PRIVACY IN THE DUMPS: ANALYZING CELL TOWER DUMPS UNDER THE FOURTH AMENDMENT

Emma Lux*

INTRODUCTION

In 2010, the FBI sought to arrest the "High Country Bandits," two men engaged in a rural bank robbing spree.[1] Law enforcement could not see the Bandits' faces in surveillance videos, but a witness saw one of them use a cell phone during a robbery.[2] To identify the suspects, the FBI sought four "cell tower dumps" from cell carriers, collections of the phone numbers "from all the devices that connected to a cell site during [the] particular interval"[3] in which four of the robberies occurred.[4] In the case of the High Country Bandits, the cell tower dumps returned the cell-site location information (CSLI) of 150,000 cell phone numbers,[5] only two of which—the Bandits' numbers—appeared near all four robberies.[6]

This type of warrantless governmental collection of cell tower dump location information is becoming ubiquitous,[7] in part because the Supreme Court in *Carpenter v. United States*[8] declined to address whether it triggers Fourth Amendment protection.[9] The *Carpenter* Court found that governmental acquisition of "seven days of [historical cell-site location information] constitutes a Fourth Amendment search."[10] But tower dumps are distinct from the *Carpenter* long-term historical CSLI in two main ways. First, cell tower dumps collect cell-site location

---

* Emma Lux is a *juris doctor* candidate at the Georgetown University Law Center, with expected graduation in 2021. She is a Featured Online Contributor for Volume 57 of the *American Criminal Law Review*.

[1] Nate Anderson, *How "Cell Tower Dumps" Caught the High Country Bandits—And Why It Matters*, ARS TECHNICA (Aug. 29, 2013, 8:00 AM), https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters/.

[2] *Id.*

[3] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[4] Anderson, *supra* note 1.

[5] *Id.*

[6] Stephen Henderson, *A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 TEX. L. REV. 28, 55 (2016).

[7] *See, e.g.*, Zack Whittaker, *T-Mobile Quietly Reported A Sharp Rise in Police Demands for Cell Tower Data*, TECHCRUNCH (July 12, 2019, 1:23 PM), https://techcrunch.com/2019/07/12/t-mobile-cell-tower-government-demands/ (describing how the number of government tower dump requests increased 27 percent from 2017 to 2018).

[8] *Carpenter*, 138 S. Ct. at 2206.

[9] *Id.* at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us [including] 'tower dumps.'").

[10] *Id.* at 2217 n.3. A Fourth Amendment search occurs, *inter alia*, when the government invades an individual's reasonable expectation of privacy. *See, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

information not from one person,[11] but from hundreds[12] or thousands[13] of people. Second, because tower dump CSLI typically spans only several hours[14] or even minutes,[15] the amount of CSLI police acquire for any given individual captured in the tower dump is likely less than the 127 days of CSLI from one individual that law enforcement obtained in *Carpenter*.[16]

Nonetheless, tower dumps still implicate massive amounts of user data[17] and trigger privacy concerns[18] that potentially implicate the Fourth Amendment. Of the lower courts that have considered whether individuals have a reasonable expectation of privacy in cell tower dump CSLI, many have found that they do not.[19] But most of those cases pre-date *Carpenter* and do not account for its reasoning,[20] and most post-*Carpenter* lower courts have not yet reached the merits of the issue.[21]

As a result, this contribution seeks to guide future courts deciding whether to permit warrantless governmental acquisition of cell tower

---

[11] *C.f. Carpenter*, 138 S. Ct. at 2212 (describing how the government used CSLI to track an individual's location for an extended period of time).
[12] Mason Kortz & Chris Bavitz, *Cell Tower Dumps*, 63 BOSTON BAR J. 27, 28 (2019).
[13] *See, e.g.*, Anderson, *supra* note 1.
[14] *See, e.g.*, *In re* U.S. ex. rel. Order Pursuant to 18 USC Section 2703(d), 930 F. Supp. 2d 698, 699 (S.D. Tex. 2012) (describing a cell tower dump that lasted two hours); United States v. James, No. 18-cr-216, 2018 WL 6566000, at *2 (D. Minn. Nov. 26, 2018) (describing multiple cell tower dumps lasting "approximately ninety-minute[s]" each).
[15] *See, e.g.*, *In re* Search of Cellular Telephone Towers, 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013) (describing a cell tower dump that lasted five minutes).
[16] *Carpenter*, 138 S. Ct. at 2212 (describing how the government collected "12,898 location points cataloging [the defendant's] movements over 127 days—an average of 101 data points per day"). *See also* Kortz & Bavitz, *supra* note 12, at 28 (describing how police obtain less information for any given individual during a cell tower dump than during a long-term collection of historical CSLI).
[17] *See, e.g.*, *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d at 770 (describing how cell tower dumps collect "hundreds, or even thousands, of telephone numbers for [the relevant] time period"). Cell tower dumps collect location information that is automatically created by cell phones approximately every seven seconds, when the cell phone connects to nearby phone towers. Henderson, *supra* note 6, at 29 n.5.
[18] Kortz & Bavitz, *supra* note 12, at 28. (describing how "tower dumps implicate the privacy of far more people than access to [the long-term] historical CSLI" at issue in *Carpenter*).
[19] *See, e.g.*, *In re* Application of the United States for an Order Pursuant to 18 USE 2703(c)(1), (d), 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014); *In re* United States for an Order Pursuant to 18 USC 2703(d), 2017 WL 6368665, at *1 (E.D. Mich. Dec. 12, 2017).
[20] *See, e.g.*, *In re US for an Order Pursuant to 18 USC 2703(d)*, 2017 WL 6368665 at *1 ("[W]hile the Supreme Court has granted certiorari [in *Carpenter*], at present the law in this Circuit is that [cell tower dump CSLI] does not require a showing of probable cause.").
[21] *See, e.g.*, United States v. James, No. 18-cr-216, 2018 WL 6566000, at *6 (D. Minn. Nov. 26, 2018) (declining to reach the merits of whether a cell tower dump is a search since the good faith doctrine would have permitted the pre-*Carpenter* search regardless). *See also* United States v. Pendergrass, No. 1:17-CR-315-LMM-JKL, 2018 WL 7283631, at *13 (N.D. Ga. Sept. 11, 2018) (same).

dump CSLI. Part I argues that cell tower dumps should constitute searches under the reasoning of *Carpenter*[22] and Justice Alito's concurrence in *Jones*[23] because governmental acquisition from cell carriers of tower dump CSLI violates an individual's reasonable expectation of privacy. Part II then proposes ways in which courts can minimize privacy intrusions into innocent individuals' tower dump CSLI under either the Fourth Amendment[24] or the Stored Communications Act.[25]

I. THE FOURTH AMENDMENT AND TOWER DUMP CELL-SITE LOCATION INFORMATION

In *Katz v. United States*,[26] the Supreme Court held that a Fourth Amendment search occurs when the government invades an individual's subjective expectation of privacy that society accepts as reasonable.[27] Such searches generally require a warrant supported by probable cause.[28]

This Part describes and analyzes the two lines of cases governing the issue of whether cell tower dumps are *Katz* searches, the public location monitoring cases[29] and third-party doctrine cases.[30] It argues that tower dumps violate reasonable expectations of privacy because they allow the government to do what society otherwise would not expect it could or would: cheaply, effortlessly, and retroactively gather with precise detail the location information of all individuals near any crime scene.[31]

---

[22] *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) ("As technology has enhanced the [g]overnment's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'") (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

[23] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (explaining that long-term GPS location monitoring violates a reasonable expectation of privacy because "society's expectation has been that law enforcement agents and others would not—and[,] in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period").

[24] U.S. CONST. amend. IV. *See also* Katz v. United States, 389 U.S. 347, 358 (1967) (describing the requisite probable cause standard generally required when a search occurs).

[25] Stored Communications Act, Pub. L. No. 99–508 (1986). *See* 18 U.S.C. § 2703(d) (2018).

[26] *Katz*, 389 U.S. at 347 (1967).

[27] *Id.* at 361 (Harlan, J., concurring) (describing how the man shut the phone booth door to protect his conversation, establishing a subjective expectation of privacy that society accepts as legitimate). *See also* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 316 (2012) (describing the reasonable expectation of privacy test).

[28] *Katz*, 389 U.S. at 357.

[29] *See infra* Section I.A.

[30] *See infra* Section I.B.

[31] *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (describing how the Fourth Amendment protects the founding era expectation of privacy against novel technological incursions).

A. *The Reasonable Expectation of Privacy Analysis for Public Location Information*

The first line of cases governing the tower dump analysis concerns whether individuals have legitimate expectations of privacy in public location information under *Katz*. Justice Harlan's concurrence in *Katz* suggested that information "in the open" that the public could hear or see "would not be protected."[32] As a result, in *United States v. Knotts*,[33] the Court held that individuals did not have an expectation of privacy in short-term location information which police collected in real-time using beeper monitoring technology.[34] Because the defendant "voluntarily conveyed [his location] to anyone who want[ed] to look,"[35] and the information would have been possible to obtain prior to the advent of beeper technology by merely following the individual,[36] the collection of the location information was not a search.[37]

A majority of the Court, however, found that individuals have a reasonable expectation of privacy in long-term public location information in *United States v. Jones*.[38] There, law enforcement's use of GPS technology to monitor the public location of a car for twenty-eight days violated a reasonable expectation of privacy because law enforcement could not practically have engaged in widespread, extensive long-term tracking prior to the advent of GPS technology. [39]

Most recently, the Supreme Court extended the reasoning of *Jones* to long-term historical CSLI in *Carpenter*, finding that individuals have a reasonable expectation of privacy in seven days of historical CSLI.[40] The Court found that cell-site location information, like the GPS data in *Jones*, [41] triggered the Fourth Amendment since it permitted law enforcement to make "novel" [42] incursions into individual privacy. Specifically, before cell companies engaged in routine location monitoring, law enforcement could not casually obtain "detailed,

---

[32] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
[33] United States v. Knotts, 460 U.S. 276 (1983).
[34] *Id.* at 281–82.
[35] *Id. See also* United States v. Karo, 468 U.S. 705, 730 (1984) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.") (quoting *Katz*, 389 U.S. at 347).
[36] *Knotts*, 460 U.S. at 282 ("Visual surveillance from public places along [the defendant's] route…would have sufficed to reveal all of these facts to the police.").
[37] *Id.*
[38] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring). *See also id.* at 415 (Sotomayor, J., concurring) (agreeing with Justice Alito's conclusion that there is a reasonable expectation of privacy in long-term public location information produced by GPS technology).
[39] *Id.* at 430.
[40] Carpenter v. United States, 138 S. Ct. 2206, 2217, n.3 (2018).
[41] *Jones*, 565 U.S. at 430.
[42] *Carpenter*, 138 S. Ct. at 2217.

encyclopedic," [43] and precise records of an individual's historical movements, but would have had to rely on word of mouth and fallible witnesses.[44] Additionally, the Court found that long-term monitoring of historical CSLI implicates additional privacy concerns since it generates a comprehensive record that can reveal the tracked individual's "familial, political, professional, religious, and sexual associations."[45]

Cell tower dumps should qualify as searches under *Carpenter* and *Jones*. While the *Carpenter* Court found that the government's warrantless acquisition of "seven days of [historical] CSLI" violated an individual's reasonable expectation of privacy,[46] it explicitly left open the question of whether governmental acquisition of historical CSLI for shorter periods of time,[47] like tower dump CSLI,[48] also triggers Fourth Amendment protections. Recall that during cell tower dumps, law enforcement usually obtains only several hours,[49] or even minutes,[50] of an individual's historical CSLI. As a result, many tower dumps do not inherently create "an all-encompassing record," of an individual's location that reveals her "'familial, political, professional, religious, and sexual associations.'"[51]

However, the short-term nature of the average cell tower dump should not toll the death knell for Fourth Amendment protection of tower dump CSLI. [52] Both *Carpenter* and *Jones* were concerned not only with protecting individuals from governmental collection of long-term location information,[53] but also with protecting individuals from technological advancements encroaching on founding-era understandings of privacy

---

[43] *Id.* at 2216.
[44] *Id.* at 2210 (describing how historical CSLI "present[s] even greater privacy concerns than the GPS monitoring" in *Jones*, because CSLI gives the government "near perfect surveillance" and allows it to "travel back in time to retrace a person's whereabouts").
[45] *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).
[46] *Id.* at 2217 n.3.
[47] *Id.* ("[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").
[48] *Id.* at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps[.]'").
[49] *See, e.g.*, *In re* U.S. ex. rel. Order Pursuant to 18 USC Section 2703(d), 930 F. Supp. 2d 698, 699 (S.D. Tex. 2012).
[50] *See, e.g.*, *In re* the Search of Cellular Telephone Towers, 945 F. Supp. 2d 769, 769–70 (S.D. Tex. 2013).
[51] *Carpenter*, 138 S. Ct. at 2208 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
[52] *See, e.g.*, *In re United States ex. rel. Order Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d at 701 (finding that a warrantless tower dump implicated the Fourth Amendment prohibition on unreasonable searches). *See also* United States v. Jones, 565 U.S. 400, 415 (Sotomayor J., concurring) (implying that "even short-term [GPS] monitoring" might implicate the Fourth Amendment).
[53] *See Carpenter*, 138 S. Ct. at 2208; *Jones*, 565 U.S. at 430 (Alito, J., concurring).

rights.[54] For example, a majority of the Court found a search in *Jones* when the government acquired twenty-eight days of an individual's GPS location information since, prior to the advent of GPS technology, "society's expectation has been that law enforcement agents . . . would not—and . . . simply could not—secretly monitor and catalogue every single movement of an individual's car for a long period."[55]

For cell tower dumps, unlike in *Jones*, it is not the length of cell tower dumps that expand law enforcement's investigative abilities—police frequently trailed individuals for short periods to monitor their locations prior to the advent of tower dump CSLI.[56] Rather, cell tower dump CSLI expands governmental capabilities since prior to the advent of the technology, police could not cheaply and effortlessly access a precise,[57] historical record[58] of hundreds of individuals[59] near any given crime scene.[60] Traditionally, police would have had to either track a suspect in real time[61] or rely on the fallible memory of the village snoop to determine who was near the scene of a crime.[62] While society accepted it as reasonable for police to engage in the type of "limited"[63] short-term tracking that occurred in *Knotts*,[64] cell tower dump technology vastly expands governmental capabilities.

---

[54] *See Carpenter*, 138 S. Ct. at 2214 (explaining that the Court guards against advancements in technology that "enhance[] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes"); *Jones*, 565 U.S. at 428 (Alito, J., concurring); *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001) (explaining that the Fourth Amendment "assure[s] preservation of that degree of privacy against government that existed" at the founding).

[55] *Jones*, 565 U.S. at 430 (Alito, J., concurring).

[56] *See, e.g.*, United States v. Knotts, 460 U.S. 270, 282.

[57] Tower dump CSLI today is even more accurate than the historical CSLI at issue in *Carpenter*. *Compare Carpenter*, 138 S. Ct. at 2218 (describing how the historical CSLI there only placed the defendant within "a wedge-shaped sector ranging from one-eighth to four square miles") *with* Brian Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 4 (2013) (describing how cell tower CSLI can accurately locate individuals "within a few hundred yards").

[58] *C.f. Knotts*, 460 U.S. at 282 (describing how police had to follow the suspect in real-time to collect the location information).

[59] Kortz & Bavitz, *supra* note 12, at 28.

[60] *C.f. Jones*, 565 U.S. at 429 ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.").

[61] *See Knotts*, 460 U.S. at 282.

[62] *Carpenter*, 138 S. Ct. at 2219. *See also* United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (2010) (Kozinski, J., dissenting) (explaining that, while individuals could previously disguise themselves to hide their public movements, "there's no hiding from the all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never get confused and never lose attention").

[63] *Carpenter*, 138 S. Ct. at 2215 (describing the "rudimentary" technology at issue in *Knotts* which made only "'limited use'" of beeper signals) (quoting *Knotts*, 460 U.S. at 284).

[64] *Knotts*, 460 U.S. at 284.

These factors should be sufficient, even absent long-term location monitoring, to find that tower dump CSLI triggers the Fourth Amendment's warrant requirement. The *Jones* concurrence that garnered a majority made governmental expansion of investigative capabilities the main consideration when determining whether location monitoring is a search.[65] Additionally, prohibiting warrantless searches of short-term tower dump CSLI avoids creating an end-run around *Carpenter* in which law enforcement could warrantlessly "collect just under the constitutional line to avoid a search occurring, and then come back the next day and do it again."[66]

B. *The Third-Party Doctrine*

If a court does find a reasonable expectation of privacy in cell tower CSLI, the third-party doctrine[67] should not bar protection of that information. The third-party doctrine describes a series of cases which held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[68] For example, in *Smith v. Maryland*, the Court found that individuals do not have a reasonable expectation of privacy in telephone numbers they dial because they "voluntarily convey[]" the information to the phone company.[69]

Carpenter, however, held that the third-party doctrine does not apply to seven days of historical CSLI.[70] The Court reasoned that, unlike the *Smith* individual who voluntarily disclosed phone numbers via the "affirmative act" of dialing,[71] cell phone users do not voluntarily share their cell-site location information with cell carriers because location monitoring is inherent to their usage and carrying a mobile phone is essential to modern life.[72] Additionally, the *Carpenter* Court reasoned that long-term, historical CSLI, with the potential to provide an "intimate window into a person's life . . ." implicated greater privacy interests than the telephone numbers conveyed to the phone company in *Smith*.[73]

By the same reasoning, the third-party doctrine should not apply to tower dump CSLI, which is created in the same manner as the historical CSLI at issue in *Carpenter*.[74] Thus, tower dump CSLI is not voluntarily

---

[65] *See Jones*, 565 U.S. at 429 (Alito, J., concurring). *C.f. id.* at 415 (Sotomayor, J., concurring) (describing how long-term tracking might implicate additional privacy incursions due to the patterns of life such tracking reveals, but not garnering a majority vote).
[66] ORIN S. KERR, THE DIGITAL FOURTH AMENDMENT (forthcoming).
[67] *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).
[68] *Smith*, 442 U.S. at 743–44.
[69] *Id.* at 744.
[70] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[71] *Id.* at 2220.
[72] *Id.* at 2219.
[73] *Id.* at 2217. *See Smith*, 442 U.S. at 742.
[74] Kortz & Bavitz, *supra* note 12, at 29.

shared since cell phones are indispensable to modern life and users cannot meaningfully control when location data is collected.[75] Additionally, even if tower dump CSLI is arguably less invasive than long-term CSLI because it provides less information about an individual's whereabouts,[76] it is unlike the "limited" technology at issue in *Smith*.[77] "[E]ven short-term" CSLI can be "'store[d] [and] efficiently mined . . . for information years into the future.'"[78]

II. PROTECTING INNOCENT BYSTANDERS' DIGITAL INFORMATION

Recall that the FBI's pursuit of the High Country Bandits returned 150,000 phone numbers, 149,998 of which belonged to innocent individuals.[79] Because cell tower dumps implicate massive amounts of user data,[80] judges should also rely on either the Fourth Amendment's warrant requirements [81] or judicial discretion under the Stored Communications Act (SCA)[82] to protect innocent Americans' CSLI.

For courts that find a reasonable expectation of privacy in the cell tower dump context,[83] the Fourth Amendment and Federal Rules of Criminal Procedure[84] should impose some protections for innocent digital bystanders whose data may be swept up in a tower dump. The Supreme Court has found that "[a] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person" [85] under the Fourth Amendment. Since most individuals in a cell tower dump inevitably have nothing to do with the crime under investigation other than the fact that they happened to be nearby,[86] it will likely be difficult for the government to establish probable cause to conduct tower dumps indiscriminately.[87] Additionally, the Federal Rules of Criminal Procedure require that the government notify the individual whose information has been searched

---

[75] Owsley, *supra* note 57, at *5 (describing how cell phones automatically connect to cell carriers approximately every seven seconds).
[76] Kortz & Bavitz, *supra* note 12, at 28.
[77] *See Smith*, 442 U.S. at 742.
[78] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).
[79] Anderson, *supra* note 1.
[80] Kortz & Bavitz, *supra* note 12, at 89.
[81] Katz v. United States, 389 U.S. 347, 357 (1967) (holding that a warrant supported by probable cause is generally necessary for a search to be reasonable).
[82] Stored Communications Act, Pub. L. No. 99–508 (1986). *See* 18 U.S.C. § 2703(d) (2018).
[83] *See supra* Part I (arguing that there is a reasonable expectation of privacy in tower dump CSLI).
[84] FED. R. CRIM. P. 41.
[85] Ybarra v. Illinois, 444 U.S. 85, 86 (1979).
[86] *See* Anderson, *supra* note 1.
[87] Owsley, *supra* note 57, at 45 (noting that the requirement to "satisfy[] [the] probable cause standard" should pose the first hurdle for law enforcement seeking tower dump CSLI).

pursuant to a warrant.[88] As one commentator noted, Congress would also be wise to add additional threshold requirements for governmental acquisition of tower dump CSLI, as it did in the Wiretap Act for wiretap surveillance.[89]

For courts that do not find a reasonable expectation of privacy in tower dump CSLI, the government may technically acquire the information under the SCA with a lesser showing than probable cause.[90] However, courts should use their discretion under the SCA[91] to minimize data intrusions given the privacy interests at stake. The SCA states that "a court order . . . *may* be issued" when the government shows "specific and articulable facts" that records are "relevant" to an ongoing investigation.[92] The Third Circuit found that the language "may be issued" grants magistrate judges discretion to require probable cause for a tower dump SCA application.[93] The Southern District of New York similarly relied on the same discretionary language in the SCA to require additional showings from the government before granting its application for a tower dump.[94] There, the court required the government to provide "a protocol to address how the Government will handle" innocent third-party information, as well as a "more specific justification" for the requested time period.[95] Measures like these help balance privacy interests against

---

[88] FED. R. CRIM. P. 41(f)(1)(C) (requiring that an officer executing a search warrant must "give a copy of the warrant and a receipt for the property taken to the person from whom…the property was taken"); *c.f.* Owsley, *supra* note 57, at 46–47 (explaining that when law enforcement obtain cell tower dumps outside the warrant process, the users whose data they access are not inherently informed).

[89] *See* Owsley, *supra* note 57, at 45–46 (suggesting that Congress add safeguards for governmental acquisition of tower dump CSLI, including requirements for threshold showings beyond probable cause, data intrusion minimization techniques, and notification for affected users). *See also* United States v. Jones, 565 U.S. 400, 429–30 (2012) (explaining that "[in] circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative").

[90] The Stored Communications Act allows the government to obtain stored electronic records from third-party providers. 18 U.S.C. § 2703(d) (2018) (requiring that the government offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of [the records] sought[] are relevant to an ongoing criminal investigation"). Courts and commentators have described this standard as "an intermediate one that is less stringent than probable cause." *See, e.g.*, Owsley, *supra* note 57, at 16.

[91] *In re* the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 315–17 (3d Cir. 2010) (quoting § 2703(d)).

[92] § 2703(d) (emphasis added).

[93] *In re the Application of the United States of America for an Order Directing*, at 319 (explaining that § 2703, by its plain language, "gives the [magistrate judge] the option to require a warrant showing probable cause").

[94] *In re* Application of the United States of America for an Order Pursuant to 18 USE 2703(c)(1), (d), 42 F. Supp. 3d. 511, 519 (S.D.N.Y. 2014).

[95] *Id. See also In re* the Search of Cellular Telephone Towers, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) (requiring, *inter alia*, that "any and all original records [of tower dump CSLI] and copies…determined to be not relevant" are returned to cell service providers).

governmental interests, even if the court does not believe individuals' privacy interests in tower dump CSLI are sufficient to trigger Fourth Amendment protection.[96]

CONCLUSION

Cell phones are mandatory to meaningful participation in modern life[97] and cell towers automatically record their location approximately every seven seconds.[98] As a result, third-party companies have been "amassing huge, ready-made databases of where we've all been."[99] The databases of cell carriers in particular have proven to be a valuable resource of CSLI for the government to "efficiently min[e]"[100] via tower dumps to identify criminals like the High Country Bandits.[101] But law enforcement's warrantless acquisition from cell carriers of tower dump CSLI potentially implicates the Fourth Amendment. Since the technology vastly expands the government's ability to intrude on society's reasonable expectations of privacy,[102] courts should find that governmental acquisition of tower dump CSLI is a search under *Carpenter*[103] and Justice Alito's opinion in *Jones*.[104] Finally, courts should protect against indiscriminate privacy incursions on innocent individuals, whether those protections derive from the Fourth Amendment[105] or the Stored Communications Act.[106]

---

[96] *See, e.g.*, *In re Application of the U.S.*, 42 F. Supp. 3d. at 519 (declining to find a search, but requiring additional protections for user privacy).
[97] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2017) ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.'") (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
[98] Owsley, *supra* note 57, at 5.
[99] United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, J., dissenting).
[100] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).
[101] Anderson, *supra* note 1.
[102] Kortz & Bavitz, *supra* note 12, at 28.
[103] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[104] *Jones*, 565 U.S. at 430 (Alito, J., concurring).
[105] U.S. CONST. amend. IV. *See also* Katz v. United States, 389 U.S. 347, 358 (1967) (describing the requisite probable cause standard generally required when a search occurs).
[106] Stored Communications Act, Pub. L. No. 99–508 (1986). *See* 18 U.S.C. § 2703(d) (2018).