Missouri Law Review

Volume 86 | Issue 4 Article 8

Fall 2022

Giving up the Ghost in the Machine: Emergency Cellphone Tracking Under 18 U.S.C. § 2702(c)(4) Is a Search

Andrew Guinan

NOTE

Giving up the Ghost in the Machine: Emergency Cellphone Tracking Under 18 U.S.C. § 2702(c)(4) Is a Search

Andrew Guinan[*]

I. INTRODUCTION

In the post-September 11th world, our judiciary has been forced to confront the truth that "all free peoples have had to balance the demands of liberty with the demands of security."[1] This tension is not new, and in the past, "we Americans have been able to plant our flag well down the spectrum towards liberty."[2] Recently, however, the interception of electronic communications and other data by local, state, and federal law-enforcement authorities has emerged as a central point in the debate.[3] While many Americans might be willing to endure some degree of intrusion under the threat of national terrorism, the situations that implicate our most deeply held constitutional protections are rarely so clear or dramatic. Should we allow police to gather location data from a suspected robber's cellphone as evidence without a search warrant?[4] What about to

[*]A.B., Dartmouth College, 2010; J.D. Candidate, University of Missouri School of Law, 2022; Associate Member, *Missouri Law Review*, 2020-2021. I am extremely grateful to Associate Dean Paul Litton for his insight, guidance, support, and patience during the writing of this Note. I would also like to thank the members of the *Missouri Law Review*, in particular, Note and Comment Editor Jack Gilkey, for their help in the editing process.

[1] Michael V. Hayden, Lt. Gen., U.S.A.F., Principal Deputy Dir. of Nat'l Intel., *Address to the National Press Club: What American Intelligence & Especially the NSA Have Been Doing to Defend the Nation* (Jan. 23, 2006), https://www.c-span.org/video/?190835-1/intelligence-strategy-terrorism [https://perma.cc/3TXL-6RUP], transcript at https://fas.org/irp/news/2006/01/hayden012306.html [https://perma.cc/5KDV-P28Q] (former director of the National Security Agency ("NSA") discussing NSA activities since September 11, 2001, including the interception of communications, and balancing privacy and security).

[2] *Id.*

[3] *Id.*

[4] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) (plurality opinion).

arrest him before he strikes again?[5] What if not a robber but a drug dealer?[6] These examples may seem innocuous, even obvious to some. But what happens when police suspect you, and what harm will you suffer when it turns out they were wrong? These questions make up some of the murkiest depths of American Fourth Amendment jurisprudence, and confusion persists over when and within what constraints law enforcement can track your cellphone's location in real time.[7]

Both statutory and constitutional law governs law-enforcement acquisition of information regarding cellphone service subscribers, including cellphone location data. The Stored Communications Act ("SCA," "the Act"), specifically 18 U.S.C. § 2702(a)(3), restricts the disclosure of cellphone data to the government by cellular service providers,[8] while § 2702(c)(4) ("the emergency provision") provides an exception for certain emergency situations.[9] Other sections provide civil remedies for "nonconstitutional violations" of the Act.[10]

The Fourth Amendment, meanwhile, prohibits unreasonable searches by the government and requires that warrants issue based on a finding of probable cause.[11] Historically, however, these protections have not attached when a person's information is held by certain third parties, including communications providers.[12] Accordingly, some courts have found that the short-term, real-time GPS tracking of a cellphone located in a public place does not implicate constitutionally protected privacy concerns and is therefore not a search under the Fourth Amendment.[13] Regardless, the exigent circumstances exception to the Fourth Amendment warrant requirement, which aligns closely with the emergency provision allowing disclosure of subscriber information under § 2702(c)(4), might justify such tracking without a warrant even if it were a search.[14] Finally, because the SCA provides exclusively civil remedies when no constitutional violation has occurred,[15] if a court finds that the Fourth Amendment does not apply, criminal defendants cannot move to

[5] *See, e.g.*, United States v. Takai, 943 F. Supp. 2d 1315, 1317–18 (D. Utah 2013).

[6] *See, e.g.*, United States v. Skinner, 690 F.3d 772, 776 (6th Cir. 2012).

[7] *Carpenter*, 138 S. Ct. at 2220.

[8] 18 U.S.C. § 2702(a)(3).

[9] 18 U.S.C. §§ 2702(a)(3), (c)(4).

[10] 18 U.S.C. §§ 2707(a), 2708.

[11] U.S. CONST. amend. IV.

[12] *See* Smith v. Maryland, 442 U.S. 735, 745 (1979).

[13] *See, e.g.*, United States v. Riley, 858 F.3d 1012, 1017–18 (6th Cir. 2017) (per curiam).

[14] *See, e.g.*, United States v. Gilliam, 842 F.3d 801, 804 (2d Cir. 2016).

[15] 18 U.S.C. §§ 2707(a), 2708.

suppress cellphone location information disclosed in violation of § 2702(c)(4).[16]

Cellphones continuously and predictably transit areas traditionally endowed with the strongest Fourth Amendment protections, like the home.[17] This supports an objectively reasonable expectation of privacy in location information gained from even short-term live tracking of a cellphone. Without a clear standard holding that such tracking is a search, police will be unable to determine if their actions will unreasonably violate this expectation during any particular instance of tracking.[18] Further, while many such instances of short-term GPS monitoring will fall within the exigent circumstances exception to the warrant requirement,[19] failing to attach constitutional protections to short-term live tracking denies defendants the opportunity to suppress evidence when police improperly obtain GPS data under § 2702(c)(4), either by mistake or as the result of misconduct.[20] Holding such tracking to be a search also accords societal expectations of privacy that change as technology advances; however, it still permits police to avoid seeking a search warrant by invoking a traditional warrant exception or by relying instead on an arrest warrant, which may suffice for the purposes of short-term GPS tracking.[21]

Part II of this Note provides an overview of Fourth Amendment protections, the SCA and its remedies, and the definition of a search in the context of the so-called third-party doctrine. It also explores contemporary cases which hold government collection of electronic location information to constitute a search. Part III considers recent developments, in which courts have nevertheless not required a warrant for police to engage in real-time tracking of a criminal defendant's cellphone. Part IV argues courts should consider such short-term live tracking to be a search when undertaken pursuant to the emergency provision of § 2702(c)(4) and therefore require a search warrant absent narrow exceptions, including exigent circumstances and the issuance of a valid arrest warrant. When police engage in this type of tracking, Fourth Amendment safeguards are required to shield a defendant's constitutionally protected activities from unforeseeable revelation, provide an adequate remedy when no exigency is found, and serve the underlying purposes of the SCA. Short-term requests for live cellphone GPS information pursuant to § 2702(c)(4)

---

[16] People v. Moorer, 959 N.Y.S.2d 868, 875–76, 879 (Co. Ct. 2013).

[17] Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018) (plurality opinion).

[18] *See* Kyllo v. United States, 533 U.S. 27, 39 (2001).

[19] *See, e.g.*, United States v. McHenry, 849 F.3d 699, 706 (8th Cir. 2017).

[20] 18 U.S.C. § 2702(c)(4).

[21] *See* United States v. Riley, 858 F.3d 1012, 1020 (6th Cir. 2017) (Boggs, J., concurring) (per curiam) (arrest warrant); United States v. Takai, 943 F. Supp. 2d 1315, 1322–23 (D. Utah 2013) (exigency).

should therefore be considered a search under the Fourth Amendment and presumptively require a search warrant.

II. THE FOURTH AMENDMENT, THE SCA, AND THE RISE AND FALL OF THE THIRD-PARTY DOCTRINE

Section 2702(a)(3) of Title 18 of the United States Code prohibits electronic communications providers from disclosing the "record[s] or *other information* pertaining to a subscriber… to any governmental entity."[22] The physical location of a user's cellphone is one example of "other information."[23] An exception to this general prohibition permits providers to voluntarily disclose subscriber information to the government when the provider, "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay."[24]

Beyond these statutory requirements, which bind service providers, government acquisition of subscriber information may be subject to additional constitutional restraints imposed by the Fourth Amendment.[25] Case law governing when a defendant has a reasonable expectation of privacy in cellphone location data and other electronically stored information held by third parties so as to trigger Fourth Amendment protections, continuously evolves alongside society's own privacy expectations.[26]

Section A of this Part provides background on the basic protections afforded by the Fourth Amendment and describes the exigent circumstances exception to the warrant requirement. Section B provides a detailed summary of the development and erosion of the so-called "third-party doctrine" in parallel with changing technology and societal expectations of privacy. Finally, Section C explores the origins and purpose of the Stored Communications Act and the remedies it provides.

A. Fourth Amendment Protections and the Exigent Circumstances Exception

The Fourth Amendment protects against "unreasonable searches and seizures" by the government.[27] It ensures that "intrusion[s] by the police" are not "arbitrary,"[28] but instead are reasonable and subjected to adequate

[22] 18 U.S.C. § 2702(a)(3) (emphasis added).
[23] United States v. Gilliam, 842 F.3d 801, 803 (2d Cir. 2016).
[24] 18 U.S.C. § 2702(c)(4).
[25] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (plurality opinion).
[26] *Id.* at 2214–17.
[27] U.S. CONST. amend. IV.
[28] Wolf v. Colorado, 338 U.S. 25, 27 (1949).

scrutiny.[29] As such, searches conducted without a warrant are presumptively unreasonable.[30] This warrant requirement empowers an impartial judge, and not the police, to decide which intrusions are necessary based on a probable-cause standard.[31] Because the "ultimate touchstone of the Fourth Amendment is 'reasonableness,'" however, exceptions to the warrant requirement do exist.[32] Relevant here is the exigent circumstances exception.[33]

When an exigency makes the need for police action "sufficiently compelling,"[34] a search without a warrant may be "objectively reasonable" based on the totality of the circumstances."[35] The State bears the heavy burden of showing such an exigency.[36] Courts have found a valid showing of exigent circumstances in a variety of factual scenarios, including those involving a threat to police officers or the public.[37]

Courts have held that police are justified in conducting a warrantless search to interrupt acts of continuing or potential violence.[38] In *Brigham City v. Stewart*, the Supreme Court of the United States held that exigent circumstances justified a warrantless entry into the defendants' home to stop a physical altercation.[39] The Court found that the subjective motivations of the officers are irrelevant in determining the propriety of a warrantless search, so long as circumstances allow for an objectively reasonable determination that immediate action is required to prevent violence or mitigate injury.[40] Similarly, in *United States v. Thomas*, the court held that exigent circumstances justified a warrantless search of a recently occupied apartment to recover a weapon and ensure nobody was left on the premises to use it against the officers or bystanders.[41]

---

[29] Brigham City v. Stuart, 547 U.S. 398, 403 (2006); Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

[30] *Coolidge*, 403 U.S. at 454–55; U.S. CONST. amend. IV.

[31] Johnson v. United States, 333 U.S. 10, 14 (1948).

[32] *Brigham City*, 547 U.S. at 403.

[33] *Id.*

[34] Missouri v. McNeely, 569 U.S. 141, 148–49 (2013) (quoting Kentucky v. King, 563 U.S. 452, 460 (2011)).

[35] *Id.* (quoting Kentucky v. King, 563 U.S. 452, 460 (2011)).

[36] Welsh v. Wisconsin, 466 U.S. 740, 750 (1984).

[37] John Mark Huff, *Warrantless Entries and Searches Under Exigent Circumstances: Why are They Justified and What Types of Circumstances Are Considered Exigent?*, 87 UNIV. DET. L. REV. 373, 379 (2010).

[38] *See, e.g.*, *Brigham City*, 547 U.S. at 406.

[39] *Id.* at 400.

[40] *Id.* at 404–06.

[41] 372 F.3d 1173, 1175, 1177–78 (2004).

Many exceptions to the warrant requirement must be applied based on the totality of the circumstances of each individual case.[42] Where courts have been willing to delineate per se rules, they have often favored the defendant's privacy over the State's right to search.[43] Nevertheless, the development of the third-party doctrine placed the retrieval of some categories of information outside of the definition of a search entirely and therefore outside the protections of the Fourth Amendment as well.[44]

B. What is a Search? Development and Erosion of the Third-Party Doctrine

The question of whether government intrusion constituted a search within the meaning of the Fourth Amendment originally turned on an act of physical trespass by government agents.[45] Modern jurisprudence, however, has evolved to protect more than merely a property interest in the place to be searched.[46] Later cases provided an alternate avenue for determining whether a search had occurred, even when a physical trespass had not,[47] by asking if the individual had a reasonable expectation of privacy in the information sought.[48] The Supreme Court articulated this concept as a two-prong test in *United States v. Katz*, requiring both a subjective expectation of privacy on the part of the person whose information was to be searched and that this expectation be objectively reasonable based on societal standards.[49] Traditional third-party doctrine provides a simple answer to the second prong: when information is voluntarily disclosed to a third party, the source of the information, "takes the risk … that [it] will be conveyed by that person to the government."[50] Accordingly, any reasonable expectation of privacy, and therefore any

[42] Missouri v. McNeely, 569 U.S. 141, 150–52, 150 n.3 (2013) (noting that while the exigent circumstances exception is applied on a case-by-case basis, certain categorical exceptions to the warrant requirement, such as for searches incident to lawful arrest, also exist).

[43] Birchfield v. North Dakota, 136 S. Ct. 2160, 2186 (2016); *McNeely*, 569 U.S. at 145.

[44] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) [hereinafter *The Case for the Third-Party Doctrine*].

[45] United States v. Jones, 565 U.S. 400, 404–05 (2012).

[46] Katz v. United States, 389 U.S. 347, 351 (1967).

[47] *Jones*, 565 U.S. at 406, 409 (declining to decide whether a defendant had a reasonable expectation of privacy in the undercarriage of a vehicle because "the *Katz* reasonable-expectation-of-privacy-test has been *added to*, not *substituted for*, the common-law trespassory test.").

[48] *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

[49] *Id.* at 361.

[50] United States v. Miller, 425 U.S. 435, 443 (1976).

Fourth Amendment protection requiring the government to seek a warrant, is forfeit.[51]

1. Development of the Traditional Third-Party Doctrine

United States v. Miller, a seminal case applying the third-party doctrine, held that a defendant indicted for tax fraud had no protectable expectation of privacy in checks and other financial records held by banks of which the defendant was a client, because the information was voluntarily given to the bank and made regularly available to bank employees.[52]

The Supreme Court soon extended the doctrine to telephone records.[53] *Smith v. Maryland* involved a prosecution for a robbery in which, after robbing the victim, the defendant made threatening phone calls to the victim's home.[54] Without a warrant, police requested, and the telephone company installed, a pen register, which detected a call from the defendant's phone to the victim's.[55] In part due to evidence stemming from the pen register, the defendant was later convicted.[56] The Court applied the *Katz* analysis in affirming the lower courts' denial of the defendant's motion to suppress the fruits of the pen register.[57]

The Court reasoned that the defendant, aware the numbers he dialed were conveyed to the phone company for a variety of purposes, including potentially to aid law enforcement, likely lacked a subjective expectation of privacy in those numbers.[58] The Court noted specifically that the defendant may have had an expectation of privacy in the actual content of the call but that a pen register is incapable of recording such information.[59] Regardless, and relying heavily on *Miller*, the Court held there was no objectively reasonable expectation of privacy in the numbers the defendant dialed, as he assumed the risk that the phone company might turn them over to the government.[60] Because this type of information is conveyed to the telephone company regardless of where a call originates, the Court

---

[51] *The Case for the Third-Party Doctrine*, *supra* note 44, at 574.

[52] 425 U.S. at 436, 442.

[53] Smith v. Maryland, 442 U.S. 735, 745 (1979).

[54] *Id.* at 737.

[55] *Id.* At the time *Smith* was decided, federal law defined a pen register as a device installed on landline telephones or phone wires to record the numbers dialed by a target phone. Deborah F. Buckman, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cellphones and Internet Use*, 15 A.L.R. Fed. 2d 537 § 2 (2006).

[56] *Smith*, 425 U.S. at 738.

[57] *Id.* at 741.

[58] *Id.* at 742–43.

[59] *Id.* at 741, 743.

[60] *Id.* at 743–44.

rejected the argument that the defendant had a privacy interest merely because he placed the call from within his own home.[61] Based on the foregoing analysis, the Court held that no search had occurred and that the installation of the pen register without a warrant was proper.[62]

A related line of cases analyzed the Fourth Amendment implications of electronically tracking the movements of a defendant when those movements are exposed to the public.[63] Early on, the Supreme Court held that electronic surveillance of a defendant's movements in public places did not implicate the Fourth Amendment.[64] In *United States v. Knotts*, police attached a "beeper" to a canister of chloroform and used it to augment physical surveillance of a defendant as he traveled on public roads to a cabin used to manufacture illegal drugs.[65] Relying in part on *Smith*, the Court found that the defendant lacked a reasonable expectation of privacy in his movements because they were exposed to public view, both on the road and around the exterior of the cabin.[66] The Court reasoned that where electronic surveillance merely accomplished what would otherwise be possible with visual surveillance of those locations, no warrant was required.[67]

The Supreme Court tacitly acknowledged the lower court's concern that warrantless electronic tracking of private property might unreasonably intrude into private areas protected by the Fourth Amendment,[68] but found that the beeper did not reveal any movements within the cabin and therefore did not implicate any such constitutional concerns.[69] In contrast, however, the Court soon found that where a beeper revealed the location of an object inside a home, and when the location could not otherwise be ascertained from the outside, a search requiring a warrant had occurred.[70]

2. *United States v. Jones* and Erosion of the Third-Party Doctrine

Despite its robust jurisprudential foundation, including in its application to changing telephone technology,[71] the third-party doctrine

---

[61] *Id.* at 743.

[62] *Id.* at 745–46.

[63] *See, e.g.*, United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); United States v. Knotts, 460 U.S. 276, 282 (1983).

[64] *Knotts*, 460 U.S. at 282.

[65] *Id.* at 278, 281–82. The Court defined a "beeper" as a "radio transmitter … which emits periodic signals that can be picked up by a radio receiver." *Id.* at 277.

[66] *Id.* at 285.

[67] *Id.* at 282.

[68] *Id.* at 285; United States v. Knotts, 662 F.2d 515, 518 (1981), *rev'd*, 460 U.S. 276 (1983).

[69] *Knotts*, 460 U.S. at 285.

[70] United States v. Karo, 468 U.S. 705, 709–10, 714 (1984).

[71] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745 (1979).

has recently begun to erode under advances in surveillance techniques.[72] In *United States v. Jones*, police affixed a GPS device to the underside of a suspected drug trafficker's vehicle and tracked him for twenty-eight days.[73] While officers had originally obtained a warrant for the device, the warrant had expired by the time police placed the device on the vehicle.[74] Though a plurality of the Court held that a search had occurred based on the officers' physical trespass on the defendant's vehicle,[75] five justices in two concurring opinions held that even under a *Katz* analysis, tracking of the kind employed in *Jones* would raise Fourth Amendment concerns.[76]

Justice Alito and three others, concurring in the judgment, reasoned that long-term GPS tracking typically implicates reasonable expectations of privacy in that such comprehensive and continuous monitoring surpassed what could otherwise be reasonably accomplished with visual surveillance, even where a defendant's movements were public.[77] Though Justice Alito found that the twenty-eight days of tracking in the present case constituted a search, he declined to define a specific threshold past which Fourth Amendment protections might attach.[78] Justice Sotomayor's concurrence, echoing the caution raised in *Knotts*, extended these concerns to even short-term GPS monitoring.[79] She noted that warrantless tracking of devices such as cellphones may follow the devices' owners into private spaces and allow the government to trawl for vast quantities of information regarding religious, medical, and sexual activities without the protections of judicial oversight.[80] In so doing, she questioned the basic application of third-party doctrine to cell phones.[81] These concurrences laid the foundation for the Court's decision in *Carpenter*.[82]

Along similar lines, and years before deciding *Jones*, the Supreme Court held that law enforcement cannot circumvent a defendant's constitutional protections by employing sense-augmenting technology to

---

[72] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (plurality opinion).

[73] United States v. Jones, 656 U.S. 400, 403 (2012).

[74] *Id.* at 402–03.

[75] *Id.* at 403, 406–08.

[76] *Id.* at 430 (Alito, J., with Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring).

[77] *Id.* at 429–30 (Alito, J., with Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment).

[78] *Id.* at 430.

[79] *Id.* at 415 (Sotomayor, J., concurring).

[80] *Id.* at 416.

[81] *Id.* at 417.

[82] ORIN S. KERR, *Implementing Carpenter: The Digital Fourth Amendment*, (forthcoming 2018) (manuscript at 10), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 [https://perma.cc/6YA6-74SU] [hereinafter *Implementing Carpenter*].

gather information that could not otherwise be obtained without a physical intrusion.[83] In *Kyllo v. United States*, federal agents used a thermal-imaging camera to locate heat emanating from marijuana grow lights inside the defendant's home.[84] The device was not capable of showing human figures and indeed showed little more than crude patches of heat.[85] Nevertheless, the Court held that any information, however vague, regarding activities within the home was sufficiently private to evoke Fourth Amendment protections under the *Katz* framework.[86]

In support of this rule, the Court opined that even rough heat signatures might reveal specific "intimate" and protectable activities.[87] They further cautioned that a standard for defining a search based on a post hoc review of what specific information was gathered would prevent law enforcement from knowing in advance whether their activities would be constitutional.[88] Finally, the Court reasoned that a clear legal boundary protecting the inside of the home anticipated the development of increasingly sophisticated technology that might reveal more specific human activity, information which even the dissent acknowledged was worthy of constitutional protection.[89] Accordingly, the Court held that any State use of technology not available to the general public and permitting "explor[ation]" of a "constitutionally protected area,"[90] which could not otherwise be accomplished without physically invading it, constituted a search and therefore required a warrant.[91]

In the forty years since the Supreme Court decided *Smith*, the Court has expanded the array of privacy interests covered by the Fourth Amendment due to the increasingly detailed and invasive nature of personal information stored by communications providers and on cellphones in particular.[92] In 2014, the Supreme Court narrowed the search-incident-to-lawful-arrest exception to the warrant requirement by

[83] Kyllo v. United States, 533 U.S. 27, 34–35 (2001).

[84] *Id.* at 29–30.

[85] *Id.* at 31.

[86] *Id.* at 35, 37.

[87] *Id.* at 38 (discussing the example of "the lady of the house tak[ing] her daily sauna and bath").

[88] *Id.* at 39.

[89] *Id.* at 35–36 (noting that "the rule we adopt must take account of more sophisticated systems that are already in use or in development."); *id.* at 48 (Stevens, J., with Rehnquist, CJ. and O'Connor and Kennedy, JJ., dissenting).

[90] *Id.* at 34 (majority opinion); *id.* at 40 (Stevens, J., with Rehnquist, CJ. and O'Connor and Kennedy, JJ., dissenting).

[91] *Id.* at 40 (majority opinion).

[92] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018) (plurality opinion).

holding that police must generally obtain a warrant before searching data stored on a cellphone seized incident to arrest.[93]

In *Riley v. California*, officers searched a defendant's smartphone for evidence of gang-related criminal activity after he was arrested for firearms possession during a routine car stop.[94] The Court found that though a cellphone is often found within reach of a defendant at the time of arrest, a search of the data stored on it falls outside the purposes of the traditional rule for searches incident to arrest.[95] Specifically, the Court found that searching the contents of a phone served neither the governmental interest in ensuring officer safety nor in preventing the destruction of evidence.[96] The Court reasoned that data could not reasonably be harmful to officers and enumerated several ways in which officers could prevent the destruction or concealment of evidentiary materials stored on a phone without searching it immediately.[97]

Moreover, the Court reasoned that though suspects have a reduced expectation of privacy while in custody, a search of cellphone data far exceeded the minimal "additional intrusion" imposed by a search of a suspect's person and effects.[98] A cellphone, they reasoned, might contain vast data in the form of communications, photos, and videos, which could give a near-complete picture of a suspect's life indefinitely into the past.[99] The Court expressed particular concern over certain categories of information related to "private interests," such as medical inquiries and a person's location history, which might reveal protected religious, political,

---

[93] Riley v. California, 573 U.S. 373, 401–02 (2014) (per curiam) (also contemplating that, in limited situations, officers might rely on exigent circumstances or another case-by-case exception to search cellphone data without a warrant after making an arrest).

[94] *Id.* at 378–80.

[95] *Id.* at 385–86. Assessing the validity of warrantless searches in general requires balancing the degree of intrusion into the subject's privacy against the need to protect government interests advanced by the search. Wyoming v. Houghton, 526 U.S. 295, 300 (1999). Searches incident to arrest specifically weigh the defendant's significantly reduced expectation of privacy while in custody against the government's dual interests in promptly recovering weapons that might be used to harm officers and evidence that might be readily concealed or destroyed. *Riley*, 573 U.S. at 385–86; Chimel v. California, 395 U.S. 752, 763 (1969). Accordingly, the traditional and enduring rule remains that the search incident to arrest must not exceed the area within the "immediate control" and reach of the defendant. *Chimel*, 395 U.S. at 763.

[96] *Riley*, 573 U.S. at 387–88.

[97] *Id.* at 387–91 (describing methods such as turning the phone off or placing it in a Faraday bag to prevent the remote wiping of the phone's contents and suggesting disabling the phone's locking feature to prevent evidence from becoming irretrievable).

[98] *Id.* at 393.

[99] *Id.* at 394.

and other activities.[100] Considering the profound level of intrusion into a defendant's privacy against the minimal potential to further governmental interests,[101] the Court concluded that, categorically, absent a case-by-case warrant exception such as exigent circumstances, an officer's obligation before searching a phone "seized incident to arrest is … simple—get a warrant."[102]

3. Electronic Location Data and the New Age of *Carpenter*

Drawing on the aforementioned cases, the Supreme Court decided *Carpenter v. United States* and specifically repudiated the third-party doctrine with regard to historical cellphone-location data.[103] In *Carpenter*, federal prosecutors obtained two court orders compelling the defendant's cellphone-service provider to surrender respectively 127 days and seven days of historical cell-site location information ("CSLI") in order to tie the defendant to a four-month string of robberies.[104]

Based upon the substantial volume of information collected and the fact that a cellphone readily enters private, constitutionally protected spaces, the Court held that historical CSLI provides so comprehensive a picture of a defendant's life as to create a reasonable expectation of privacy.[105] Reasoning that this level of intrusion could not have been imagined at the time the third-party doctrine was fashioned, the Court noted that cellphone location data is passively siphoned from a user instead of actively and voluntarily shared, like the dialed phone numbers in *Smith*.[106] The Court further highlighted the *Jones* concurrences, which reasoned that comprehensive tracking of even public movements might constitute a search.[107]

---

[100] *Id.* at 395–96 (quoting United States v. Jones, 565 U.S. 400, 414–15 (2012) (Sotomayor, J., concurring)).

[101] *Id.* at 396.

[102] *Id.* at 402–03.

[103] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (plurality opinion).

[104] *Id.* at 2212. The second order resulted in the production of only two days of records. *Id.* The records were obtained pursuant to a provision of the Stored Communications Act that required disclosure based upon court orders issued after a showing lower than the probable cause required to obtain a search warrant. *Id.*; *see infra* Section II-C.

[105] *Carpenter*, 138 S. Ct. at 2219. CSLI triangulates a cellphone's location based on the phone's connection to nearby cell sites. *Id.* at 2211, 2219. As a result, the accuracy of CSLI depends on the concentration of cell sites in the phone's vicinity. *Id.* At the time *Carpenter* was decided, CSLI, which was accurate to within fifty meters, had not even reached the level of precision provided by GPS data. *Id.* at 2219.

[106] *Id.* at 2220.

[107] *Id.* at 2219–20.

Even though CSLI is disclosed to a service provider in the regular course of using a cellphone, and even though many of the defendant's movements may have been public, technological innovation had reframed societal standards regarding a reasonable expectation of privacy and rendered the third-party doctrine inapplicable to government requests for historical CSLI.[108] The Court therefore opined that a person has a reasonable expectation of privacy in, "the record of his physical movements as captured through CSLI."[109] Leaving open the possibility that the government might, in limited circumstances, rely on an exception such as exigent circumstances to obtain CSLI without a warrant, the Court held that, under the *Katz* framework, a demand for seven, and certainly 127 days' worth of CSLI constituted a search.[110]

In his dissenting opinion, Justice Gorsuch agreed with the plurality that traditional third-party doctrine could not be extended to cover CSLI and other customer information stored electronically by service providers.[111] He went further, however, rejecting the *Katz* framework entirely in his Fourth Amendment analysis of CSLI. Returning instead to protections rooted in property law, Justice Gorsuch imagined that providers held a customer's data as an "involuntary bailment," in which the customer retains a constitutionally protectable ownership interest.[112] As such, the customer would not surrender all Fourth Amendment protections in information entrusted to a third party,[113] and these protections would remain intact regardless of whether the information must be turned over as a condition of service.[114]

The *Carpenter* Court specifically declined to extend its ruling to other forms of information collection, including real-time CSLI tracking.[115] Therefore, while *Carpenter* significantly narrowed the scope of the third-party doctrine as applied to cellphone location records, lower courts have been free to hold that factual situations on the fringes of *Carpenter* fail to raise Fourth Amendment protections.[116]

C. The Stored Communications Act and Its Remedies

The Stored Communications Act was enacted in 1986 as Title II of the Electronic Communications Privacy Act ("ECPA"), which provided

---

[108] *Id.* at 2217, 2223.
[109] *Id.* at 2217.
[110] *Id.* at 2217 & n.3, 2223.
[111] *Id.* at 2272 (Gorsuch, J., dissenting).
[112] *Id.* at 2270.
[113] *Id.* at 2269.
[114] *Id.* at 2270.
[115] *Id.* at 2220 (plurality opinion).
[116] *See* United States v. Howard, 426 F. Supp. 3d 1247, 1257 (M.D. Ala. 2019).

amendments to the Wiretap Act of 1968 designed to protect electronic communications from unlawful interception and disclosure.[117] Application of the traditional third-party doctrine to changing technology, specifically electronic data increasingly stored by private telecommunications companies, had created gaps in Fourth Amendment protections.[118] The newly-enacted provisions of the SCA were intended keep pace with these changes and fill the gaps.[119] The same reasoning was later extended to information in the possession of Internet Service Providers ("ISPs").[120] The bill sought to enact "clear standards" to shield police from liability, preserve the "admissibility of evidence," and, significantly, stop the "gradual erosion" of the constitutional right to privacy.[121] The ECPA eventually passed both houses of Congress with strong support from the United States Department of Justice.[122] The emergency disclosure provision in § 2702(c)(4), which permits a communications provider to voluntarily disclose certain user data to the government in the face of a threat to life or limb,[123] was not included in the original bill and was added later as part of the USA PATRIOT Act in 2001.[124]

The ECPA generally was inspired in part by a letter from the Justice Department's Criminal Division to one of the senators who later introduced a version of the bill.[125] The letter suggested that electronic communications were protected from "unauthorized acquisition only where a reasonable expectation of privacy exists."[126] In the face of newly developed communication modalities, however, when such a reasonable expectation existed was unclear.[127]

Case law up to that point suggested that users of electronic communications services may not have the required reasonable privacy expectation in the information and communications they disclosed to their

---

[117] S. REP. NO. 99-541, at 1, 25 (1986).

[118] *See id.* at 3, 5.

[119] *See id.* at 1–3, 5.

[120] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004) [hereinafter *A User's Guide to the Stored Communications Act*].

[121] S. REP. NO. 99-541, at 5.

[122] H.R.4952 – Electronic Communications Privacy Act of 1986, LIBRARY OF CONGRESS, https://www.congress.gov/bill/99th-congress/house-bill/4952/all-actions?overview=closed#tabs [https://perma.cc/3VJM-DTR3] (last visited Nov. 20, 2020); S. REP. NO. 99-541, at 4.

[123] 18 U.S.C. § 2702(c)(4).

[124] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 284.

[125] S. REP. NO. 99-541, at 2, 4.

[126] *Id.*

[127] *Id.*

service providers by virtue of using these services.[128] These decisions left no clear answer as to whether Fourth Amendment protections attached to this type of information when held by these third-party providers.[129] Even if the Fourth Amendment were applicable, however, courts had traditionally permitted government agencies to gain access to this information through the use of subpoenas and court orders issued on requirements less stringent than the probable cause standard against which warrant applications are judged.[130]

Courts generally held these subpoenas to be compatible with an individual's Fourth Amendment rights unless the subpoena was overbroad in its request for records.[131] A subpoena may not have been overbroad unless it sought information that was irrelevant or vague, or it was "unduly burdensome" to the recipient.[132] Therefore, where information was held by a third-party electronic communication provider, the government could compel disclosure of the information via subpoena instead of by means of "a warrant based on probable cause."[133] Finally, as a private entity, an electronic communication provider could itself search the communications and information of a user and disclose them voluntarily to a government agency free from the Fourth Amendment constraints applicable to state actors.[134]

The SCA regulates some of the aforementioned contingencies.[135] It restricts disclosure of subscriber communications and information by public providers of remote computing services and electronic communication services.[136] Under the SCA, an electronic communication service is any entity which allows users to send or receive "electronic communications," defined elsewhere as the transfer of signals by radio or various other electronic means.[137] Notably, this definition does not include wire or oral communications, the interception and disclosure of which are governed by separate statutes;[138] it does, however, cover other forms of electronic communication such as e-mail.[139]

---

[128] *A User's Guide to the Stored Communications Act*, *supra* note 120, at 1210–11.

[129] *Id.* at 1211.

[130] *Id.*

[131] *Id.*

[132] *In re* Horowitz, 482 F.2d 72, 79 (2d Cir. 1973).

[133] *A User's Guide to the Stored Communications Act*, *supra* note 120, at 1211.

[134] *Id.* at 1212.

[135] 18 U.S.C. §§ 2702–03.

[136] 18 U.S.C. § 2702(a).

[137] 18 U.S.C. § 2510(12), (15).

[138] 18 U.S.C. § 2511.

[139] *See A User's Guide to the Stored Communications Act*, *supra* note 120, at 1211.

The SCA restricts disclosure of information differently based on whether the disclosure is voluntary or compelled by a government agency.[140] Section 2702 generally prohibits electronic communication service providers from *voluntarily* disclosing the contents of stored electronic communications, as well as any "record or other information pertaining to" a user of the provider's service.[141] The section then enumerates several carveouts, which allow the voluntary disclosure of either the contents of an electronic communication or of a record or other information pertaining to a user.[142] For the purposes of § 2702, the physical location of a cellphone, when stored by a cellphone service provider, is a protected form of "other information."[143]

Exceptions allowing the disclosure of records or other information include consent of the subscriber and situations in which disclosure is necessary to protect the property of the provider.[144] Moreover, the SCA allows for free disclosure of records or other information to nongovernmental entities.[145] Disclosure of such information to the government, however, is restricted under § 2702(c)(4) to circumstances in which, "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury" requires immediate disclosure of information related to the exigency.[146] The relatively stringent restrictions on disclosure to a governmental entity as compared to a nongovernmental entity reflect the congressional effort to prevent the "gradual erosion" of Fourth Amendment protections against government intrusion.[147]

Section 2703 enumerates restrictions on the government's ability to *compel* disclosure of the contents of electronic communications and other subscriber information and records from providers by several means, including by warrant, subpoena, or other court order.[148] *Carpenter*, and other lower-court decisions, however, have held that § 2703 violates the Fourth Amendment when applied to historical CSLI and other categories of electronically stored information.[149] Moreover, while the

---

[140] *Compare* 18 U.S.C § 2702 (voluntary disclosures), *with* § 2703 (compelled disclosures).

[141] 18 U.S.C. § 2702(a)(1), (3).

[142] 18 U.S.C. § 2702(b), (c).

[143] United States v. Gilliam, 842 F.3d 801, 803 (2d Cir. 2016).

[144] 18 U.S.C. § 2702(c)(2)–(3).

[145] 18 U.S.C. § 2702(c)(6).

[146] 18 U.S.C. § 2702(c)(4).

[147] S. REP. NO. 99-541, at 5 (1986).

[148] 18 U.S.C. § 2703(a)–(c).

[149] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (plurality opinion) (explaining that, "an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a

constitutionality of § 2703 under the Fourth Amendment may be relevant for assessing the constitutionality of related provisions of the SCA, this Note primarily considers voluntary disclosure of records and other information pertaining to an electronic communication service subscriber under § 2702.

Finally, later sections of the SCA provide a series of remedies for violations of the Act.[150] Section 2707 provides for a right of civil action against any entity other than the government, including providers, who knowingly or intentionally violate SCA provisions.[151] It also provides an avenue for administrative discipline against government agents for similar violations.[152] Section 2712 mirrors § 2707, but provides for civil action against the government for "willful violation[s]" of the SCA and related statutes,"[153] and specifies that such civil action is the exclusive remedy against the government for "any claims within the purview of this section."[154] As § 2702 restricts the actions of providers, however, and not those of the government directly, it is not clear that even § 2712's exclusive remedies against the government would apply to unauthorized disclosure of records or other information under § 2702.[155] Interestingly, § 2708 comprises a separate, but broader exclusivity-of-remedies provision, providing that any remedies enumerated in the SCA are the exclusive remedies for any "nonconstitutional" violations of the Act.[156]

Against the backdrop of traditional Fourth Amendment law, and the evolution of the third-party doctrine through *Carpenter*, lower courts have continued to rule on the propriety of law-enforcement efforts to secure short-term, live tracking of criminal suspects' cellphones under the emergency provision of § 2702(c)(4).[157]

III. WHEN SHORT-TERM, LIVE TRACKING OF A CELLPHONE DOES NOT REQUIRE A WARRANT

This Part explores recent lower court decisions regarding the short-term, live tracking of cellphones to facilitate the apprehension of wanted criminals. Section A describes cases in which courts held such tracking

familiar one—get a warrant."); United States v. Ramirez, 471 F. Supp. 3d 354, 359 (D. Mass. 2020) (recognizing Carpenter's effect on orders under section 2703(d) when involving CSLI).

[150] 18 U.S.C. §§ 2707, 2708, 2712.

[151] 18 U.S.C. § 2707(a).

[152] 18 U.S.C. § 2707(d).

[153] 18 U.S.C. § 2712(a).

[154] 18 U.S.C. § 2712(d).

[155] 18 U.S.C. §§ 2702, 2712.

[156] 18 U.S.C. § 2708.

[157] *See infra* Part III.

does not constitute a search at all, while Section B describes those in which exigent circumstances were found to justify the tracking, regardless of whether a search occurred. In the shadow of *Carpenter*, these cases illustrate the incongruous treatment of such tracking under the Fourth Amendment, when compared with other forms of electronic surveillance upon which the Supreme Court has already rendered decisions.

A. Short-Term, Real-Time GPS Tracking of a Cellphone May Not Constitute a Search Within the Meaning of the Fourth Amendment

As noted above, the traditional third-party doctrine vitiated Fourth Amendment protections when an individual "voluntarily turn[ed] [certain information] over to third parties," including metadata stored by a telephone company when a subscriber used the company's service.[158] Defendants may also lack a privacy interest in their physical location when they travel on "public thoroughfares" and so voluntarily subject their movements to public scrutiny.[159] While the Supreme Court has already held that acquisition of long-term, historical CSLI constitutes a search,[160] no binding opinion has yet ruled on whether short-term, real-time GPS tracking does as well.[161]

The pre-*Carpenter* decisions of some lower courts, however, have held that this type of tracking does not constitute a search because a defendant has no reasonable expectation of privacy in otherwise public movements.[162] In *United States v. Skinner*, federal authorities tracked a suspected drug trafficker along public highways for three days using GPS data from his cellphone before apprehending him at a rest stop.[163] The United States Court of Appeals for the Sixth Circuit found that this did not reveal such comprehensive information as to implicate Fourth Amendment privacy concerns because the tracking was relatively brief and did not disclose any information that could not have been reasonably ascertained through visual observation.[164] On these grounds, the court held the defendant had no reasonable expectation of privacy in the "signal

[158] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[159] United States v. Knotts, 460 U.S. 276, 281 (1983).

[160] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (plurality opinion).

[161] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., with Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring).

[162] *Carpenter*, 138 S. Ct. at 2219–20; United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012) (superseded by regulation on unrelated grounds pertaining to the U.S. Sentencing Guidelines as noted in United States v. Penny, 777 Fed. App'x 142, 151 (6th Cir. 2019)).

[163] *Skinner*, 690 F.3d at 776, 778, 780.

[164] *Id.* at 778, 780.

emanating from his phone," despite the fact that police had never physically surveilled him before his arrest.[165]

Similarly, in *United States v. Riley*, federal agents tracked the cellphone of a suspected armed robber for approximately seven hours after obtaining a warrant for his arrest, but no search warrant for his phone.[166] Using GPS information, officers tracked the defendant to a motel, and only then determined his precise location and room number by asking an employee.[167] Relying on the Supreme Court's contrast between *Knotts* and *United States v. Karo*, the court reasoned that because the tracking, which persisted for even less time than in *Skinner*, revealed only the defendant's otherwise public movements, and not his movements within the motel room itself, it did not amount to a search under the *Katz* framework.[168]

While the majority opinion noted the district court's reliance on the prior issuance of an arrest warrant to justify the GPS tracking,[169] the arrest warrant did not meaningfully factor into the panel's holdings. In a concurring opinion, however, one judge noted that, while GPS tracking sufficiently precise to detect the defendant's location or movements within a home or specific motel room might ordinarily amount to a search, it should not when the defendant was already subject to a valid arrest warrant.[170] This concurrence noted that officers may already enter a home subject to an arrest warrant issued on probable cause when they reasonably suspect the defendant to be inside.[171] By analogy, the concurrence reasoned, officers armed with an arrest warrant should be able to conduct what would otherwise amount to a search of a defendant's cellphone location data, even if it would reveal the defendant's precise movements within a constitutionally protected space, provided they reasonably suspect the defendant to be in possession of the phone.[172]

Post-*Carpenter* opinions, however, illustrate the confusion the latter decision infused into lower-court determinations related to GPS tracking.[173] In *United States v. Howard*, police received consent from a confidential informant to place a GPS tracker on her truck, which she

---

[165] *Id.* at 775, 779; *see also* United States v. Knotts, 460 U.S. 276, 278, 280 (1983).

[166] United States v. Riley, 858 F.3d 1012, 1013 (6th Cir. 2017) (per curiam). Note that GPS data in this case were obtained pursuant to a court order under § 2703 of the SCA as opposed to the emergency provisions under § 2702(c)(4). *Id.* at 1014.

[167] *Id.* at 1013.

[168] *Id.* at 1017–18.

[169] *Id.* at 1016.

[170] *Id.* at 1019–20 (Boggs, J., concurring).

[171] *Id.* at 1020 (citing Payton v. New York, 445 U.S. 573, 602–03 (1980)).

[172] *Id.* (citing Payton v. New York, 445 U.S. 573, 602–03 (1980)).

[173] *See, e.g.*, United States v. Howard, 426 F. Supp. 3d 1247, 1251 (M.D. Ala. 2019).

subsequently lent to a suspected methamphetamine dealer.[174] Police tracked the defendant on exclusively public roads for just under twenty-four hours before arresting him and without performing direct visual surveillance.[175] The court ultimately held that, as in *Knotts*, the defendant had no reasonable expectation of privacy because his movements were tracked live during only a single trip on public roads.[176] In its opinion, however, the court discussed the complexity introduced by the holding in *Carpenter* that, under the right circumstances, a defendant might have a reasonable expectation of privacy in his physical movements as documented by electronic tracking, even where many of those movements were otherwise public.[177] In particular, the court recognized that, in explicitly declining to rule on live tracking using GPS, *Carpenter* left lower courts with little clear guidance in assessing electronic surveillance.[178]

The court considered factors from prior decisions, such as the duration of tracking, whether the data gathered were live or historical, and the ability of the tracking device to enter constitutionally protected spaces.[179] Because the instant defendant was tracked for a relatively short period, in real time, and using a vehicle in public, the data collected failed to impinge on several of the privacy concerns raised in *Carpenter*.[180] The court reasoned, however, that the GPS tracking of a cellphone might, as in *Karo* and *Carpenter*, lead police impermissibly into spaces protected by the Fourth Amendment.[181] The holding in *Carpenter*, the court acknowledged, inched the Supreme Court closer to "revisiting" *Knotts*.[182]

Recent decisions at the appellate and district levels suggest a general tendency by the United States Court of Appeals for the Eighth Circuit to align with the Sixth Circuit, as in *Skinner*, above.[183] In *United States v. McHenry*, the court noted in dictum, "substantial doubt that [the defendant] had a reasonable expectation of privacy in cellphone location information voluntarily provided" to his cellular carrier.[184] Similarly, in

---

[174] *Id.* at 1249–50.

[175] *Id.* at 1250.

[176] *Id.* at 1257.

[177] *Id.* at 1254; Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (plurality opinion).

[178] *Howard*, 426 F. Supp. 3d at 1254.

[179] *Id.* at 1257.

[180] *Id.*

[181] *Id.*

[182] *Id.* at 1258.

[183] *See, e.g.*, United States v. McHenry, 849 F.3d 699, 706 (8th Cir. 2017) (citing *Skinner*, 690 F.3d at 777–81); United States v. Sauceda, No. 4:16-CR-40083-01-KES, 2017 WL 4676606, at *10 (D.S.D. Sept. 27, 2017).

[184] 849 F.3d at 706. Interestingly, the Court in *McHenry* references the defendant's disclosure of his cellphone's location to his wireless provider, raising the

United States v. Sauceda, police fearful for the safety of a confidential informant made an emergency request to a suspected drug dealer's cellphone provider for the provider to "ping" the GPS on the defendant's cellphone.[185] Though police obtained the relevant GPS tracking data without a search warrant, a separate warrant had previously been issued to track another of the defendant's cellphones, which was no longer registered to him at the time police attempted to execute the search.[186] Further, just before pinging the defendant's phone pursuant to the emergency request, officers secured a warrant for the defendant's arrest.[187]

Using pings from the emergency request, officers tracked the defendant to the vicinity of a hotel where he was apprehended.[188] As in *United States v. Riley*, GPS tracking led officers only to the hotel itself, at which point they relied on traditional surveillance and interviews with hotel staff to ascertain the defendant's precise location.[189] The court found that the warrantless GPS tracking of the defendant's cellphone did not constitute a search.[190] Though the court discussed factors raised in *Skinner* and *United States v. Riley*, including the short duration of the tracking and the fact that it revealed no information from inside a home or hotel room,[191] the court's opinion entirely adopted the concurrence in *United States v. Riley*.[192] Specifically, the court held that the defendant had no reasonable expectation of privacy in his location, regardless of the characteristics of the electronic tracking used to locate him, because a warrant had been issued for his arrest before police pinged his phone.[193]

While *Carpenter* suggests a trend towards recognizing an expanded expectation of privacy in cellphone location data obtained from third parties,[194] courts in the Eighth and surrounding circuits have allowed the short-term, real-time GPS tracking of cellphones without a search warrant

---

specter of traditional third-party doctrine in *Smith*. *Id.* In so doing, however, the Court cites *Skinner*, wherein the decision rested instead on the defendant's disclosure of his location to the *general public*, which therefore could have been ascertained by police without the assistance of electronic tracking. *Skinner*, 690 F.3d at 778.

[185] 2017 WL 4676606, at *4.

[186] *Id.*

[187] *Id.* at *5.

[188] *Id.* at *4–5.

[189] *Id.* at *5.

[190] *Id.* at *10.

[191] *Id.* at *6–7.

[192] *Id.* at *7, 10 ("It is not necessary in this instance for this court to determine whether Skinner rules the day, or whether the Eighth Circuit might adopt the Skinner analysis if faced squarely with the question.").

[193] *Id.* at *9–10 (quoting United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016)) ("A person wanted on probable cause (and an arrest warrant) who is taken into custody in a public place, where he had no legitimate expectation of privacy, cannot complain about how the police learned his location.").

[194] *Implementing Carpenter*, *supra* note 82 (manuscript at 1, 8).

in public places and seem willing to allow it when the tracking enters private spaces as well when an arrest warrant has already been issued.[195] It is unclear, however, what effect *Carpenter* might have on any future ruling on this subject by the Eighth Circuit.

B. Short-Term, Real-Time GPS Tracking Without a Warrant, Pursuant to 18 U.S.C. § 2702(c)(4) May Be Justified by Exigent Circumstances

As noted above, police must generally obtain a warrant before undertaking a search, subject to limited exceptions.[196] Exigent circumstances provide such an exception when, "lives are threatened, [or] a suspect's escape is imminent."[197] Section 2702(c)(4) similarly allows providers to disclose cellphone location data to the government when the provider believes there is a danger of injury or death.[198] Courts have found, in a variety of circumstances, that these constitutional and statutory standards coalesce into a single analysis.[199] Short-term, real-time, warrantless tracking of a cellphone may therefore be justified by exigent circumstances and, when it is, disclosure under § 2702(c)(4) will generally also be proper.[200]

Several courts have found that exigent circumstances justified the short-term, real-time tracking of a cellphone without a warrant under §2702(c)(4) to protect victims of human trafficking.[201] In *United States v. Gilliam*, the court upheld warrantless tracking of a defendant's cellphone over a single day to find a child trafficked for sex work and effect the defendant's arrest after police located him on a New York City street corner.[202] Considering both the statutory and constitutional exigency provisions in one analysis,[203] the court found that forced sex work itself exposed the minor to a sufficiently "significant risk of serious bodily injury" that exigent circumstances justified warrantless tracking of the

---

[195] United States v. Riley, 858 F.3d 1012, 1017–18 (6th Cir. 2017) (per curiam); *id.* at 1020 (Boggs, J., concurring); United States v. McHenry, 849 F.3d 699, 706 (8th Cir. 2017); *Sauceda*, 2017 WL 4676606, at *9–10.

[196] Riley v. California, 573 U.S. 373, 382 (2014).

[197] United States v. Ball, 90 F.3d 260, 263 (8th Cir. 1996).

[198] 18 U.S.C. § 2702(c)(4).

[199] *See, e.g.*, United States v. Gilliam, 842 F.3d 801, 804 (2d Cir. 2016).

[200] *See, e.g.*, *id* at 804–05.

[201] United States v. McHenry, 849 F.3d 699, 706 (8th Cir. 2017); *Gilliam*, 842 F.3d at 804 (2d Cir. 2016).

[202] 842 F.3d at 802, 804.

[203] *Id.* at 804 ("Both the second statutory issue [of whether or not the emergency provision of § 2702(c)(4) was satisfied] and the Fourth Amendment issue turn on whether the circumstances known to law enforcement and present to Sprint were within the category of 'exigent circumstances' that permit warrantless searches.").

cellphone.[204] The court further noted that the defendant's cell service provider therefore had a good faith basis for releasing the tracking data to police under § 2702(c)(4).[205]

Similarly, in *McHenry*, police used an emergency GPS tracking request under § 2702(c)(4) to warrantlessly trace a cellphone used to facilitate the sex trafficking of a minor.[206] On the same day, police went to the motel where the phone was located and ascertained the precise location of the victim and defendant by speaking with motel staff.[207] Citing *Gilliam*, the court held that exigent circumstances justified the relevant cell service provider in releasing GPS location data to police.[208]

Courts have also permitted such tracking to locate suspected perpetrators of violent crimes.[209] In *United States v. Andrews*, police made an emergency request under § 2702(c)(4) to track the cellphone of a defendant with an lengthy criminal history, suspected of committing two shootings on the day in question, and believed to still be armed.[210] Police monitored the defendant remotely for approximately seven hours before arresting him.[211] The District Court held that these circumstances justified both disclosure of the location data to police under the SCA and tracking of the cellphone without a warrant.[212]

In *United States v. Takai*, police sought a defendant suspected in two similar robberies committed on the same day, one of which involved a shooting.[213] Fearing the defendant might attempt another robbery and believing him to still pose a danger to the public, police obtained emergency GPS tracking data for the defendant's cellphone under § 2702(c)(4) without a warrant.[214] Within a day, police located and arrested the defendant.[215] As in *Andrews*, the court held that the circumstances permitted disclosure of the tracking data to police under § 2702(c)(4) and, separately, that it was proper for police to obtain the data without a warrant under the traditional exigent circumstances exception.[216] The *Takai* court added, however, that "even if the court were required to find" that tracking the defendant's phone without a warrant "violat[ed] the …

---

[204] *Id.*

[205] *Id.* at 805.

[206] *McHenry*, 849 F.3d at 702.

[207] *Id.*

[208] *Id.* at 706.

[209] United States v. Andrews, 381 F. Supp. 3d 1044, 1063 (D. Minn. 2019); United States v. Takai, 943 F. Supp. 2d 1315, 1322–23 (D. Utah 2013).

[210] 381 F. Supp. 3d at 1049–51.

[211] *Id.* at 1049–52.

[212] *Id.* at 1063.

[213] 943 F. Supp. 2d at 1317–18.

[214] *Id.* at 1318, 1320.

[215] *Id.* at 1318.

[216] *Id.* at 1322–23.

Fourth Amendment," suppression of the resulting evidence would be an improper remedy based on the officers' "good faith reliance" on the emergency provision of the SCA.[217]

Finally, courts have found exigent circumstances where there is an articulable danger to law-enforcement officers or agents.[218] In *United States v. Caraballo*, when police suspected that the defendant committed a murder because of the victim's cooperation with law enforcement,[219] officers sought emergency GPS location data without a warrant, under § 2702(c)(4).[220] Exigent circumstances justified tracking the defendant's cellphone for about two hours to apprehend him in a public place, because police were concerned the defendant was still armed and that other officers and informants might be in danger.[221] In *Sauceda*, the defendant sought to meet with a confidential informant to retrieve drugs and money, which, unbeknownst to him, had already been seized from the informant by police.[222] Exigent circumstances justified pinging the defendant's cellphone, presumably pursuant to § 2702(c)(4),[223] to effect his arrest before the meeting, based on concerns that the defendant might have known the informant was working with police.[224]

Exigent circumstances may therefore excuse the Fourth Amendment warrant requirement for short-term, real-time tracking of a cellphone by GPS.[225] When this is the case, the emergency requirements of § 2702(c)(4) are generally also satisfied to permit disclosure by cellphone service providers.[226] The courts' treatment of the underlying constitutional nature of such tracking in the cases above, however, reveals several internal inconsistencies. Notably, in light of finding exigent circumstances – and in *Sauceda*, the presence of an arrest warrant as well – most of the courts either failed to,[227] or explicitly declined to answer the thornier

[217] *Id.* at 1323–24 (citing United States v. Leon, 468 U.S. 897 (1984)); United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012).

[218] United States v. Caraballo, 831 F.3d 95, 105 (2d Cir. 2016); United States v. Sauceda, No. 4:16-CR-40083-01-KES, 2017 WL 4676606, at *13 (D.S.D. Sept. 27, 2017).

[219] 831 F.3d at 105.

[220] *Id.* at 99.

[221] *Id.* at 98, 100, 104.

[222] 2017 WL 4676606, at *11–12.

[223] *Id.* at *12.

[224] *Id.* at *12–13 (alternative justification to the court's ruling, as noted above, that, under the circumstances, tracking the defendant's cellphone did not violate his Fourth Amendment interests at all).

[225] *See* United States v. Gilliam, 842 F.3d 801, 804 (2d Cir. 2016).

[226] *See id.* at 805; United States v. Andrews, 381 F. Supp. 3d 1044, 1062–63 (D. Minn. 2019).

[227] *Andrews*, 381 F. Supp. 3d at 1062–63; United States v. Takai, 943 F. Supp. 2d 1315, 1321–23 (D. Utah 2013).

constitutional question of whether the GPS tracking described would otherwise constitute a search at all.[228] The *Gilliam* court *assumed* that Fourth Amendment protections applied to cellphone location data, but did not specifically analyze the issue.[229] The court in *Caraballo*, meanwhile, appeared to vacillate, repeatedly referring to tracking the phone as "the search,"[230] and noting that, despite the presence of exigent circumstances, seeking a warrant would have been "preferable."[231] The court nevertheless described the defendant's privacy interest in his location as "dubious at best,"[232] but ultimately, rendered no firm decision on the issue, finding in the end, "at most … a limited intrusion into [the defendant's] privacy interests."[233]

Either way, there is no statutory remedy against the government to suppress information improperly disclosed by a communications provider under § 2702, and injured parties are limited to a private action against the provider.[234] Therefore, if the Fourth Amendment is not applicable, evidence obtained under § 2702(c)(4) cannot be suppressed as the product of an improper search, even if a court finds the emergency conditions of that section have not been met.[235]

Courts may find that the short-term, real-time tracking of a cellphone in a public place, using GPS location data held by a cellular provider is not subject to the protections of the Fourth Amendment,[236] in particular when an arrest warrant has previously issued.[237] Regardless, exigent circumstances may justify such tracking to locate suspected criminals and also permit disclosure of the data by cell service providers under the § 2702(c)(4) emergency provision.[238]

---

[228] United States v. McHenry, 849 F.3d 699, 706 (8th Cir. 2017); *Sauceda*, 2017 WL 4676606, at *13.

[229] *Gilliam*, 842 F.3d at 804 n.2.

[230] United States v. Caraballo, 831 F.3d 95, 103, 105 (2d Cir. 2016).

[231] *Id.* at 105 n.9 (suggesting that officers both seek a warrant and ask the cellphone provider to "apply[] its emergency process.").

[232] *Id.* at 105.

[233] *Id.* at 106.

[234] United States v. Beckett, 369 Fed. App'x. 52, 55–56 (11th Cir. 2010); 18 U.S.C § 2707(a); § 2708.

[235] *See* People v. Moorer, 959 N.Y.S.2d 868, 875–76, 879 (Co. Ct. 2013).

[236] *See, e.g.*, United States v. Riley, 858 F.3d 1012, 1017–18 (6th Cir. 2017) (per curiam).

[237] *See, e.g.*, United States v. Sauceda, No. 4:16-CR-40083-01-KES, 2017 WL 4676606, at *9–10 (D.S.D. Sept. 27, 2017).

[238] *See, e.g.*, United States v. Andrews, 381 F. Supp. 3d 1044, 1063 (D. Minn. 2019).

IV. DISCUSSION: SHORT-TERM, REAL-TIME TRACKING OF CELLPHONES UNDER § 2702(C)(4) SHOULD CONSTITUTE A SEARCH

If the discussion above appears convoluted, that sentiment is shared by the courts.[239] From the inconsistencies in the case law, however, several general principles emerge: (1) the longer tracking persists, the more likely it is to constitute a search;[240] (2) tracking that is "retrospective" is more likely to constitute a search than tracking that is live or prospective;[241] (3) when tracking crosses out of public areas and provides information from inside a space, such as the home, that is protected by an expectation of privacy society has traditionally recognized as reasonable, the tracking is likely to constitute a search;[242] (4) where a valid arrest warrant has been issued, a defendant may lose any reasonable expectation of privacy in his or her physical location, regardless of the foregoing factors;[243] (5) when tracking is found to be constitutionally sufficient, the emergency provision contained in § 2702(c)(4) generally permits service providers to disclose a subscriber's GPS location data to police;[244] (6) where the Fourth Amendment does not apply, the SCA does not independently provide for suppression of GPS data improperly obtained by the government.[245]

These observations, however, do not provide direct guidance on the proper constitutional treatment of short-term, real-time GPS tracking pursuant to § 2702(c)(4). In this vacuum, some lower courts have found that such tracking does not constitute a search,[246] and, alternatively, that if a search had occurred, it might be justified by the exigent circumstances exception to the warrant requirement.[247] These holdings, however, should be reconsidered; even short-term GPS tracking of a cellphone might

---

[239] *See* United States v. Howard, 426 F. Supp. 3d 1247, 1254 (M.D. Ala. 2019) (noting that in analyzing electronic surveillance after *Carpenter*, district "courts like this one are left to decide just how long is a piece of string.").

[240] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (plurality opinion); United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., with Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring).

[241] *Carpenter*, 138 S. Ct. at 2218; *Howard*, 426 F. Supp. 3d at 1257.

[242] *Carpenter*, 138 S. Ct. at 2217; *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); Kyllo v. United States, 533 U.S. 27, 40 (2001); United States v. Karo, 468 U.S. 705, 709–10, 714 (1984); *Howard*, 426 F. Supp. 3d at 1257.

[243] United States v. Riley, 858 F.3d 1012, 1020 (6th Cir. 2017) (Boggs, J., concurring) (per curiam); United States v. Sauceda, No. 4:16-CR-40083-01-KES, 2017 WL 4676606, at *10 (D.S.D. Sept. 27, 2017).

[244] *See, e.g.*, United States v. Andrews, 381 F. Supp. 3d 1044, 1063 (D. Minn. 2019).

[245] People v. Moorer, 959 N.Y.S.2d 868, 876, 879 (Co. Ct. 2013).

[246] *Howard*, 426 F. Supp. 3d at 1256–57.

[247] *Andrews*, 381 F. Supp. 3d at 1063.

violate an objectively reasonable expectation of privacy by revealing information from inside a protected space, and when tracking is performed in real time, police will be unable to predict in advance whether such a violation will occur. Moreover, without constitutional protection, defendants may lack any adequate remedy if a court later finds that no exigency existed to otherwise justify the tracking. Therefore, real-time, short-term tracking of a cellphone under § 2702(c)(4) should be considered a search and presumptively require a warrant.

A. GPS Tracking May Violate an Objectively Reasonable Privacy Expectation by Revealing Information from Inside Protected Spaces

Certain spaces, such as the home, have always received the highest Fourth Amendment protections.[248] Keeping these spaces secure from improper police intrusion accords both subjective and objectively reasonable expectations of privacy and is therefore one of the few continuous threads running through the cases above.[249] Accordingly, none of the previously cited decisions have held that tracking is permissible in any form or for any length of time, if it transmits a defendant's location from inside such a space, and for which neither a search nor an arrest warrant has been issued. Excepting short-term, live GPS tracking of cellphones from Fourth Amendment protections would expose defendants to the risk that information, which would be protected in other scenarios, will be available to law enforcement without judicial oversight,[250] thereby violating an objectively reasonable expectation of privacy.

This view is not without precedent. *Karo* found short-term, live tracking to constitute a search where the tracked object left a public road and transmitted its location from inside a residence.[251] The *Kyllo* court similarly concluded that, "[t]he Fourth Amendment's protection of the home has never been tied to … the quality or quantity of information obtained,"[252] and therefore held that using technology to gather any information that otherwise would have required "physical 'intrusion into a constitutionally protected area'" constitutes a search.[253]

---

[248] *See* Kyllo v. United States, 533 U.S. 27, 37, 40 (2001).

[249] *Id.* at 40; United States v. Karo, 468 U.S. 705, 709–10, 714 (1984); *Howard*, 426 F. Supp. 3d at 1257.

[250] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217, 2223 (2018) (plurality opinion) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)) (holding that obtaining historical CSLI requires a warrant in part because of information it might reveal from constitutionally protected paces).

[251] *Karo*, 468 U.S. at 709–10, 714.

[252] *Kyllo*, 533 U.S. at 37.

[253] *Id.* at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

With respect to cellphones in particular, Justice Sotomayor's concurrence in *Jones*, a case which itself involved real-time tracking,[254] cautioned that "even short-term" GPS monitoring might create a "comprehensive record of a person's public movements that reflects … familial, political, professional, religious, and sexual associations."[255] That this information could be collected covertly and maintained indefinitely by the government, she opined, rendered such monitoring practices particularly "susceptible to abuse" when unconstrained by judicial scrutiny.[256] This concern formed part of the basis for the Supreme Court's opinion in *Carpenter*, which held that the collection of historical CSLI required a warrant and noted that cellphones, "faithfully follow[] [their] owner[s] beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[257] These views have similarly been echoed by lower courts analyzing short-term, real-time electronic surveillance post-*Carpenter*.[258] In justifying the warrantless tracking of a truck, the *Howard* court, citing both *Carpenter* and *Karo*, noted that, unlike vehicles, "[c]ell phones follow their owners into homes and other constitutionally protected spaces."[259]

If the purpose of these prior holdings is to protect the "sanctity of the home" and similar locations from technological penetration otherwise impossible without a warrant,[260] then in a post-*Carpenter* era, courts should consider short-term, live GPS tracking of a cellphone a search, at least in those instances where the phone enters a protected space.[261] The sophistication of modern GPS technology exacerbates the potential problems in failing to do so. When *Caraballo* was decided in 2016, the court described cellphone GPS tracking as "quite precise," noting it to be accurate within "8 to 46 meters."[262] Even two years prior, however, the average smartphone's GPS could pinpoint the phone's location to within

---

[254] *Jones*, 565 U.S. at 403.

[255] *Id.* at 415 (Sotomayor, J., concurring).

[256] *Id.* at 416.

[257] Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018) (plurality opinion).

[258] United States v. Howard, 426 F. Supp. 3d 1247, 1257 (M.D. Ala. 2019).

[259] *Id.*

[260] Kyllo v. United States, 533 U.S. 27, 37 (2001).

[261] *See Implementing Carpenter*, *supra* note 82 (manuscript at 3) (suggesting a framework under which, to be protected by the Fourth Amendment after *Carpenter*, information must be made available through "digital-age" technology, must not be revealed by a "user's meaningful, voluntary choice," and must reveal an "intimate portrait of a person's life"). It is unclear whether short-term tracking under § 2702(c)(4) would meet this proposed standard. *Id.*

[262] United States v. Caraballo, 831 F.3d 95, 99 (2d Cir. 2016).

4.9 meters – sixteen feet – under ideal conditions.[263] This is at least an order of magnitude more precise than the information ascertainable from CSLI in 2018, when the Supreme Court determined that acquisition of Timothy Carpenter's location data constituted a search.[264] The Court considered that, over a long enough time, even location information accurate within a range of fifty meters to four miles could provide a sufficiently clear picture of a defendant's private activities to warrant constitutional protection.[265]

Even under less than ideal conditions, the level of accuracy now achievable with GPS is likely more than sufficient to reveal not only a person's near-precise location within a home or other protected space but also, by extension, myriad "intimate" activities as contemplated in *Kyllo*.[266] With limited additional information, police could readily determine,[267] "at what hour each night the lady of the house takes her daily sauna and bath" even more precisely than with the heat-vision camera the *Kyllo* court confronted.[268] Overall, the precision of modern GPS creates privacy concerns that surely surpass those in both *Kyllo* and *Karo*, where the Court found the officers' actions to constitute a search.[269] It is unlikely that many members of society subjectively expect police to have the unbridled authority to precisely track them between and within the constitutionally protected areas contemplated in *Carpenter*.[270] In light of the ubiquity and sophistication of cellphones and their virtual necessity to nearly every aspect of modern life, this privacy expectation is objectively reasonable.[271] The determination to allow even the possibility of such

---

[263] *GPS Accuracy*, GPS.GOV, https://www.gps.gov/systems/gps/performance/accuracy/#:~:text=For%20example%2C%20GPS%2Denabled%20smartphones,receivers%20and%2For%20augmentation%20systems [https://perma.cc/QRF7-6JBB] (Apr. 22, 2020) (official U.S. government website describing the functioning of GPS infrastructure. Noting that precision can be reduced by features such as buildings or trees in the landscape or when the device is indoors); Frank van Diggelen & Per Enge, *The World's First GPS MOOC and Worldwide Laboratory Using Smartphones*, Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation 361–69 (Tampa, Fla. Sept. 2015) (compiling worldwide GPS data from 2014, which revealed a mean accuracy of 4.9 meters).

[264] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (plurality opinion).

[265] *Id.* at 2218–19.

[266] Kyllo v. United States, 533 U.S. 27, 38–39 (2001).

[267] *See Implementing Carpenter*, *supra* note 82 (manuscript at 34) (noting that without clearer Fourth Amendment protections, the "invasiveness" of information police gather and, therefore, whether their actions constitute a search, may change based on what other information police know).

[268] *Kyllo*, 533 U.S. at 34–35.

[269] *Id.*; United States v. Karo, 468 U.S. 705, 714 (1984).

[270] *Carpenter*, 138 S. Ct. at 2217–18.

[271] *See id.* at 2220.

invasion should therefore be made by a, "neutral and detached magistrate instead of … by the officer engaged in the often competitive enterprise of ferreting out crime."[272]

Cases which have found that short-term, live tracking is not a search may have done so in part because the tracked object never transmitted information from inside a protected space prior to the defendant's arrest.[273] Further, unlike the historical CSLI in *Carpenter*, it may not be necessary to protect a defendant's real-time GPS position in exclusively public spaces because the tracking is brief, and the information gathered about the defendant's life is comparatively minimal.[274] It may therefore be tempting, as hypothesized in *Kyllo*, to fashion a standard by which only tracking that in fact reveals protected activities constitutes a search.[275] When police initiate tracking of a phone, however, they have no way of knowing whether the person to be monitored will carry the phone into a protected space.[276] This would leave police, as the *Kyllo* court noted, "unable to know in advance whether [their activities are] constitutional."[277] As cellphones so rarely leave their owners' sides, however,[278] the chances that even short-term live tracking will capture activity within a protected space is substantial.

Finally, insofar as the duration of tracking may influence whether a search has occurred,[279] little specific guidance has been provided to courts as to how much is enough to trigger Fourth Amendment protections.[280] "[T]he Fourth Amendment requires certainty,"[281] and the foregoing

---

[272] Johnson v. United States, 333 U.S. 10, 14 (1948).

[273] *See* United States v. Riley, 858 F.3d 1012, 1018 (6th Cir. 2017) (per curiam); United States v. Skinner, 690 F.3d 772, 778, 780 (6th Cir. 2012); United States v. Howard, 426 F. Supp. 3d 1247, 1257 (M.D. Ala. 2019).

[274] *Carpenter*, 138 S. Ct. at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

[275] Kyllo v. United States, 533 U.S. 27, 38–39 (2001); *see also Implementing Carpenter*, *supra* note 82 (manuscript at 28) (rejecting a "subjective approach" which would determine whether a search occurred based on whether an "[intimate] portrait has [actually] been painted" based on the information police learn).

[276] Police initiate tracking specifically *because* they do not know where a defendant is.

[277] *Kyllo*, 533 U.S. at 39; *see also Implementing Carpenter*, *supra* note 82 (manuscript at 29) (noting that determining whether a search under *Carpenter* has occurred in general, based on a retrospective look at information actually learned, would prevent police from knowing in advance whether their actions would constitute a search and prevent defendants from knowing whether a search had occurred).

[278] *See Carpenter*, 138 S. Ct. at 2218.

[279] *Implementing Carpenter*, *supra* note 82 (manuscript at 36).

[280] *Id.* (manuscript at 37).

[281] *Id.* (manuscript at 2) ("[T]he Fourth Amendment requires certainty. The police need to know what they legally can do, and the citizen needs to know what the police legally *can't* do." (emphasis in original)).

ambiguities therefore lend further credence to the position that all short-term, real-time tracking of cellphones, however defined, should constitute a search and presumptively require a warrant.[282] Such a standard respects an objectively reasonable expectation of privacy in live cellphone location data.

B. Section 2702(c)(4) Provides an Inadequate Remedy When a Court Finds No Exigency Existed

Police tracking a cellphone pursuant to a § 2702(c)(4) request often do so in order to effect the immediate arrest of a potentially dangerous subject.[283] When the emergency provision in § 2702(c)(4) and the exigency exception to the warrant requirement are held to be coextensive, any proper disclosure under the emergency provision will render a warrant unnecessary, even if a search was technically performed.[284] As such, the question of whether this form of tracking constitutes a search may often appear moot, and it may be so in many cases. Because the SCA does not provide a means of suppressing information improperly disclosed under its provisions, however,[285] when courts hold that the Fourth Amendment is not applicable, a defendant is left only with the possibility of a civil action were the court to find that police failed to meet the emergency standard in § 2702(c)(4).[286] Such a remedy is inadequate in the face of a criminal conviction.

Some of the cases that justified tracking based on exigent circumstances tacitly referenced the possibility of an underlying warrant requirement.[287] In *Sauceda*, police sought a warrant for a second phone owned by the defendant before requesting emergency location data for the tracked phone without a warrant.[288] The *Caraballo* court at one point suggested a warrant would have been "preferable,"[289] while in *Gilliam*,

---

[282] *See id.* (manuscript at 40–41) (Advocating for a near bright-line rule that a search has occurred when police use "digital technology to obtain information" previously unavailable, "and that can reveal the privacies of life." No specific discussion of short-term, live GPS tracking or the emergency provision of the SCA.).

[283] *See, e.g.*, United States v. Takai, 943 F. Supp. 2d 1315, 1317–18 (D. Utah 2013).

[284] United States v. Gilliam, 842 F.3d 801, 804 (2d Cir. 2016).

[285] 18 U.S.C §§ 2707, 2708, 2712 (respectfully, exclusive civil remedy against an entity for improper disclosure, general exclusivity of remedies, and civil remedy against the government for willful violations of the SCA).

[286] *See, e.g.*, People v. Moorer, 959 N.Y.S.2d 868, 875–76, 879 (Co. Ct. 2013).

[287] *See, e.g.*, *Gilliam*, 842 F.3d at 803–04 n.2 (2d Cir. 2016); United States v. Caraballo, 831 F.3d 95, 105 n.9 (2d Cir. 2016); United States v. Sauceda, No. 4:16-CR-40083-01-KES, 2017 WL 4676606, at *4 (D.S.D. Sept. 27, 2017).

[288] *Sauceda*, 2017 WL 4676606, at *4.

[289] *Caraballo*, 831 F.3d at 105 n.9.

GPS tracking was presumed to constitute a search.[290] At least in the latter case, this suggests the possibility that had no exigency existed to satisfy both the statutory and constitutional standards involved, a warrant would have been required.

Courts may fail to find an exigency for a variety of reasons. Whether or not an exigency exists is a fact-specific determination,[291] and courts may simply differ on this point.[292] Further, a lack of judicial oversight may permit misconduct by police and abuse of the § 2702(c)(4) emergency request process, or at least create a perverse incentive to stretch the bounds of what constitutes an exigency. The defendant in *Andrews* alleged that police lied on their emergency request to his service provider for GPS data.[293] While the court found no evidence of this,[294] if police are merely required to send a request to a cellphone company claiming exigent circumstances, the possibility exists. Justice Sotomayor voiced similar concerns over the potential for such abuses should police have unrestricted access to GPS tracking data.[295]

Where a court finds, for any reason, that no exigency existed to justify a § 2702(c)(4) request, a defendant facing 240 months in prison is unlikely to be satisfied by the chance to sue the government or a cellphone company;[296] the courts should not be either, as this remedy provides little deterrence to law-enforcement agencies against filing facially inappropriate emergency requests. Moreover, this assumes a defendant would even be able to sue the government under § 2712 for a violation of § 2702(c)(4), as the later section, by its terms, restricts only the behavior of service providers and not of the government.[297] In light of this, and perhaps unsurprisingly, Timothy Carpenter himself, facing over 100 years in prison, challenged part of the SCA on constitutional grounds and specifically sought suppression of his CSLI data.[298] Treating GPS tracking as a search would still permit waiver of the warrant requirement where a true exigency exists,[299] but it would also allow defendants to attempt to exclude evidence obtained through tracking where a court later determines

---

[290] *Gilliam*, 842 F.3d at 804 n.2.

[291] *Id.* at 804 (quoting United States v. MacDonald, 916 F.2d 766, 769 (2d Cir. 1990)).

[292] Brigham City v. Utah, 547 U.S. 398, 407 (2006) (reversing the Supreme Court of Utah based on a finding of exigent circumstances).

[293] United States v. Andrews, 381 F. Supp. 3d 1044, 1062 (D. Minn. 2019).

[294] *Id.*

[295] United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

[296] *Gilliam*, 842 F.3d at 802; 18 U.S.C. §§ 2707, 2712.

[297] 18 U.S.C. §§ 2702(a), 2712.

[298] Carpenter v. United States, 138 S. Ct. 2206, 2212–13 (2018) (plurality opinion).

[299] *See id.* at 2211.

one did not.[300] Suppression of evidence resulting from an improper search is a typical remedy for a Fourth Amendment violation and is often justified by its deterrent effect on police misconduct.[301] Eventually, police might also be less able to avoid suppression based on "good faith reliance" on § 2702(c)(4).[302]

The SCA too seems to contemplate the possibility of a remedy based upon a constitutional violation, in that the general exclusivity-of-remedies provision covers only "nonconstitutional" violations of the Act.[303] Failing to consider GPS tracking under § 2702(c)(4) a search appears to flout this purpose. Defendants are incongruously denied the ability to suppress evidence obtained based on a standard that is nearly identical to the exigent circumstances exception but that is not necessarily subject to a Fourth Amendment inquiry.[304] The need to provide defendants with an adequate remedy when the emergency standard under § 2702(c)(4) is not met further substantiates the argument that live, short-term GPS tracking of cellphones should be treated as a search.

C. Courts May Decide Not to Require a Search Warrant for GPS Tracking under § 2702(c)(4) when an Arrest Warrant Has Already Issued

Absent an exception,[305] police seeking to explore items and locations protected by the Fourth Amendment must first obtain a search warrant.[306] Both search and arrest warrants, however, issue based on a finding of probable cause.[307] Because live GPS tracking seeks only the defendant's physical location, an arrest warrant may provide sufficient grounds to initiate tracking.[308]

---

[300] *The Case for the Third-Party Doctrine*, *supra* note 44, at 581–82 ("If the police violate a reasonable expectation of privacy and no exception applies, the evidence obtained ordinarily will be suppressed and the wrongdoer may go free.").

[301] *Id.* at 581; Hudson v. Michigan, 547 U.S. 586, 591 (2006) (quoting Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 363 (1998)).

[302] *See, e.g.*, United States v. Takai, 943 F. Supp. 2d 1315, 1323–24 (D. Utah 2013) (citing United States v. Leon, 468 U.S. 897 (1984); United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012)).

[303] 18 U.S.C. § 2708. Note, however, that § 2712, which provides for an exclusive civil remedy against the government, contains no similar carveout for potential "constitutional" violations. 18 U.S.C. § 2712(a), (d).

[304] *See, e.g.*, *Takai*, 943 F. Supp. 2d 1315, 1324.

[305] Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

[306] *The Case for the Third-Party Doctrine*, *supra* note 44, at 574.

[307] *See* United States v. Riley, 858 F.3d 1012, 1020 (6th Cir. 2017) (Boggs, J., concurring) (per curiam) (quoting Payton v. New York, 445 U.S. 573, 602–03 (1980)) (arrest warrants); United States v. Beckett, 369 Fed. App'x. 52, 56–57 (11th Cir. 2010) (search warrants).

[308] *See Riley*, 858 F.3d at 1020 (Boggs, J., concurring).

As explained by the concurrence in *United States v. Riley*, when police have an arrest warrant based on probable cause and reasonable suspicion to believe that a defendant is physically located within his home, they may enter and effect an arrest without a search warrant.[309] That opinion reasoned that police should therefore be permitted the lesser intrusion of obtaining only the physical location of a defendant's cellphone, even inside a protected space, based on an arrest warrant, when they reasonably suspect the defendant to be in possession of the phone.[310] This argument is persuasive and was later adopted by the district court in *Sauceda*.[311]

It is unclear whether, in the presence of an arrest warrant, courts would find that no Fourth Amendment protections attach to the defendant's location at all,[312] or merely that the existence of an arrest warrant satisfies the Fourth Amendment's warrant requirement.[313] Regardless, if presumptively required to seek a warrant of any kind in conjunction with a § 2702(c)(4) request, police would lack the unrestricted access to GPS location data that might permit abuse of the emergency tracking process.[314]

To prevent unforeseeable intrusion into protected spaces and to provide defendants with the ability to suppress location data when the § 2702(c)(4) emergency provision is not satisfied, courts should treat the real-time, short-term GPS tracking of the cellphone of a criminal suspect as a search subject to the protections of the Fourth Amendment. Such tracking would presumptively require a search warrant unless an arrest warrant had previously been issued.[315] The *Katz* framework requires an objectively reasonable expectation of privacy based on societal standards.[316] These standards, however, may change to demand greater protections as tracking technology evolves.[317] Perhaps the best evidence

---

[309] *Id.*

[310] *Id.*

[311] United States v. Sauceda, No. 4:16-CR-40083-01-KES, 2017 WL 4676606, at *10 (D.S.D. Sept. 27, 2017).

[312] *See Riley*, 858 F.3d at 1020 (Boggs, J., concurring) ("[O]fficers … may track that cellphone's location in order to facilitate the execution of the [arrest] warrant, without implicating the Fourth Amendment.").

[313] *See* Payton v. New York, 445 U.S. 573, 603 (1980) ("for Fourth Amendment purposes, an arrest warrant founded on probable cause implicitly carries with it the limited authority to enter a dwelling…").

[314] United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

[315] *See* Katz v. United States, 389 U.S. 347, 353 (1967).

[316] *Id.* at 361 (Harlan, J., concurring).

[317] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (plurality opinion); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *see also Implementing Carpenter*, *supra* note 82 (manuscript at 8) ("[T]he question is whether technological

of this is the disclosure restrictions placed on providers by the SCA itself, the plain purpose of which was to prevent overreaching intrusion by the government with regard to electronically stored information.[318] Insofar as congressional representatives execute the will of the electorate, the SCA safeguards enacted these changing societal expectations based on a flexible standard that "advance[s] with … technology."[319]

V. CONCLUSION

In its Fourth Amendment decisions through *Carpenter*, the Supreme Court narrowed the scope of the third-party doctrine while expanding constitutional protections for electronically stored information commensurate with the evolution of cellphone technology and societal expectations of privacy.[320] The concurrences in *Jones* heralded a binding opinion in *Carpenter* six years later,[321] and while the question of whether constitutional privacy protections will swell to categorically encompass the short-term, live tracking of cellphones under § 2702(c)(4) remains unanswered, history seems bound to repeat itself. Whether such protections might similarly be founded on a dissenting opinion, such as the principles of bailment described by Justice Gorsuch in *Carpenter*,[322] or on other grounds is unclear.

Regardless, when police engage in the real-time tracking of a suspect's cellphone, based on an emergency request under § 2702(c)(4), courts should presumptively require a warrant, even if the tracking is limited in time. This approach still allows for situations in which a search warrant may not be required, such as when a true exigency exists or when police possess a valid warrant for the defendant's arrest.[323] Absent such mitigating circumstances, however, attaching constitutional protections to this type of monitoring enhances safeguards for a defendant's constitutionally protected activities,[324] serves the fundamental goals of the SCA,[325] and provides a meaningful remedy when police get it wrong.[326]

---

change has rendered obsolete a past expectation of a practical limit on government power.").

[318] S. REP. NO. 99-541, at 5 (1986).

[319] *Id.*

[320] *See Implementing Carpenter*, *supra* note 82 (manuscript at 1, 8).

[321] *Carpenter*, 138 S. Ct. at 2215, 2217.

[322] *Id.* at 2270 (Gorsuch, J., dissenting).

[323] *See* United States v. Riley, 858 F.3d 1012, 1020 (6th Cir. 2017) (Boggs, J., concurring) (per curiam) (arrest warrant); United States v. Takai, 943 F. Supp. 2d 1315, 1322–23 (D. Utah 2013) (exigency).

[324] *See* Kyllo v. United States, 533 U.S. 27, 38 (2001).

[325] S. REP. NO. 99-541, at 5 (1986).

[326] *Contra* People v. Moorer, 959 N.Y.S.2d 868, 875–76, 879 (Co. Ct. 2013).

Managing the balance of privacy and security in a free society is a precarious and constantly evolving challenge and one that is ultimately left to the voting public. The present issue is ripe for litigation, and the Supreme Court should avail itself of any opportunity to further expand and standardize Fourth Amendment protections for electronically stored location data.