusion that the Supreme Court of South Carolina—like the Supreme Court of New Jersey—extend constitutional protection to CSLI.

In contrast to the U.S. Constitution, the South Carolina constitution explicitly states that the people shall be protected against “unreasonable invasions of privacy.” In addition, state law requires a warrant supported by probable cause before authorities can install and use an electronic tracking device. And perhaps most importantly, the South Carolina Supreme Court has explicitly recognized that the state constitution provides greater privacy protections than the U.S. Constitution.

of the writing of this Note, the Author is aware of no reports that Montana, Maine, or New Jersey have descended into anarchy.

201. See Henderson, supra note 130, at 425 (“In a world in which we give so much information to third parties, piecemeal statutory protection is insufficient.”); see also id. at 386 (observing that legislative protections can be removed as easily as they can be created).

202. S.C. CONST. art. I, § 10. Compare id. (“The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated . . . .”) (emphasis added), with U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .”). Montana, another state with an explicit privacy provision in its constitution, recently enacted legislation requiring warrants for the police acquisition of CSLI. See supra notes 137–40 and accompanying text.

203. See S.C. CODE ANN. § 17-30-140 (2014). The statute not only makes clear that courts can require greater specificity than that required by the statute, but also that its provisions are subject to the standards established by the U.S. Supreme Court regarding the installation and use of tracking devices. Id. § 17-30-140(D)-(E). The statute defines a tracking device as “an electronic or mechanical device which permits the tracking of the movement of a person or object.” Id. § 17-30-140(F). Relying heavily on the Supreme Court’s decision in Jones, one South Carolina court held that the police committed an unreasonable search in violation of the suspect’s constitutional rights when they placed a GPS tracking device on the suspect’s vehicle without first obtaining a warrant. See State v. Adams, 397 S.C. 481, 487-89, 725 S.E.2d 523, 527 (Ct. App. 2012) (quoting United States v. Jones, 132 S. Ct. 945, 949 (2012); Minnesota v. Dickerson, 508 U.S. 366, 372 (1993)). Given the tracking capabilities of cell phones, applying the same standard to CSLI as to external tracking devices would not be a great leap.

204. See State v. Forrester, 343 S.C. 637, 541 S.E.2d 837 (2001); see also Christopher R. Jones, Note, “eyePhones”: A Fourth Amendment Inquiry into Mobile Iris Scanning, 63 S.C. L. REV. 925, 942 (2012) (stating that the South Carolina Supreme Court has interpreted article I, section 10 of the state constitution to offer a higher level of privacy protection than that offered by the Fourth Amendment of the U.S. Constitution).
The South Carolina Supreme Court fully recognized the greater protections afforded by the state constitution in *State v. Forrester.*205 The court observed that the Federal Constitution establishes the minimum for individual rights, whereas the state constitution establishes the outer limits of those rights.206 Accordingly, state courts can interpret state constitutional provisions so as to provide greater protection than analogous federal provisions.207 The South Carolina Supreme Court further stated that “by articulating a specific prohibition against ‘unreasonable invasions of privacy,’ the people of South Carolina have indicated that searches and seizures that do not offend the [F]ederal Constitution may still offend the South Carolina Constitution.”208 Therefore, the state constitution “favors an interpretation offering a higher level of privacy protection than the Fourth Amendment.”209

Most importantly, for the purposes of this Note, the South Carolina Supreme Court noted that “the drafters of our state constitution’s right to privacy provision were principally concerned with the emergence of new electronic technologies that increased the government’s ability to conduct searches.”210 The drafters intended to create a provision that would provide protections separate from, and in addition to, those provided by the Fourth Amendment in case future Supreme Court jurisprudence proved less protective of individual rights.211 It is telling that the comments made by the drafters of the South Carolina constitution and relied upon by the South Carolina Supreme Court in *Forrester* were made in September and October of 1967—well before the U.S. Supreme Court’s opinions in *Miller, Smith,* and *Knotts,* which are so heavily relied upon today by courts refusing to extend privacy protection to CSLI.212

205. *See Forrester,* 343 S.C. at 644, 541 S.E.2d at 841.
206. *See id.* at 643, 541 S.E.2d at 840.
207. *See id.* at 644, 541 S.E.2d at 840 (“[The South Carolina Supreme] Court can interpret the state protection against unreasonable searches and seizures in such a way as to provide greater protection than the federal Constitution.”); *see also State v. Austin,* 306 S.C. 9, 16, 409 S.E.2d 811, 815 (Ct. App. 1991) (“It is firmly established that state courts may interpret their own constitutions in such a way as to expand rights conferred by the Federal Constitution. The principle of federalism envisions two separate and independent judicial systems: federal courts, which construe federal law, and state courts, which construe state law. State courts may, therefore, develop state law to provide their citizens with a second layer of constitutional rights.”) (footnotes omitted) (citing William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights,* 90 HARV. L. REV. 489, 503 (1977)).
208. *Forrester,* 343 S.C. at 644, 541 S.E.2d at 841.
209. *Id.* at 645, 541 S.E.2d at 841.
210. *Id.* at 647, 541 S.E.2d at 842. The South Carolina Supreme Court also quoted the drafters as saying that the state constitution “should be revised to take care of the invasion of privacy through modern electronic devices.” *Id.* (quoting COMMITTEE TO MAKE A STUDY OF THE CONSTITUTION OF SOUTH CAROLINA, 1895, MINUTES OF COMMITTEE MEETING 6 (Sept. 15, 1967)).
211. *See id.* (quoting COMMITTEE TO MAKE A STUDY OF THE CONSTITUTION OF SOUTH CAROLINA, 1895, MINUTES OF COMMITTEE MEETING 7 (Oct. 6, 1967)).
Although the comments are not binding, the foresight shown by the drafters of the South Carolina constitution is compelling evidence that the protection against unreasonable invasions of privacy in the state constitution should be extended to include a prohibition against the warrantless tracking of individuals through a device that has become as intimately intertwined with modern life as the cell phone.

Lest this Note appear naively optimistic, it is worth noting that there are, of course, significant differences between South Carolina jurisprudence and the jurisprudence of New Jersey, which this Note argues South Carolina should follow. For instance, unlike South Carolina, New Jersey has effectively rejected the third-party doctrine. Professor Henderson also notes that, although the South Carolina Supreme Court has held that the state constitution provides greater privacy protections than the Fourth Amendment, it has—at least so far—interpreted the state constitutional provision in lockstep with the Fourth Amendment.

Professor Henderson also notes, however, that it is difficult to analyze state analogs to the Fourth Amendment, particularly given the lack of relevant case law. Indeed, the only case Professor Henderson cites to demonstrate that South Carolina does not recognize a reasonable expectation of privacy in phone numbers dialed is a more than two-decades-old decision dealing with a caller ID service for landline telephones. The dearth of cases further lends support to the notion that the South Carolina Supreme Court should find a reasonable expectation of privacy in CSLI. Indeed, on the same day the South Carolina Supreme Court issued its decision in Southern Bell Telephone & Telegraph Company v. Hamm, the South Carolina Court of Appeals made clear that state courts can interpret state constitutions to provide greater protections than the Federal Constitution; the court of appeals even expressed surprise that the defendant did not make an argument along those grounds. Furthermore, given the vast technical differences between the caller ID system involved in Hamm and present-day cell phone tracking technology, relying on Hamm to deny privacy protection to CSLI would be the equivalent of relying on cassette tapes

213. See Forrester, 343 S.C. at 647 n.7, 541 S.E.2d at 842 n.7.
215. See id. at 412 n.165.
216. See id. at 394 & n.116.
217. See id. at 412 n.165.
for a personal music collection: the listener would be stuck in analog, while the world has become digital.

V. CONCLUSION

Clearly, South Carolina courts need not wait for the U.S. Supreme Court or the Fourth Circuit to declare that the Fourth Amendment requires a warrant supported by probable cause for police to obtain CSLI. The South Carolina Supreme Court has made it clear that the state constitution can provide greater protections for civil liberties than its federal counterpart.220 Likewise, should the U.S. Supreme Court or the Fourth Circuit hold that police do not need to obtain a warrant supported by probable cause to acquire CSLI, South Carolina courts can, and should, still do so. Such a requirement is the inexorable conclusion, particularly given the state’s constitution and the privacy protections it grants.221

W. Jacob Henerey

220. See supra notes 204-09 and accompanying text.
221. See supra notes 202, 204-12 and accompanying text. Of course, exceptions for exigent circumstances, which already exist in constitutional jurisprudence and which have been codified by statutes in Montana and Maine, should likewise apply to CSLI in South Carolina. No one can deny the benefits of using CSLI in situations such as searching for escaped mental health patients. See Jeffrey Collins, Escapee from SC Mental Hospital Captured in Tenn., ASSOCIATED PRESS, Jan. 3, 2014, available at http://bigstory.ap.org/article/escapee-sc-mental-hospital-captured-tenn (describing how a man found not guilty by reason of insanity of murdering his parents escaped from a mental health hospital in Columbia, South Carolina, and was found in Tennessee when the police tracked his cell phone to a motel there).