I. Introduction

The Fourth Amendment to the U.S. Constitution protects individuals against unreasonable searches and seizures of their “persons, houses, papers, and effects.”1 Before executing a search or seizure (arrest, placing an individual in custody, impounding personal effects, property2), police must obtain a warrant supported by probable cause.3 Massachusetts has, at times, applied a more stringent standard under its constitution on search and seizure matters.4 This Note will focus mainly on how Massachusetts courts have approached law enforcement’s use of Global Positioning System (GPS) technology to apprehend a criminal suspect and subsequent prosecution and to the use of historical cell site information data—records on

---

1 U.S. CONST. amend. IV.
3 See U.S. CONST. amend. IV (establishing the warrant requirement for searches and seizures).
4 See, e.g., Commonwealth v. Connolly, 913 N.E.2d 356, 369 (Mass. 2009) (holding a seizure had occurred under the Massachusetts Constitution upon a “GPS device” being installed in a vehicle).
cell phone usage which police can obtain from phone providers.\(^5\) This Note will address GPS tracking of defendants where courts required a warrant, and other circumstances under which they excepted the warrant requirement. It will also consider policies and recommendations provided by the U.S. Department of Justice (DOJ), efforts by the legislature, and implementation by the police. Legislation like the USA PATRIOT Act of 2001 has expanded the government’s ability to use electronic surveillance domestically in the name of public safety.\(^6\) The tension between our desire to preserve public safety and to maintain a sense of individual privacy, while upholding constitutional protections against abuse of surveillance measures, has raised issues because of the increased sophistication and ubiquity of consumer electronics.\(^7\)

Some Massachusetts lawyers have observed, after *United States v. Jones*,\(^8\) that in light of circuit splits on Fourth Amendment issues pertaining to GPS surveillance, its use as a tool for law enforcement and prosecution is ripe for the Supreme Judicial Court (SJC) to take up again.\(^9\) *Jones* has not settled issues arising where

---


\(^6\) See *Electronic Surveillance Manual*, U.S. DEP’T OF JUSTICE 42 (June 2005) [hereinafter U.S. DEP’T OF JUSTICE], archived at www.perma.cc/0wR75J2wHTV (pointing out USA PATRIOT Act amendments broadened scope of records that may be obtained with subpoena from local and long distance phone billing records to records of connections, session times and durations).

\(^7\) See Maeve Duggan & Lee Rainie, *Cell Phone Activities 2012*, PEW RESEARCH CENTER (Nov. 25, 2012), archived at www.perma.cc/0DRdMekQkmD (finding 85% of American adults own a cell phone used for a wide range of activities involving sensitive information like online banking).

\(^8\) See 132 S. Ct. 945, 947-48 (2012) (bringing the issue of secret surveillance technology back before the Supreme Court).

\(^9\) See Sara E. Silva, *Oh the Places You’ve Been! Preserving Privacy in a Cellular Age*, BOSTON BAR JOURNAL (Sept. 12, 2012), archived at www.perma.cc/0j1AYj1mdbd (challenging the contention that GPS tracking of a cell phone is less invasive than having access to cell phone records and physical surveillance).
GPS is intrinsic to the device for tracking, as it only addressed a situation where an external GPS device is attached. The Supreme Court has left state courts and law enforcement leeway to determine how to balance GPS tracking and Fourth Amendment protections against unreasonable search and seizure.

This Note will look at Commonwealth v. Connolly, the most recent case the SJC has heard on the use of GPS on a defendant’s automobile, bearing some factual similarity to Jones. Connolly, too, failed to make clear what the policy should be where no physical attachment of a separate device is required, such as when law enforcement utilizes an individual’s cellphone, smartphone, or vehicle already equipped with the GPS device in order to track that person. In such cases, police could request that telephone carriers grant access to stored information generated by their target’s use of the GPS. Will a warrant supported by probable cause always be required for impounding those records? What about legal issues arising where police have used more creative means like installing dummy cell towers that allow interception of a defendant’s telecommunications? Are there exigent circumstances under which a warrant will not be required as in other search and seizure cases because of the

---

10 See Maclin & Rader, infra note 59, at 1226-27 and accompanying text (inferring limitations to the Jones holding beyond GPS trackers physically attached to target).
11 See Maclin & Rader, infra note 59, at 1224-26 and accompanying text (predicting that the Roberts Court’s “reassessment” of the exclusionary rule will allow law enforcement excessive leeway and will render the Fourth Amendment devoid of meaning).
12 See 913 N.E.2d at 360 (addressing police surveillance via GPS attachment).
13 See 132 S.Ct. at 947-48 (describing a fact pattern similar to that found in Connolly).
14 See discussion of Justice Sotomayor’s Jones concurrence, infra notes 50, 56, 57 (considering questions unanswered by majority only dealing with physical attachment of tracking device).
15 See sources cited infra notes 113-114 (recognizing no reasonable expectation of privacy for the cell phone owner in cell phone location records so police can obtain them upon request from cell service providers without a warrant); see also Catherine Crump, The Geolocational Privacy and Surveillance Act Before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, AMERICAN CIVIL LIBERTIES UNION, (May 17, 2012), archived at www.perma.cc/0JTCnoqoPgF (noting police frequently track cell phones).
risk of defeating the purpose of police pursuit, such as likely destruction of evidence or risk of violence where a defendant is armed?

This Note will look at some of the proposals intended to protect individuals who arguably face a violation of a reasonable expectation of their privacy in terms of locational data, even when third party resources are being used to generate that data as the individuals move through public and private spaces. Although legislation that would require phone carriers to retain data for only as long as it would be useful to the customer may be a promising measure, would that in turn be impractical for the carriers themselves as part of their business records? There likely needs to be stronger policy that creates clarity and continuity for government agencies and law enforcement. Otherwise, ubiquitous GPS technology could be more likely abused in violation of constitutional rights, where legitimately warranted and targeted surveillance slides into generalized long-term surveillance, becoming part of building probable cause itself. From the prosecutorial side, there should be clarity about a jurisdiction’s policy on the showing required to use GPS surveillance and how to appropriately implement it to preserve that data’s admissibility into evidence rather than bar it under the Fourth Amendment exclusionary

---


17 See Mandatory Data Retention: United States, ELECTRONIC FRONTIER FOUNDATION, Mar. 2, 2013, archived at www.perma.cc/0f8joozDLiz (noting that the U.S. currently has no mandatory data retention law in place, but reviewing some pertinent legislation regarding access to stored communications records).

18 See id. (observing the lack of mandatory data retention law in the U.S.).

19 See Jones, 132 S.Ct. at 956-57 (Sotomayor, J., concurring) (discussing potential for abuse of unfettered use of surveillance technology).
principle as “fruit of the poisonous tree,”20 in the interest of public safety and government resources.21

II. History

A. Massachusetts Supreme Judicial Court

The Massachusetts Supreme Judicial Court dealt with the surreptitious installation of a GPS tracker on an automobile as a matter of first impression in 2009, analyzing the issue separately under the Massachusetts Declaration of Rights22 and the U.S. Constitution.23 Police obtained a valid warrant beforehand and the court determined police complied with constitutional requirements.24 The Court held the police’s attachment and use of the GPS device constituted a seizure under the Massachusetts constitution.25

20 JOSEPH A. GRASSO & CHRISTINE M. MCAVOY, SUPPRESSION MATTERS UNDER MASSACHUSETTS LAW § 20-2 (LexisNexis 2013) (discussing fruit of the poisonous tree doctrine as excluding from criminal trials any evidence procured by violating constitutional principles).
22 See Mass. Const. pt. 1, art. XIV (establishing the right of freedom from unreasonable searches and seizures).
23 See Connolly, 913 N.E.2d at 372 (outlining Fourth Amendment case law, but holding under Article 14 of the Massachusetts Declaration of Rights).
24 See id. at 361-62 (describing how the police procured a search warrant to attach a GPS device to defendant for fifteen days after observing him engaged in drug transactions).
25 See id. at 369 (ruling that tracking of the GPS data by the police constituted use and control of the defendant’s vehicle and interfered with his right to exclude others from his vehicle in violation of Article 14 of the Massachusetts Declaration of Rights); see also Adam R. Waldstein, Looking Beyond Jones: GPS Surveillance in
The SJC cites the Stevens partial dissent in *United States v. Karo*, which only deals with seizure based on attaching a tracking device to the automobile. Should *Connolly* be understood therefore as providing no guidance where there is no attachment of a device, as where GPS is already installed in a cellphone, smartphone or vehicle?

**B. U.S. Supreme Court**

Past cases have analyzed the use of trackers hidden in items that police anticipated would enter a defendant’s custody without his knowledge. The court held that constitutionally it was enough that the party with possession of the item, prior to the defendant, had voluntarily allowed the tracker to be hidden inside it. The defendant could not claim an expectation of privacy about his subsequently traced movements leading to his arrest.

*Massachusetts, MASSACHUSETTS BAR ASSOCIATION, April 2012, archived at www.perma.cc/0hsH7ugPyVt (explicating the difference between Federal and Massachusetts laws covering data procurement).*

Federal law (unlike Massachusetts, where there is no analogous statute) explicitly prohibits the use of such data under the Stored Communications Act, 18 U.S.C. Sections 2701-2712. Service providers may only disclose the contents of a stored electronic communication pursuant to a warrant, if the information deals with an emergency involving danger of death or serious injury (building in an exigent circumstances exception), or if the service provider believes it “pertain[s] to the commission of a crime.” This last exception should not be seen to eviscerate the rule; location data on its face without more should not be seen as evidence of a crime…. Article 14 provides individuals more substantive protection than under the U.S. Constitution, and provides a greater expectation of privacy.

*Id.* (citations omitted).

20 See *Connolly*, 913 N.E.2d at 369 (citing *Karo* dissent stating that tracking of beeper constituted seizure).


28 See *Knotts*, 460 U.S. at 278 (allowing tracking by device attached to effect with prior owner’s consent).

29 See *id.* at 282 (holding no reasonable expectation of privacy in public area).
In past cases discussed below, the Supreme Court held it was not unconstitutional for law enforcement to place a tracking device on a defendant’s effect, some property of which he takes possession, to track him without his knowledge. In *United States v. Knotts*, a “beeper” was placed in a container of chloroform and used to track its location. The beeper was placed in the container with the consent of the then-owner before it came into the defendant’s possession. The Court held the defendant had no reasonable expectation of privacy in his movements tracked principally in public streets.

In *Karo*, the Federal Drug Enforcement Agency (DEA) acted on a tip that the defendant was buying canisters of ether as part of a drug smuggling operation. With the seller’s consent, agents placed an electronic device in a canister included in the sale to the defendant. They followed signals received from the device and tracked him from various locations including his private home. The Court held installing the beeper in the canister was not a seizure because the informant consented to the beeper being hidden among the

---

30 See id. at 277 (outlining whether concealing beeper violated Fourth Amendment); See also *Karo*, 468 U.S. at 718 (permitting surveillance where tracker was attached with prior consent and tracked while in public areas).
31 See *Knotts*, 460 U.S. at 277 (describing the method of concealment police used to track chemicals transported by codefendants en route to defendant later charged with conspiracy to manufacture controlled substances).
32 See id. at 278 (noting officers received permission from chemical company to install beeper having observed one of the codefendants purchasing chemicals from it).
33 See id. at 281 (holding no reasonable expectation of privacy by the defendant under the circumstances).
34 See 468 U.S. at 706 (holding no search or seizure occurred when beeper was installed in a container while it belonged to a third party with that original owner’s consent and the defendant who later bought it had no knowledge thereof).
35 See id. at 708 (stating that DEA agent learned respondents ordered gallons of ether from government informant to be used to extract cocaine from goods imported into the U.S.).
36 See id. (explaining that police obtained court order authorizing installation and monitoring of beeper in a can of ether which they substituted for one of the ten sold to defendant by informant with informant’s consent and painted all ten uniformly).
37 See id. at 708-10 (explaining the police followed the beeper’s signals as it was moved between storage facilities).
canisters later sold to the defendant.\textsuperscript{38} The Court further concluded the transfer of the canister bearing the hidden beeper to the defendant neither infringed a privacy interest nor constituted a seizure.\textsuperscript{39} The government could not, however, monitor the beeper without a warrant and without probable cause or reasonable suspicion in private residences.\textsuperscript{40}

In \textit{Katz v. United States},\textsuperscript{41} government agents wiretapped and recorded the defendant while he was making a call in a phone booth.\textsuperscript{42} The Court determined this conduct violated the defendant’s reasonable expectation of privacy.\textsuperscript{43} Justice Harlan’s concurrence reiterated a test for determining whether a defendant has a reasonable expectation of privacy: whether the individual exhibited an actual expectation of privacy, a subjective inquiry, and secondly, whether society would recognize that expectation as reasonable, an objective inquiry.\textsuperscript{44} Justice Stewart stressed the importance of antecedent justification of law enforcement’s actions to Fourth Amendment protections and a procedural requirement for the electronic surveillance in this case, rather than justifications after the fact.\textsuperscript{45}

\textsuperscript{38} See id. at 711-12 (justifying the concealed beeper based on the seller’s consent to use it in the canister while it belonged to him).

\textsuperscript{39} See id. at 712-13 (determining no meaningful interference with defendant’s possessory interest occurred).

\textsuperscript{40} See \textit{Karo} at 717-19 (rejecting “Government’s contention that it should be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper wherever it goes is likely to produce evidence of criminal activity”).

\textsuperscript{41} 389 U.S. 347 (1967).

\textsuperscript{42} See id. at 348 (describing the mode of police surveillance by eavesdropping on the calls petitioner placed in a public telephone booth).

\textsuperscript{43} See id. at 351, 358 (stating “the Fourth Amendment protects people, not places” and suggesting that a person has a reasonable expectation of privacy in a telephone booth).

\textsuperscript{44} See id. at 361 (Harlan, J., concurring) (articulating a twofold requirement for Fourth Amendment protections).

\textsuperscript{45} See id. at 359 (stating that government agents “ignored the procedure of antecedent justification that is central to the Fourth Amendment”).
In *United States v. Davis*, the Supreme Court stated that where police conduct exhibits ‘‘deliberate,’ ‘reckless,’ or ‘grossly negligent’ disregard for Fourth Amendment rights’’ during surveillance, it will exclude the evidence gathered by the offending techniques to deter future violations of the Fourth Amendment. However, *Davis* recognized an exception to this exclusionary rule for law enforcement acting on a reasonable, good faith belief that they were acting consistent with legal authority by relying on a search warrant, later found to be legally defective. Justice Breyer expressed concern in his dissent that the ‘‘good faith’ exception will swallow the exclusionary rule.’’

**III. Facts**

*A. GPS*

In *Jones* the Supreme Court held attaching a GPS tracker to a defendant’s vehicle was a search, but did not decide on whether using data from a GPS device already embedded in defendant’s property such as in a cell phone would be implicated under the Fourth Amendment. A warrant issued to law enforcement to install a GPS tracker on the defendant’s vehicle within ten days in the District of Columbia on suspicion of narcotics trafficking. Police attached the device to the undercarriage of the defendant’s wife’s vehicle outside the scope of the warrant by doing so on the eleventh day, a day after the warrant expired. The GPS was attached outside the warrant’s jurisdiction since it was done while the vehicle was in Maryland rather than the District of Columbia. Law enforcement then used the

---

47 *Id.* at 2427-28 (discussing the strong deterrent value of excluding evidence obtained with reckless disregard for the Fourth Amendment).
48 *See id.* at 2428-29 (citing the police’s lack of culpability as triggering exception to exclusionary rule and making evidence admissible).
49 *Id.* at 2439 (Breyer, J., dissenting).
50 *See Jones*, 132 S.Ct. at 949, 954 (holding Government’s attachment of GPS to defendant’s vehicle and using it to track his movements constituted a search). Justice Sotomayor’s concurrence raised concerns of duration of surveillance and types of offenses for which such surveillance may be unconstitutional. *See id.* at 954-57 (Sotomayor, J., concurring).
51 *See id.* at 948 (discussing the circumstances under which GPS was used).
52 *See id.* (describing the facts of Jones).
53 *See id.* (describing how the use of GPS was unauthorized by the warrant issued).
GPS to track his movements for about four weeks as he went through public streets, generating large amounts of locational data leading to the defendant’s arrest.\(^{54}\)

The concurring opinions raise additional issues not decided by the majority where attaching an external device would not be required for the intended surveillance.\(^ {55}\) In her concurring opinion, Justice Sotomayor raises the proposition that the Court may need to reconsider the premise that individuals have no reasonable expectation of privacy in information voluntarily disclosed to third parties.\(^ {56}\) She further expresses concern about this technology’s potential chilling effect on associational freedoms and the risk of abuse if it is unregulated.\(^ {57}\) Justice Alito’s concurring opinion expresses concern that the majority provides little guidance on the issue of GPS technology where no physical intrusion is necessary as with GPS-

\[^{54}\text{See id. (continuing to outline the facts of Jones).}\]
\[^{55}\text{See id. (Sotomayor, J., concurring) (expressing concern over unanswered questions).}\]
\[^{56}\text{See Jones, 132 S.Ct. at 948 (raising concerns about the incongruence of the third party doctrine with the digital age).}\]
\[^{57}\text{See id. at 956 (Sotomayor, J., concurring) (stating “[a]wareness that the Government may be watching chills associational and expressive freedoms” and “the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.”).}\]

---

equipped smartphones, and emphasizes scrutiny of the duration of surveillance without offering a specific limit.58 Some suggest the Roberts court has eroded the exclusionary rule, not raised in Jones, and allowed law enforcement to reasonably rely on the existing state of the law where no binding precedent exists in a jurisdiction’s circuit as a means for admitting evidence from GPS surveillance.59 The exclusionary rule, to be discussed further below, continues to play a role in cases where investigations were conducted before the Jones decision came down.60

In United States v. Baez,61 a Massachusetts federal court addressed whether evidence gathered by federal agents without a warrant by attaching a GPS device to a defendant’s vehicle while on a public road in front of his apartment should be suppressed.62 Two mid-2009 fires in Boston two months apart were determined to be acts of arson using gasoline, piles of burnt tires and clothing, and led to the investigation of a dark Chevrolet Caprice with silver trim, a light-colored steering wheel cover, and a silver emblem by the driver-side windshield, which was recorded on surveillance cameras driving away from each scene moments before each fire began.63 Though acknowledging that Jones held such a technique constituted a search under the Fourth Amendment, the court did not suppress data used to track the defendant because law enforcement officers at the time had a “good faith basis to rely upon a substantial consensus among prece-

58 See id. at 962-63 (Alito, J., concurring) (acknowledging newer technology may require revisiting Fourth Amendment approaches); see also Daniel K. Gelb, Defending a Criminal Case From the Ground to the Cloud, 27 CRIM. JUST. 28, 57 (2012) (discussing the practical concerns of discovery of electronically stored information with respect to smartphones which are essentially computers that demand a greater privacy interest).
59 See Tracey Maclin & Jennifer Rader, No More Chipping Away: The Roberts Court Uses An Axe To Take Out The Fourth Amendment Exclusionary Rule, 81 MISS. L.J. 1183, 1227 (2012) (predicting that the Court is reserving application of the exclusionary rule only where police conduct is found egregious, rendering it ineffective).
60 See case cited infra notes 67-68 and accompanying text (discussing the application of the exclusionary rule).
62 See id. at 297 (applying Davis over Jones in declining to suppress warrantless GPS-acquired locational data).
63 See id. at 289-91 (describing fires prompting investigation).
dential courts.” The court pointed to the three circuit courts that concluded no warrant was required under the Fourth Amendment for monitoring a GPS tracking device on a car in public. The agents stopped using the GPS tracking device on the defendant’s car and arrested him three days after United States v. Maynard created a circuit split by holding that GPS tracking was a search in the D.C. Circuit. The Baez court decided that the investigators acted in good faith given the “vast weight” of persuasive authority pre-dating Jones at the time they used the GPS tracker.

In applying Davis, the Baez court reiterated the precedent that exclusion should be a last resort, triggered where the benefits of suppressing evidence as a deterrent to future Fourth Amendment violations outweigh its costs, which turns on the “culpability of law en-

---

64 See id. at 289, 297-98 (justifying admission of the evidence based on good faith reliance on precedent at the time).
65 See id. at 292-93 (pointing to the three circuit courts that concluded no warrant was required under the Fourth Amendment); see also United States v. Marquez, 605 F.3d 604, 609-10 (8th Cir. 2010) (holding defendant lacks reasonable expectation of privacy while driving on public street). Furthermore, the Marquez court found that the attachment of a GPS device to the defendant’s vehicle for a reasonable time in absence of warrant to be constitutional. Id. See also United States v. Pineda-Moreno, 591 F.3d 1212, 1216-17 (9th Cir. 2010) cert. granted, judgment vacated, 132 S. Ct. 1533 (2012) (holding no reasonable expectation of privacy on public street or in driveway or curtilage of residence, and attaching GPS device to car was not a search); United States v. Garcia, 474 F.3d 994, 997-98 (7th Cir. 2007) (holding no search in attaching external GPS device to vehicle). Pineda-Moreno was granted certiorari and was vacated and remanded to the 9th Circuit on February 21, 2012, in light of Jones. See United States v. Pineda-Moreno, 688 F.3d 1087, 1088 (9th Cir. 2012) cert. denied, 133 S. Ct. 994 (2013) (applying post-Jones analysis to determine whether exclusionary rule applies to GPS placed on underside of car by law enforcement).
66 See Baez, 878 F. Supp. 2d at 293 (noting the timing of the D.C. Circuit’s holding); United States v. Maynard, 615 F.3d 544, 555-56 (D.C. Cir. 2010) (holding continuous, warrantless GPS-surveillance over four months was a Fourth Amendment search). Maynard emphasized the duration of surveillance and the more intimate information wrought by allowing long stretches of continuous surveillance, and revealing patterns of behavior that would not be perceptible by an individual member of the public. Id. at 562-63 (discussing the more revealing picture apparent in prolonged periods of surveillance).
67 See Baez, 878 F. Supp. 2d at 293-94 (recalling the Davis court’s approach to the exclusionary rule).
The court decided that the cost-benefit analysis weighs heavily in favor of allowing officers to act on good faith reliance rather than making them unduly cautious in their investigations because the value to public safety far outweighs nominal deterrence value.

Other federal courts have applied the exclusionary rule to GPS evidence with a similar approach to that in Baez. The approach is criticized, however, by the court in United States v. Robinson, which notes that three other districts take the contrary view that “Davis does not apply in absence of binding precedent from the Circuit and that permitting officers to rely on non-binding precedent would allow [them] to pick and choose what law to follow, and would not properly serve the deterrent function of the exclusionary rule.”

B. Cell Phone Data

68 See id. at 294 (indicating that the deterrence value of excluding evidence is higher the more deliberate or recklessly law enforcement disregards Fourth Amendment rights in a given case); see also Herring v. U.S., 555 U.S. 135, 141 (2009) (articulating the costs of excluding evidence illegally obtained by law enforcement as “letting guilty and possibly dangerous defendants go free—something that ‘offends basic concepts of the criminal justice system.’”).

69 See Baez., 878 F. Supp. 2d at 297 (advancing an approach that provides more leeway for law enforcement based on the conclusion that there would be no meaningful deterrence value in discouraging good faith reliance).


72 See id. at 783 (warning that the exclusionary rule and case law against retroactive application of a new rule is undermined by allowing law enforcement to select which laws to apply when there is no binding precedent).
Lower federal courts have found seizure of historical cell site data to be a Fourth Amendment search.\textsuperscript{73} By contrast, more recently in \textit{United States v. Skinner},\textsuperscript{74} the Sixth Circuit held a defendant did not have a reasonable expectation of privacy in the GPS data emitted by his pay-as-you-go cell phone.\textsuperscript{75} In \textit{In re United States}, the U.S. District Court for the Eastern District of New York held that a court order for cell-site data may be granted to the government only if it “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.”\textsuperscript{76} It further stated that this is a lower standard than the probable cause standard required for a search warrant.\textsuperscript{77} The issue’s salience grows as police requests

\textsuperscript{73} See \textit{In re United States}, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) (holding warrant was required for court order for cell-site location records spanning about 113 days from cell carriers). The request was made pursuant to 18 U.S.C. § 2703(c)(1), (d) (2009) (the “Stored Communications Act” or “SCA”). See \textit{id.} at 114; see also \textit{In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority}, 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) [hereinafter \textit{Pen Register and Trap/Trace}] (denying government’s request for prospective cell site data without probable cause showing).

\textsuperscript{74} 690 F.3d 772 (6th Cir. 2012) \textit{cert. denied}, 133 S. Ct. 2851 (2013).

\textsuperscript{75} See \textit{id.} at 775, 777 (holding defendant had no reasonable expectation of privacy in cell phone’s GPS data). In a concurring opinion however, Judge Donald contends that society recognizes “a legitimate expectation of privacy in the GPS data emitted from any cell phone.” See \textit{id.} at 786 (Donald, J., concurring). See also H. MARSHALL HARRETT, MICHAEL W. BAILIE, ED HAGEN, NATHAN JUDISH, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 151 (2009), archived at \textit{www.perma.cc/0kcEZsjDFcy} (defining Pen Register and Trap and Trace Device and relevant statutes in electronic surveillance in communications networks):

Real-time electronic surveillance in federal criminal investigations is governed primarily by two statutes. The first is the federal Wiretap Act, 18 U.S.C. §§ 2510-2522, first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (and generally known as “Title III”). The second statute is the Pen Registers and Trap and Trace Devices chapter of Title 18 (“the Pen/Trap statute”), 18 U.S.C. §§ 3121-3127, first passed as part of the Electronic Communications Privacy Act of 1986. Failure to comply with these statutes may result in civil and criminal liability, and in the case of Title III, may also result in suppression of evidence.).

\textit{Id.}

\textsuperscript{76} 809 F. Supp. 2d at 115.

\textsuperscript{77} See \textit{id.} (noting the standard required for obtaining the records sought).
to cell carriers increase as a means for pursuing investigations.  

Other Massachusetts courts have supported the approach in *In re Application*.  

The U.S. District Court of Massachusetts held cell phone owners did not have a reasonable expectation of privacy in historical cell site information. The court reasoned that the holding in *Jones* was irrelevant to the court order the government sought to obtain regarding the historical cell site information because *Jones* did not involve attachment of a device to an individual’s real or personal property. The court did not require a showing of probable cause before issuing an Order pursuant to section 2703 (d) of the Stored Communications Act, and so authorized the acquisition of records containing historical cell site information and took the guarded approach of the Supreme Court in *City of Ontario, Cal. v. Quon*, because the “judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has be-

---


80 See Disclose Subscriber and Cell Site Info, 849 F.Supp.2d at 177-79 (agreeing with its 2007 holding and a more recent holding in Maryland federal court to not require probable cause because there was no reasonable expectation of privacy in cell site records).

81 See id. at 178 (deeming holding of *Jones* irrelevant because no physical trespass is involved in obtaining historical cell site information); see also United States v. Jones, 908 F.Supp.2d 203 (2012) (citing Disclose Subscriber and Cell Site Info later granted certiorari by the U.S. Supreme Court in *Jones*, which addressed whether the Fourth Amendment is triggered even in the absence of attaching an external device and followed United States v. Graham, 846 F.Supp.2d 384 (D. Md. 2012)).

come clear.” The court chose to remain in line with the Massachusetts federal court’s 2007 decision not requiring probable cause for authorizing the acquisition of records containing historical cell site information until the First Circuit or Supreme Court rule otherwise or Congress enacts new legislation on the issue.

In United States v. Rose, a Massachusetts federal court heard a case on the order of a defendant’s motion for disclosure of GPS information in light of Jones. The defendant requested that the government turn over records of its surveillance and disclosure of internal memos of the Department of Justice or FBI informing agents that no warrant would be required to attach a GPS locator to his car because he claimed that it contained potentially exculpatory information, which could reveal a Fourth Amendment violation and therefore guard against the data being used against him. The defendant’s claim was not enough to compel disclosure, and the court only required the government to produce an affidavit in response to those discovery requests containing “information regarding: (1) the tracking radius of the GPS devices; and (2) how the devices were used in conjunction with surveillance in this investigation” and it denied his other requests. Its rationale, taken from U.S. v. Davis, was that no personal constitutional right serves to exclude such information and that the exclusionary rule was intended to deter future Fourth Amendment violations by law enforcement which does not apply.

83 See Disclose Subscriber and Cell Site Info, 849 F.Supp.2d at 179 (quoting Quon, 130 S.Ct. at 2629) (leaving Fourth Amendment questions unanswered where no GPS attachment is required); see also 18 U.S.C. § 2703(d) (describing the requirements to issue an order of disclosure); see also Quon, supra note 82 at 2629-30 (declining to elaborate anticipatorily on the Fourth Amendment implications of rising technology).
84 See Disclose Subscriber and Cell Site Info, 849 F.Supp.2d at 179 (following Massachusetts’s federal court decision regarding probable cause showing for obtaining historical cell site information).
86 See id. at *1 (reviewing “request for discovery of GPS data in light of…United States v. Jones”) (citation omitted).
87 See id. at *1-*5 (outlining defendant’s requests from the government regarding surveillance and warrant requirement).
88 See id. at *4 (requiring affidavit rather than full disclosure by government).
where they acted in reasonable reliance on binding appellate precedent. 89

The third-party doctrine has been interpreted to preclude a party from claiming a reasonable expectation of privacy in its records when it has voluntarily turned them over to a third party. 90 Law enforcement has taken other innovative measures to intercept cell site data through cell-site simulators, or “stingray” technology, but the details have been held to be privileged information. 91 The DOJ manual for electronic surveillance notes cases that have recognized historical cell-site information as within the scope of §2703(c)(1) of the Stored Communications Act. 92 The electronic surveillance manual discusses how amendments to §2703 enacted in the USA PATRIOT Act of 2001 have allowed closer domestic surveillance and the ability to acquire cell phone records by subpoena or a lower required showing for obtaining a warrant. 93 More recently, in 2009, the DOJ has

89 See id. at *5 (applying Davis to deny Andrews’ discovery request for government documents). Andrews anticipated raising a defense that law enforcement acted in good faith reliance on existing precedent. See id.
90 See United States v. Graham, 846 F. Supp. 2d 384, 400-403 (D. Md. 2012) (holding the cell phone user does not have reasonable expectation of privacy in historical cell site information, thereby rejecting that a warrant should be required under the Stored Communications Acts); see also Kerr, supra note 16, at 588-90 (discussing third party doctrine as a consent doctrine).
92 See U.S. Dep’t of Justice, supra note 6, at 44 (discussing how court orders under 2703(d) are an appropriate way to prospectively get cell phone location records).
93 See U.S. Dep’t of Justice, supra note 6, at 45, 48 (providing guidance on obtaining records or other information from customer or subscriber); see also USA Patriot Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 290 (2001) (broadening coverage of 18 U.S.C. § 3127 pen register statute under Title II Enhanced Surveillance Procedures); David Johnston & Eric Lipton, U.S. Report to Fault
made a third edition of their search and seizure manual on electronic evidence in criminal investigations. Congress has proposed legislation such as the GPS Act and ECPA 2.0 Act of 2012 that would require law enforcement to produce a warrant before cell phone providers could give them their customers’ cell phone locational records, referred them to committees, but did not enact them.

IV. Analysis

Connolly remains the SJC’s last case regarding GPS surveillance, and the question remains of what is required of law enforcement where the GPS is already in the targeted party’s phone or vehicle. As a result, Massachusetts courts have looked to other jurisdictions for guidance and have applied the third party doctrine and the good faith exception while precedent remains unclear to allow law enforcement to obtain GPS data and cell phone records from providers. At some point, clearer policy will need to be prescribed,

F.B.I. on Subpoenas, N.Y. TIMES, Mar. 7, 2007, archived at www.perma.cc/04UbFBEgXuj (discussing the use of “national security letters” under the USA Patriot Act since 2001 which in effect act as administrative subpoenas for phone, business, and financial records without prior judicial approval).

94 See JARRETT, ET. AL., supra note 75, at 151 (providing prosecutors and law enforcement guidance from the DOJ on search and seizure of electronic evidence in criminal investigations and noting historical cell-site information falls within scope of § 2703(c)(1) of the SCA as recognized in Massachusetts cases).

95 See Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. § 2602 (2011) [hereinafter GPS Act], archived at www.perma.cc/0h7ZwJYvVha (proposing legislation that would prohibit acquiring geolocation information of a person for protective activities or law enforcement or intelligence purposes except pursuant to a warrant issued under the Federal Rules of Criminal Procedure or the Foreign Intelligence Surveillance Act as summarized by the Congressional Research Service).

96 See ECPA 2.0 Act of 2012, H. R. 6529, 112th Cong. § 2602 (2012) (introducing bill requiring warrants for disclosures to the government by communications-related service providers of certain information relating to communications).

97 See GPS Act, S. 1212 (calling for warrants to obtain geolocation information in proposed legislation that went to committee); ECPA 2.0 Act of 2012, H. R. 6529, 112th Cong. § 2602 (2012) (proposing warrant requirement for communications-related records in bill that went to committee).

98 See Connolly, 913 N.E.2d at 360, 367, 372 (applying Massachusetts law to GPS surveillance via a device attached by the police).

99 See Quon, 560 U.S. 746, 130 S.Ct.at 2629-30 (declining to overturn precedent which did not require probable cause).
whether by the legislature or through common law. A holistic approach will need to address potential changes in the third party doctrine to better reflect evolving expectations of privacy with respect to electronic devices with embedded GPS. New policies might incorporate minimizing retention of cell phone data by carriers, toughen limitations on retention of locational data information, and move to minimize the storage towards the extent required only for the consumer to use the GPS function.

A better rule on GPS surveillance should incorporate a stricter application of the exclusionary rule for warrantless surveillance and address the concerns about the more invasive nature of continuous, extended periods of surveillance without a warrant expressed under the Maynard approach, sometimes referred to as the mosaic theory. Allowing this type of surveillance without a warrant flouts the purpose of warrant requirements, eroding the preservation of Fourth Amendment rights by allowing too much discretion by law enforcement. A clearer standard, however, should not be intended to hamper law enforcement’s important efforts to keep the public safe through anticipating criminal acts where there is probable cause to support a warrant.

The Baez court could have used the case to bolster the Fourth Amendment protection of requiring a warrant before attaching a GPS device. Instead the court applied the good-faith exception based

100 See Disclose Subscriber and Cell Site Info, 849 F.Supp.2d at 178-79 (discussing concerns beyond those answered by Jones, and the U.S. District Court of Massachusetts’s decision to not require probable cause for police to get cell site data from providers).
101 See Crump, supra note 15 (addressing third party doctrine and its shortcomings).
102 See ELECTRONIC FRONTIER FOUNDATION, supra note 17 (noting lack of policy requiring specific retention limits for records).
103 See Maynard, 615 F.3d at 555 (discussing how continuous GPS surveillance over extended periods yields more sensitive information than intermittent GPS tracking).
104 See Baez, 878 F.Supp.2d at 290-92 (discussing how police caught arsonist using tracking device after he caused two fires).
105 See Robinson, 903 F.Supp.2d at 778-79 (declining to exclude evidence gathered using surreptitious GPS tracking based on good faith reliance argument by law enforcement).
on pre-Jones cases. It criticized a regime that would require law enforcement to get court permission before taking any steps as seeming “unnecessarily unwieldy—and potentially enervating to timely police action in other settings—when as here a substantial consensus among precedential courts provides a good faith basis for the investigatory initiative law enforcement agents seek to pursue.” While the Baez holding follows precedent in other circuit decisions, the larger problem is that liberally applying a good faith exception potentially renders the exclusionary rule meaningless.

Looking to older Supreme Court cases, the Katz approach is insufficient in cases of smartphone GPS data. Under Katz, law enforcement would not readily be able to determine whether their actions would be constitutional until after the fact since the location of their target would be unknown to them until after they obtain the locational data. This data would show whether the targeted party was at their private dwelling where they would have a reasonable expectation of privacy as opposed to if they were on a public road where they would not. On the related issue of historical cell site

106 See Baez, 878 F.Supp.2d at 297 (applying good faith exception to exclusionary rule).
107 Baez, 878 F.Supp.2d at 297.
108 See id. at 292-93; see also Marquez, 605 F.3d at 609-10 (holding defendant lacks reasonable expectation of privacy while driving on public street and allowing non-invasive GPS device to be attached to his vehicle for reasonable period without warrant where police had reasonable suspicion vehicle was transporting drugs); Pineda-Moreno, 591 F.3d at 1216-17 (holding no reasonable expectation of privacy on public street or in driveway or curtilage of residence, and attaching GPS device to car was not a search); Garcia, 474 F.3d at 997-98 (holding no search or seizure in attaching external GPS device to vehicle).
109 See Davis, 131 S. Ct. at 2439 (Breyer, J., dissenting) (expressing concern that frequent use of the good faith exception could swallow the exclusionary rule).
110 See Jones, 132 S. Ct. at 962 (Alito, J., concurring) (noting the difficulties of applying the reasonable expectation of privacy test in part because expectations likely change with the technology).
111 See Katz, 389 U.S. at 359 (stating the importance of antecedent justification as a Fourth Amendment requirement for electronic surveillance in Katz); see also Mark, infra note 112, at 38 (noting Katz approach allows only after-the-fact determination of reasonable expectation of privacy).
112 See Monica Mark, GPS Tracking, Smartphones, and the Inadequacy of Jones and Katz, 27 CRIM. JUST. 36, 38 (2013) (noting that only after police acquire the
information as another means of acquiring locational data, the U.S. District Court of Massachusetts did not require law enforcement to show probable cause, echoing another court’s reasoning that the “judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”\textsuperscript{113} This explanation is unsatisfying in that it does not elaborate on its rationale, but is understandable as even the U.S. Supreme Court has not yet suggested parameters for tracking embedded GPS devices.\textsuperscript{114} The Massachusetts federal court has opted to leave it to the Supreme Court to take this issue up later.\textsuperscript{115} It is not clear what the court believes would clarify the role of GPS technology in society enough to compel the high courts to toughen the application of warrant requirements, but it seems to say that legislative action is better-suited to reflect that role.\textsuperscript{116} Further, the trend in the last couple of decades towards increasing dissemination of personal information and storing information in the cloud seems to make the “reasonable expectation of privacy” a fluid concept.\textsuperscript{117}

\textsuperscript{113}See Disclose Subscriber and Cell Site Info, 849 F.Supp.2d at 179 (holding cell phone owners did not have reasonable expectation of privacy in historical cell site information); see also Lichtblau, supra note 78 (discussing how technological advances have altered what is legally required to use GPS systems); see also Wyatt, Criminal Action No. 2010-00693, 2012 WL 4815307 at *7 (reasoning an individual’s subjective expectation of privacy in cell site data is recognized as reasonable).

\textsuperscript{114}See Jones, 132 S.Ct. at 954 (declining to set a maximum permissible time for constitutional GPS surveillance).

\textsuperscript{115}See Disclose Subscriber and Cell Site Info, 849 F.Supp.2d at 179 (deferring to earlier federal court holding, higher courts, or legislature).

\textsuperscript{116}See, e.g., id. (concurring with past opinions not requiring probable cause for cell site data disclosure to police until U.S. Supreme Court or legislature require otherwise).

\textsuperscript{117}See Jones, 132 S.Ct. at 957 (Sotomayor, J., concurring) (reflecting on changing technology, and responding to Justice Alito’s statement that technology “continues to shape the average person’s expectations about the privacy of his or her daily movements,” and possible insufficiency of older Fourth Amendment case law to address these changes); id. at 964 (Alito, J., concurring) (stating while legislature is “well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way,” Supreme Court must apply Fourth Amendment jurisprudence where Congress has not reached the issue at bar).
At the moment, prospects for both judicial and legislative action to toughen privacy protections seem dim in terms of both requiring warrants before resorting to GPS tracking and showing probable cause for disclosure of cell phone location records. The courts discussed here seem to leave that task to the legislature, both state and federal, though it is not clear what will spur enough political will or incentive to set preemptive safeguards by passing bills that will regulate surveillance measures expanded post-9/11. The GPS Act of 2011 and ECPA 2.0 Act of 2012 are two bills introduced that would support such privacy protections as requiring warrants before communications providers can disclose electronic communications records to government agents, but the bills have remained stagnant.

Their introduction at least signals that members of Congress recognize GPS and cell-phone privacy issues are significant to their constituents, but the chances that the bills would be codified in some form soon appear remote as even other state jurisdictions that are

---

118 See Jones, 132 S.Ct. at 964 (Alito, J., concurring) (leaving the task of a new approach to the legislature). Proposed legislation outlining procurement of warrants for obtaining locational and communications data have found themselves hung up in committee, unlikely to be passed. See GPS Act, S. 1212 (proposing warrants be required to obtain geolocational data); H. R. 6529 § 2602 (proposing warrant be required to obtain communications-related records in bill that went to committee). See U.S. DEP’T OF JUSTICE, supra note 6, at 45 (recounting how the USA Patriot Act expanded definitions of surveillance equipment under the Pen/Trap Statute and further discussing a related House Judiciary Committee Report).

119 See sources cited supra notes 95-96 (discussing the bills that would require warrants for electronic surveillance). The GPS Act was read twice and referred to the Committee on the Judiciary on June 15, 2011. The ECPA 2.0 Act was referred to the House subcommittee on Crime, Terrorism, and Homeland Security on October 3, 2012. See ECPA 2.0 Act of 2012, H. R. 6529, 112th Cong. § 2602 (2012). For some context from another jurisdiction, the California governor recently vetoed a bill introduced by Senator Mark Leno (D-San Francisco), which would require a warrant before law enforcement officers can obtain location information generated by cell phones, tablet computers, and automobile navigation systems, or other electronic devices. See James Temple, Governor Should Sign Cell Phone Privacy Bill, SFGATE, Jan. 20, 2013, archived at www.perma.cc/0ZoS4G7Tst; Letter from Edmund Brown, Governor, State of Cal., to Members of Cal. State Senate (Sep. 30, 2012) (on file with California State Senate), archived at www.perma.cc/0ZGwfCrXp51 (expressing the California governor’s rejection of the bill proposing a warrant requirement before law enforcement can obtain cell phone records from phone providers).
otherwise quite liberal could not secure a codified warrant requirement for law enforcement to reach electronic locational data.121

Could local districts in states across the country turn the issue of third party doctrine as applied to their expectation of privacy when it comes to their phone records with their cell phone providers into ballot questions? A ballot initiative might ask, for example, whether you as a phone customer expect police to produce a warrant for your historical cell site data or any records of your service usage before the provider can release them. More such empirical data might be useful to support what courts assert on behalf of the “reasonable” person.122 A court could reasonably argue that such data and the studies required to get it are for the legislature; that the legislature has the resources and institutional competence to have hearings and acquire that data.123 If the onus should ultimately fall on the legislature, the courts could help protect the Fourth Amendment by more rigorously applying the exclusionary sanction, suppressing illegally-acquired evidence in violation of the Fourth Amendment, with sparing recourse to the “good faith” exception, if it is to be used at all.124 The issues presented are complicated and divisive, so it is difficult to imagine a bill passing that would codify meaningful changes to privacy protections while providing clear guidance to law enforcement from the federal level.125

While some cases have upheld a probable cause requirement, it appears that in Massachusetts cases, as the matters reach higher

---

121 See Temple, supra note 120, (covering the veto of bill proposing warrant requirement for electronic communications data retrieval by law enforcement).
123 See Jones, 132 S.Ct at 964 (Alito, J., concurring) (stating “the best solution to privacy concerns may be legislative” and that “a legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way”).
124 See Davis, 131 S.Ct. at 2439 (expressing concern that overuse of the good faith exception to the exclusionary rule could swallow the rule itself).
125 See GPS Act, S. 1212 (ending with referral to committee); ECPA 2.0 Act of 2012, H. R. 6529, 112th Cong. § 2602 (2012) (ending with referral to committee).
courts, opponents of warrantlessly acquired location data face a difficult burden for suppression since government procedures in procuring that information are given special protection.\textsuperscript{126} The holding in In re Application of the United States for Pen Register, denying the government’s request for prospective cell site data without a probable cause showing, and its later application in Commonwealth v. Wyatt maintain the probable cause requirement for prospective cell site data.\textsuperscript{127} In Rose, a higher court decision, a defendant could not get access to the full government records of its surveillance of his whereabouts by claiming that such records potentially contained exculpatory information in that it could be protected under the Fourth Amendment and therefore be suppressed.\textsuperscript{128} The court acknowledges that the government is primarily responsible for how much it decides to give up in discovery and that such a decision is final unless it is later found that exculpatory information was not disclosed.\textsuperscript{129} The holding makes clear that speculation that exculpatory evidence is in the records is not enough to compel the government to disclose.\textsuperscript{130} The affidavit required of the government instead seems to leave it with enough leeway to protect its records and guard against potential Fourth Amendment violations if any in the surveillance it conducted.\textsuperscript{131} Perhaps a better argument might have helped; the defense would have needed to show that the government had no way of ac-

\textsuperscript{126} See Rose, Criminal No. 11-10062-NMG, 2012 WL 1720307, at *4 (recognizing government interest in confidentiality of its surveillance methods, requiring government only to produce affidavit stating tracking radius of its GPS device and how it was used to track the targeted party rather than full disclosure).

\textsuperscript{127} See Pen Register and Trap/Trace, 396 F.Supp.2d at 756-57 (denying government’s request for prospective cell site data because location information was not voluntarily conveyed in user’s records and a warrant was required for the prolonged surveillance the records constitute under Maynard); see also Wyatt, Criminal Action No. 2010-00693, 2012 WL 4815307 at *6-*7 (suppressing CSLI records and recognizing an objectively reasonable expectation of privacy in them).

\textsuperscript{128} See Rose, Criminal No. 11-10062-NMG, 2012 WL 1720307, at *6 (holding that a defendant must make some showing that the material in question could contain favorable, material evidence). The showing cannot be based on speculation. Id.

\textsuperscript{129} See id. (citing Pa. v. Ritchie, 480 U.S. 39, 59-60 (1987) in holding that the government can decide how much to disclose to the defendant).

\textsuperscript{130} See id. (holding defendant could not compel government disclosure based on mere speculation).

\textsuperscript{131} See id. at *4 (requiring limited disclosure of government’s GPS use for defendant’s discovery request).
quiring data without acting in bad faith and violating the Fourth Amendment. The court does not address the issues where no GPS attachment is required.

At the federal level, In re Application of U.S. for Order Pursuant to Title 18, U.S.C. §2703(D) to Disclose Subscriber Info. and Cell Site Info. seems like a missed opportunity for the federal court to have created precedent to require a probable cause showing before the government can access records containing historical cell site information. Perhaps understandably it chose a prudent course in following the existing precedent. The court opted out of setting more protective precedent, instead waiting for higher courts to take up the issue in the future. The Supreme Judicial Court could interpret the Massachusetts Constitution as requiring a probable cause showing and therefore providing more protection than has so far been interpreted under the Fourth Amendment, as it did in Connolly with respect to GPS installations.

The higher Massachusetts courts will likely need to address issues of intrinsic GPS, and what showing will be required for the government to get an order to compel disclosure by telecommunic-
tions providers. Case law appears to favor the government continuing to operate based on the good faith exception to the exclusionary rule under *Davis*, to the point where the exception becomes the rule and law enforcement can selectively apply persuasive authority as suggested in *Robinson*.

Clearer policy and new precedent should strike a better balance between privacy protections and equipping law enforcement with a valuable tool, with the understanding that such policy and precedent are likely to lag behind unanticipated applications of technology. Without requiring a warrant supported by probable cause before cell phone locational data can be retrieved from providers, electronic surveillance could be conducted on very sensitive cell phone information about a person’s whereabouts at almost any time, that even visual surveillance could not practically yield. Further weighing against privacy protection is the inconsistent application of the exclusionary rule and frequent resort to the “good faith exception.” There appears to be little to safeguard against random

---

139 *See Leon*, 856 F.Supp.2d at 1195 (denying motion to suppress drugs found when police attached GPS tracker before *Jones* decision); *Oladosu*, 887 F.Supp.2d at 442-43(denying motion to suppress where law enforcement had reasonable good-faith reliance on the state of the law as permitting warrantless-GPS tracking on defendant); *cf. Rose*, 914 Supp.2d at 28, (denying suppression of GPS-derived evidence because police acted in good faith where the First Circuit had not required a warrant for such tracking); *Pitt*, No. 2010-0061, 2012 WL 927095 at *4 (concluding Motion to Suppress allowable as pertaining to warrantless search of CSLI).; *Wyatt*, 30 Mass. L. Rptr. 270, at *1 (Mass. Super. Ct. 2012) (suppressing historical cellular tower site location information the Commonwealth seized pursuant to warrantless search of defendants’ cell phone records).

140 *See Robinson*, 903 F.Supp.2d at 783-84 (determining good faith exception only applied to law enforcement where there was no binding precedent and that police here used a GPS without a warrant but with reasonable suspicion).

141 *See Duggan & Rainie, supra note 7* (showing the increased sophistication of electronics that has led to tension between individual privacy and maintaining a sense of public safety); *see also Jones*, 132 S. Ct. at 956-57 (Sotomayor, J., concurring) (discussing different privacy issues raised by new technology pertaining to third party doctrine, and reasonable expectation of privacy).

142 *See Silva, supra note 9*, (noting the pervasiveness of smartphones and their capacity to tag a user’s movements and generate highly sensitive information as acknowledged by Justice Sotomayor in *Jones*).

143 *See Leon*, 856 F. Supp. 2d at 1195 (denying motion to suppress drugs found when police attached GPS tracker before *Jones* decision); *see also Oladosu*, 887 F. Supp. 2d at 442-43.
screening of cell phone records by law enforcement, which on one hand gives the public a powerful tool for police protection by anticipating or apprehending someone while in the act of committing an inchoate crime, but on the other hand, cellphone screening leaves the public essentially exposed; the public may falsely perceive that they retain some semblance of privacy in their everyday movements.\(^{144}\)

For the moment, perhaps paranoia and uncertainty about the extent of electronic surveillance serves some of the deterrent function against illicit conduct that more transparent jurisprudence and policy otherwise might not.\(^{145}\)

### V. Conclusion

The goal of stricter application of the exclusionary rule, both where warrantless GPS surveillance has occurred and where a warrant is required to obtain historical cell site location data, is to not let guilty defendants go free. However, privacy rights should be given greater recognition and attention in a way that acknowledges that violating privacy is a cost, and actions that violate privacy should be deterred. Further, this does not foreclose relaxation of warrant requirements where law enforcement makes a true showing of exigency.\(^{146}\)

---

\(^{144}\) See \textit{Jones}, 132 S. Ct. at 956-57 (Sotomayor, J., concurring) (discussing the unsettled issues raised by \textit{Jones} majority, setting no time limit on GPS tracking, risk of abuse where powerful surveillance technology is used without regulation, updated appraisal of expectations of privacy); \textit{Baez}, 878 F. Supp. 2d 288, 297-98 (exemplifying benefits some application of the good faith doctrine can have in allowing some leeway to police to deal with time-sensitive emergencies as intercepting an arsonist); \textit{see also} cases cited supra note 143 (listing various cases where good faith exception to exclusionary rule has been applied and a case expressing Supreme Court dissenter’s concern that the exception will overtake the rule).

\(^{145}\) See \textit{Jones} 132 S.Ct. at 956 (Sotomayor, J., concurring) (discussing the chilling effect of awareness that government may be watching).

\(^{146}\) See Waldstein, \textit{supra} note 25 (discussing federal requirement of a showing of exigent circumstances by law enforcement before a service provider can divulge stored communications).
Clarifying the policy and precedent will prevent the loophole of “good faith reliance” or perhaps even something that moves closer to willful blindness from enabling abuse of a valuable tool for surveillance. Courts might at least consider bolstering the procedural protections of requiring probable cause and securing a warrant before surveillance is allowed, or when a phone provider must hand over records. Where legislatures cannot or will not act, courts should not abdicate the judicial tools that remain available to them to protect privacy.