Journal of Law & Commerce
Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

NOTES

THIRD-PARTY PRIVACY INTERESTS IMPLICATED BY CELL TOWER DUMPS AND THE INEFFICACY OF THE WARRANT REQUIREMENT TO PROTECT THEM: POST-*CARPENTER* JUDICIAL AND STATUTORY REMEDIES

Alexander Dettwyler

NOTES

THIRD-PARTY PRIVACY INTERESTS IMPLICATED BY CELL TOWER DUMPS AND THE INEFFICACY OF THE WARRANT REQUIREMENT TO PROTECT THEM: POST-*CARPENTER* JUDICIAL AND STATUTORY REMEDIES

Alexander Dettwyler[*]

I. ABSTRACT

While some forms of cellular data collection[1] are recognized as Fourth Amendment searches requiring a warrant supported by probable cause, the Supreme Court has not ruled on whether cellular tower dumps[2] ("tower dumps") should be accorded the same status. The reasoning underlying the 2018 *Carpenter*[3] decision makes it doubtful that the Court would answer that question in the affirmative if presented with it.

In most jurisdictions, the Government is able to obtain a court order—pursuant to a provision of the Stored Communications Act ("SCA")[4]—compelling a wireless carrier to provide it with a tower dump. These court

---

[*] Alexander Dettwyler is a student at University of Pittsburgh School of Law (J.D. 2022). The author thanks Judge Lisa Lenihan, whose prescient interest in the Fourth Amendment brought about this Article, and Jean Yesudas, whose friendship made finishing it possible.

[1] Namely, the collection of long-term Cell Site Location Information ("CSLI") that is particularized to an individual. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("[A]n individual maintains a legitimate expectation of privacy in the record of [their] physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.").

[2] Defined *infra* Section II.

[3] *See Carpenter*, 138 S. Ct. at 2216–20.

[4] Specifically, 18 U.S.C. § 2703(d).

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

orders may be obtained with a factual showing less than probable cause.[5] The consequences of a tower dump that places the *suspect* of an investigation near the scene of a crime require little explanation.[6] Less obvious are the privacy implications for the potential thousands of innocent third parties whose information is furnished to the Government in the course of a single tower dump.[7]

Brian Owsley, a former United States Magistrate Judge and DOJ trial attorney, has written extensively on this topic. In analyzing the privacy implications of tower dumps, he argues that:

> Based on the Fourth Amendment and developing case law, requests for cell tower dumps should not be handled through applications pursuant to § 2703. The provision of location information invades numerous individuals' privacy rights. . . . [R]equests for access to such information should be filed pursuant to Rule 41 of the Federal Rules of Criminal Procedure. Such a warrant must satisfy the probable cause standard based on the totality of the circumstances.[8]

---

[5] *Id.* ("A court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."); *see also In re* Application of the U.S. for an Ord. Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to the Gov't, 620 F.3d 304, 315 (3d Cir. 2010) [hereinafter *In re* Third Cir. Application] ("[T]he legislative history provides ample support for the proposition that the standard is an intermediate one that is less stringent than probable cause. . . . the SCA does not contain any language that requires the Government to show probable cause as a predicate for a court order under § 2703(d).").

[6] But just in case, *see infra* note 17.

[7] *See* Emma Lux, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. ONLINE 109, 109–10 (2020) ("[C]ell tower dumps collect cell-site location information not from one person, but from hundreds or thousands of people. . . . [They] implicate massive amounts of user data and trigger privacy concerns that potentially implicate the Fourth Amendment.") (footnotes omitted) (citing Mason Kortz & Chris Bavitz, *Cell Tower Dumps*, 63 BOS. B. J. 27, 28 (2019)); Tricia A. Martino, *Fear of Change:* Carpenter v. United States *and the Third-Party Doctrine*, 58 DUQ. L. REV. 353, 373 (2020) ("While the *Carpenter* Court did not address tower dumps, the magnitude of information about innocent people received through tower dumps cautions against the continuation of the third-party doctrine in the Information Age.").

[8] The Honorable Brian L. 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, 44–45 (2013).

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

However, this remains a minority position.[9] While at first glance *Carpenter* may seem to offer it some support,[10] the substantive differences between the data at issue there[11] and that contained in a typical tower dump[12] make the future imposition of a warrant requirement (with its attending probable cause standard) unlikely.

Furthermore, even if the Supreme Court were to hold that tower dumps qualify as Fourth Amendment searches,[13] such a result would not fully address the issue. This is because both of the ensuing protections—the probable cause determination and the exclusionary rule—are inherently relevant only to the *subject* of the Government's investigation, and all but useless to the innumerable innocent[14] third parties whose privacy interests have also been invaded.

---

[9] Kortz & Bavitz, *supra* note 7 ("The majority of courts to consider the question have rejected these arguments and held that a warrant is not required to obtain a cell tower dump."); *see also infra* notes 32–35, 40.

[10] After all, both CSLI and tower dumps involve the same variety of information, and before *Carpenter* both were being acquired pursuant to the same oft-critiqued reading of § 2703(d).

[11] Carpenter v. United States, 138 S. Ct. 2206, 2209 ("[T]he Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days—an average of 101 data points per day.").

[12] Kortz & Bavitz, *supra* note 7 ("[A] typical tower dump is confined in the sense that it covers both a small area and a relatively short time period—often a few hours or even a few minutes. Thus, a tower dump reveals less about any given individual's movements over a period of time than does historical CSLI.").

[13] Which is not likely to happen anytime soon. Pre-*Carpenter*, explicit discussion of the Fourth Amendment's application to tower dumps in case law was rare. *See* Owsley, *supra* note 8, at 23 ("The few existing judicial decisions addressing cell tower dumps . . . do not analyze the standard by which courts should authorize [them]. They also generally do not address Fourth Amendment concerns and seemingly never address the privacy issues related to individuals who are not the subject of the criminal investigation."). Also, given that so little time has elapsed since *Carpenter*, many of the tower dumps that have been challenged in its wake actually occurred *prior* to the publishing of that decision. Therefore, even if *Carpenter* had definitively classified tower dumps as Fourth Amendment searches, their acquisition without a warrant would still not merit suppression. *See, e.g.*, United States v. Pendergrass, No. 117CR315LMMJKL1, 2019 WL 2482169, at *2 (N.D. Ga. Feb. 6, 2019) ("Assuming for the sake of argument that *Carpenter* applies to tower dumps, I remain of the view that the tower dump in this case fits within the *Leon* good-faith exception to the exclusionary rule . . . ."). *See also* Owsley, *supra* note 8, at 44 ("[T]here are a significant number of decisions by magistrate judges as well as some district judges addressing § 2703. However, the government generally appears opposed to appealing adverse decisions to federal appellate courts—no doubt interested in avoiding creating bad case law.") (an assumption that is even more credible post-*Carpenter*, given the government's loss there).

[14] The author would like to emphatically clarify that reference to these third parties as "innocent" is done only for the sake of clarity and maintaining consistency with existing writing on this topic; it should in no way detract from the fact that the subjects of the government's investigation must themselves be presumed innocent.

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

In the interest of shielding those third parties from excessive and unnecessary intrusion, some US Magistrate Judges have imposed prophylactic measures on the Government as conditions of court orders issued under § 2703(d).[15] These measures accomplish more than a warrant requirement alone, but are ad hoc and not yet widely adopted.

A legislative solution in which Congress amends the SCA to constrain the provision of this data to the government by the cell carriers themselves—including proactively anonymizing identifying consumer information and facilitating analysis of the data by the government without allowing it to retain that data permanently—would embody a more consistent and permanent solution.

II. TOWER DUMPS, DEFINED

A tower dump is a surveillance technique used by law enforcement agencies. The typical use case aims to identify persons of interest—who were near the scene of a crime when it was committed—by requesting data from one or more wireless carriers detailing what cell phones[16] communicated with a particular cell tower (or set of towers) within a certain period of time.[17] As a general principle, a cell phone will seek out the strongest signal available to it multiple times a minute, regardless of whether or not it is being used.[18] This allows the phone to be in a perpetual—and convenient—state of

[15] *See, e.g.*, *In re* Application of the U.S. for an Ord. Pursuant to 18 U.S.C. §§ 2703(c) and 2703(d) Directing AT&T, Sprint/Nextel, T-Mobile, Metro PCS, and Verizon Wireless to Disclose Cell Tower Log Info., 42 F. Supp. 3d 511, 519–20 (S.D.N.Y. 2014) [hereinafter *In re* S.D.N.Y. Application]; *see also In re* Application of the U.S. for an Ord. Pursuant To 18 U.S.C. § 2703(d), No. 2:17-MC-51662, 2017 WL 6368665 at *2 (E.D. Mich. Dec. 12, 2017) [hereinafter *In re* E.D. Mich. Application]; *In re* Cell Tower Recs. Under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673, 677 (S.D. Tex. 2015) [hereinafter *In re* S.D. Tex. Recs.]; *In re* Search of Cellular Tel. Towers, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) [hereinafter *In re* S.D. Tex. Search].

[16] (or mobile devices generally)

[17] For an illustrative and ironic case, see United States v. Adkinson, 916 F.3d 605 (7th Cir. 2019) (wherein T-Mobile furnished data to the FBI showing that the defendant's phone—itself purchased from T-Mobile—was in the vicinity of multiple T-Mobile stores at the time that they were robbed). *Carpenter* also dealt with, among other things, the robbery of a T-Mobile store.

[18] *In re* Application of the U.S. for an Ord. Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to the Gov't, 534 F. Supp. 2d 585, 589–90 (W.D. Pa. 2008) [hereinafter *In re* W.D. Pa. Application] ("Cell phones . . . automatically communicate with cell towers, constantly relaying their location information to the towers that serve their network and scanning for the one that provides the strongest signal/best reception . . . approximately every seven seconds."); Judge Herbert B. Dixon Jr., *Your Cell*

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

readiness, but records of these "pings" also allow for anyone with access to a cell carrier's records to know where a given phone was at a given time.[19]

Tower dumps are often used as an investigatory technique, meaning that law enforcement agents are attempting to *identify* a suspect, rather than merely corroborate the location of a suspect that is already known to them.[20] A prototypical scenario would involve a series of bank robberies, occurring within a few hours of each other and in the same general locale. Police may suspect (or even know) that these robberies are related, and tower dumps from the tower closest to each bank during the period in which that bank was robbed may be cross-referenced, yielding the identifying information of cell phones that were present near each bank at the time of its robbery. In all likelihood, this list will be a short one, and will lead the police directly to their new suspect,[21] who made the ill-advised choice to keep a tracking device in their pocket while committing a felony.

While there are legitimate concerns about the propriety and constitutionality of law enforcement tracking and identifying their suspects with tower dumps,[22] an even more insidious potential lurks within the data that is *not* used. A tower dump inherently involves the provision of an exhaustive list of *all* phones that connected to the tower during whatever period of time is requested by law enforcement.[23] Depending on the density of users near the tower, the number of devices whose location is disclosed to police may number in the thousands.[24] The data of these third parties

---

Phone Is a Spy!, ABA (July 29, 2020), https://www.americanbar.org/groups/judicial/publications/judges_journal/2020/summer/your-cell-phone-a-spy/ ("When a phone is in standby mode ready to make or receive a call, it initiates several searches a minute seeking the strongest network signal from nearby cell towers, which is often the closest tower. In this situation, the phone identifies its approximate location by connecting with a particular cell tower.").

[19] Dixon, *supra* note 18 ("Additionally, the GPS feature of a cell phone allows tracking within several feet of its precise location.").

[20] *See In re* S.D. Tex. Search, 945 F. Supp. 2d at 769; *see also Adkinson*, 916 F.3d at 608 (although that case involved *voluntary* disclosure of data that was the result of an *internal* investigation).

[21] Or perhaps someone's grandmother who, with unlucky timing, was visiting multiple bank branches trying to find enough two-dollar bills to fill a birthday card.

[22] *See generally* Owsley, *supra* note 8.

[23] Hence the (unfortunate) word "dump."

[24] Katie Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, ACLU (Mar. 27, 2014, 11:58 AM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/cell-tower-dumps-another-surveillance-technique ("[T]he FBI was able to identify the two numbers belonging to the robbers. But they still had around 150,000 numbers left over—meaning the FBI was in possession of location information about many thousands of people who were not suspected of any

becomes collateral damage, caught up in what can very reasonably be characterized[25] as a dragnet search.[26]

In a different era, and in response to much cruder technology, Justice William Douglas presaged the threat posed by such surveillance:

> The citizen is completely unaware of the invasion of his privacy. The invasion of privacy is not limited to him, but extends to his friends and acquaintances—to anyone who happens to talk on the telephone with the suspect or who happens to come within the range of the electronic device. Their words are also intercepted; their privacy is also shattered. Such devices lay down a dragnet which indiscriminately sweeps in all conversations within its scope, without regard to the nature of the conversations, or the participants. A warrant authorizing such devices is no different from the general warrants the Fourth Amendment was intended to prohibit.
>
> Such practices can only have a damaging effect on our society. Once sanctioned, there is every indication that their use will indiscriminately spread. The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone.[27]

III. CSLI

It is important to distinguish between tower dumps and the collection of historical cell-site location information[28] that is particularized to an individual. *Carpenter*—in holding that the Government's acquisition of 127 days' worth of a defendant's CSLI was a Fourth Amendment search requiring

---

wrongdoing."); *In re* S.D. Tex. Recs., 90 F. Supp. 3d 673, 676 ("[A tower dump] might retrieve several thousand phone numbers in a metropolitan area like Houston.").

[25] Nathan Freed Wessler, *New York Court Recognizes Privacy-Invasive Nature of Cell Tower Dumps But Stops Short of Requiring a Warrant*, ACLU (June 2, 2014, 5:49 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/new-york-court-recognizes-privacy-invasive-nature ("[T]he government's request for a tower dump amounts to a highly invasive dragnet search.").

[26] Referring to any overbroad technique that ensnares far more than is necessary. Stop-and-frisk policing is a classic example. The NSA's widespread surveillance of American citizens is another; *see* Alex Abdo, *Is Dragnet Surveillance Constitutional?*, JURIST (Mar. 26, 2014, 1:37 PM), https://www.jurist.org/commentary/2014/03/alex-abdo-nsa-cell-surveillance/.

[27] Osborn v. United States, 385 U.S. 323, 353–54 (1966) (Douglas, J., dissenting).

[28] Carpenter v. United States, 138 S. Ct. at 2208 ("Each time a phone connects to a cell [tower], it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information for their own business purposes.").

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

a warrant—dealt exclusively with the latter.[29] While the *kind* of data at issue in *Carpenter* is ostensibly identical to that involved in a tower dump, *Carpenter*'s holding was expressly limited to individualized long-term CSLI collection.[30]

IV. § 2703 AND PRIOR CONTROVERSY

Before *Carpenter*, it was unsettled whether both tower dumps and more focused, long-term collection of CSLI were Fourth Amendment searches. No statute directly addressed the issue, but:

> Assistant United States Attorneys, with the encouragement of the United States Department of Justice, appl[ied] for court orders authorizing cell tower dumps pursuant to a provision in the Electronic Communications Privacy Act of 1986. The pertinent provision poses a procedural hurdle less stringent than a warrant based on probable cause, which in turn raises significant constitutional concerns.[31]

The above-mentioned provision is of course § 2703(d), and the majority position (consisting of the Fourth,[32] Fifth,[33] Sixth,[34] and Eleventh[35] Circuits) was that § 2703's less stringent hurdle[36] was constitutional, pursuant to the third-party doctrine. I.e., because "cell-phone users generally know that their phones must connect with towers to make and receive calls, and that service providers archive those connections for billing purposes,"[37] they have no reasonable expectation of privacy[38] in that information, meaning its acquisition does not constitute a search under the Fourth Amendment.

---

[29] *Id.* at 2209.

[30] *Id.* at 2220 ("We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval).").

[31] Owsley, *supra* note 8, at 2.

[32] United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc).

[33] *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) [hereinafter *In re* Fifth Cir. Application].

[34] United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206.

[35] United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc).

[36] *See supra* note 6.

[37] Zanders v. State, 73 N.E.3d 178, 184 (Ind. 2017) (in adopting the majority position, the Indiana Supreme Court gave a thorough survey and explanation of the "disagreement" amongst the Circuits. Of course, their decision was soon vacated by the Supreme Court, pursuant to *Carpenter*), *vacated*, 138 S. Ct. 2702 (2018).

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

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

Therefore, § 2703(d)'s less-than-probable-cause standard is not in conflict with constitutional requirements.

The Third Circuit, in answering a slightly different question,[39] rejected application of the third-party doctrine,[40] and ultimately held that a magistrate judge, with sufficient factual justification, *may* exercise their discretion by refusing to issue a § 2703(d) order and instead requiring probable cause sufficient to obtain a warrant.[41]

While *Carpenter* took this issue to the Supreme Court without a circuit split,[42] and resolved in contravention of the lower courts' seeming consensus, it was not entirely unprecedented. Magistrate Judge Owsley had long rejected the idea that this kind of data collection was within the ambit of § 2703 in the first place, and, free from that statute's confines, independently determined that both tower dumps and the acquisition of CSLI were Fourth Amendment searches requiring a warrant.[43]

In multiple cases, parties and amici (often the ACLU) argued for § 2703's inapplicability by emphasizing the singular phrasing present throughout the statute.[44] They urged courts to hold that such phrasing was irreconcilable with the inherently plural data gathering involved in tower

---

[39] To wit: whether a magistrate judge, statutory language notwithstanding, may *demand* probable cause before issuing a § 2703(d) order; *see infra* note 42.

[40] *In re* Third Circuit Application, 620 F.3d 304, 317 ("A cell phone customer has not 'voluntarily' shared [their] location information with a cellular provider in any meaningful way.").

[41] *Id.* at 319 ("Because the [SCA] as presently written gives the MJ the option to require a warrant showing probable cause, we are unwilling to remove that option although it is an option to be used sparingly . . . .").

[42] Orin Kerr, *Will the Supreme Court agree to hear the Fourth Amendment cell-site cases? (And should they?)*, WASH. POST (Apr. 26, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/04/26/will-the-supreme-court-agree-to-hear-the-fourth-amendment-cell-site-cases-and-should-they/ ("[T]here's no split. Every circuit court and state supreme court to rule on the issue has ruled that the Fourth Amendment does not protect historical cell-site data. The cert petitions claim a circuit split with the U.S. Court of Appeals for the 3d Circuit, but I don't think that's right. The 3d Circuit merely speculated about the possibility of Fourth Amendment protection in the course of making a statutory ruling.").

[43] *E.g.*, *In re* Application of the U.S. for an Ord, Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Locations Recs., 930 F. Supp. 2d 698, 700–01 (S.D. Tex. 2012) ("[§ 2703] does not address cell tower dumps" and "[C]ell site data are protected pursuant to the Fourth Amendment from warrantless searches"); *see also* Owsley, *supra* note 8, at 33–40 (a more thorough treatment of this argument by the same judge).

[44] *E.g.*, 18 U.S.C. § 2703(c) ("A governmental entity may require a provider of electronic communication service or remote computing service to disclose *a* record or other information pertaining to *a* subscriber to or *customer* of such service.") (emphasis added).

dumps and CSLI retrieval.[45] Ultimately, this argument has been rejected in the jurisdictions where it appeared,[46] pursuant to the canon of statutory construction that, unless otherwise specified, usage of the singular includes the plural.[47]

In other jurisdictions, judges predicated their rejection of court order applications under § 2703(d) for a more fundamental reason: they felt that the collection of CSLI was a Fourth Amendment search requiring a warrant obtained through a showing of probable cause, and therefore it was unconstitutional for the SCA to say otherwise.[48] While this view didn't always triumph on appeal,[49] it was of course eventually vindicated—for CSLI alone—by the Supreme Court in *Carpenter*.

---

[45] *See, e.g.*, United States v. Pembrook, 119 F. Supp. 3d 577, 585 (E.D. Mich. 2015) ("[Defendant] concludes that Congress' use of the singular 'a subscriber' means that the Act 'does not authorize a request for records pertaining to a large set of unidentified persons [and that to] rule otherwise is to conclude that Congress intended to authorize broad-based requests for information about potentially thousands of people by using language plainly limited to a single person.'") (citing Defendant's Motion to Suppress); *In re* S.D. Tex. Records, 90 F. Supp. 3d 673, 676 ("[T]he ACLU argued in the negative, pointing out that the SCA is consistently phrased in the singular . . . .").

[46] *See, e.g.*, United States v. Pendergrass, No. 1:17-CR-315-LMM-JKL, 2019 WL 1376745 at *2 (N.D. Ga. Mar. 27, 2019) ("[T]he Court finds, consistent with other district courts that have considered the issue, the Stored Communications Act's plain language does not prevent a tower dump because the default rule of statutory construction is that use of the singular includes the plural meaning."); *In re* S.D. Tex. Records, 90 F. Supp. 3d at 677 ("[T]he default rule of interpretation is to include both singular and plural, absent a contrary indication in the statute."); *Pembrook*, 119 F. Supp. 3d at 585 ("This argument is not novel and has been rejected by other district courts.") (citing *In re* S.D.N.Y. Application, 42 F. Supp. 3d 511, 513, and *In re* S.D. Tex. Records, 90 F. Supp. 3d at 677).

[47] Codified at 1 U.S.C. § 1 ("In determining the meaning of any Act of Congress, unless the context indicates otherwise . . . words importing the singular include and apply to several persons, parties, or things . . . .").

[48] *In re* W.D. Pa. Application, 534 F. Supp. 2d 585, 591 ("[T]his Court believes that citizens continue to hold a reasonable expectation of privacy in the information the Government seeks regarding their physical movements/locations—even now that such information is routinely produced by their cell phones—and that, therefore, the Government's investigatory search of such information *continues* to be protected by the Fourth Amendment's warrant requirement; *i.e.*, the Government must meet a probable cause background standard."); *see also In re* Application of the U.S. for an Ord. Authorizing the Release of Historic Cell-Site Info., No. 10-MC-0897 JO, 2010 WL 5437209, at *1 (E.D.N.Y. Dec. 23, 2010) ("[A]s a statutory matter, I interpret the SCA to permit the relief the government now seeks. . . . I also conclude that granting the government's application would violate the Fourth Amendment.") (footnote and internal citations omitted).

[49] *E.g.*, *In re* Third Cir. Application, 620 F.3d 304 (3d Cir. 2010).

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

V. TOWER DUMPS TODAY, AND THEIR STATUS UNDER *CARPENTER*

So where does this leave tower dumps today? With no specific statutory guidance or Supreme Court commentary, the Government is still able to proceed under § 2703(d),[50] at least so long as judges allow them to.

It is worth noting here that, historically, lower courts have not taken pains to distinguish between tower dumps and the collection of individualized long-term CSLI the way the Supreme Court eventually would. In many of the pre-*Carpenter* cases, the two techniques are spoken of interchangeably. Because *Carpenter* addresses only CSLI and not tower dumps, gleaning contemporary insight[51] from the cases that predate it is inherently fraught. Despite this, some inferences may be drawn from the language of *Carpenter* itself.

The Court speaks of a quantitative difference warranting a qualitative distinction (the so-called "mosaic theory"),[52] whereby the sum total of evidence sought, despite being made up of facially minor intrusions, paints a vivid picture through sheer multiplicity:

> Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.[53]

Put simply, the *Carpenter* majority acknowledged that, when it comes to CSLI, the whole may be greater than the sum of its parts.[54] The government's

---

[50] *Cf.* Owsley, *supra* note 8, at 22–23 (discussing internal DOJ guidance instructing AUSAs to proceed under § 2703(d)) (citing *Electronic Surveillance Manual*, U.S. DEPT. OF JUSTICE, at 41 (revised June 2005), https://www.justice.gov/file/1071991/download.

[51] Into how tower dumps *should* or *will* be treated in the future.

[52] Paul Rosenzweig, *In Defense of the Mosaic Theory*, LAWFARE INSTITUTE (Nov. 29, 2017, 3:18 PM), https://www.lawfareblog.com/defense-mosaic-theory (defining the theory as "the idea that large scale or long-term collections of data reveal details about individuals in ways that are qualitatively different than single instances of observation"). *See also* Elizabeth E. Joh, *Artificial Intelligence and Policing: Hints in the* Carpenter *Decision*, 16 OHIO ST. J. CRIM. L. 281, 281 (2018) ("Chief Justice Roberts focuses on the *quality* of the information sought by the police as a means of deciding the case in Carpenter's favor.") (emphasis added).

[53] *Carpenter*, 138 S. Ct. at 2219.

[54] *Id.* at 2217 ("[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.").

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

acquisition of any individual "piece" of CSLI may not amount to a Fourth Amendment search, but a collection of those pieces, viewed holistically, tells a bigger story.

Applying this reasoning to the relatively minimal amount of information about any given mobile device (and associated individual) that a tower dump yields, the same concerns about obtaining nuanced knowledge of an individual are arguably moot.[55] The privacy of innocent third parties is only invaded to the extent that the location of their cellular device at a *single* point in time is now in the possession of law enforcement.[56] A far cry from the "exhaustive chronicle" spoken of in *Carpenter*.[57] If the reasoning that motivated the Court's holding in *Carpenter* bears little applicability to tower dumps, it can hardly be argued that *Carpenter* itself supports their classification as Fourth Amendment searches requiring a warrant.

Years before *Carpenter*, Professor Shaun Spencer provided an eloquent framing of this very distinction.[58] Spencer referred to the type of collection at issue in *Carpenter* as data "aggregation going forward in time, or 'vertical' aggregation"[59] and to "aggregation that captures data on the many innocent cell phone users who pass near the cell towers under surveillance"[60] as "horizontal aggregation."[61] Ultimately, Spencer concluded that tower dumps are unlikely to be classified as Fourth Amendment searches.[62]

---

[55] However, while a single tower dump seems to work no great intrusion into the privacy of any one individual, a series of tower dumps coupled with cross-referencing of any given mobile device could produce precisely the sort of longitudinal location tracking that the Court took issue with in *Carpenter*. For this reason, a per se rule that the government will *never* need probable cause to obtain a tower dump seems ill-advised, as some requests could theoretically stray within *Carpenter*'s bounds. By analogy, such a rule (coupled with *Carpenter*'s per se warrant requirement for CSLI) would be akin to the familiar (with apologies to teetotalers and/or those not lucky enough to be citizens of the Commonwealth) Pennsylvania prohibition against buying more than two six-packs of beer from a gas station, readily circumvented by a brief trip to one's car between transactions. *Cf.* 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, 1232 (2004) ("If an agent wants to wiretap an e-mail account to obtain copies of every incoming message, does he need to obtain a wiretap order, or can he get a series of 2703(a) search warrants and serve one a day, or even one every hour?").

[56] And has, with all likelihood, been disregarded entirely.

[57] *Carpenter*, 138 S. Ct. at 2219.

[58] Shaun B. Spencer, *Data Aggregation and the Fourth Amendment*, 19 J. INTERNET L. 13 (2015).

[59] *Id.* at 15.

[60] *Id.* (i.e., tower dumps and similar non-individualized techniques).

[61] *Id.* (internal quotation marks omitted).

[62] *Id.* ("Admittedly, tower dumps gather vast amounts of information about innocents with no reasonable suspicion whatsoever, but horizontal integration does not paint an intimate portrait of any

Cases regarding the Fourth Amendment status of tower dumps post-*Carpenter* are scarce. However, *United States v. Walker* provides a concise analysis of how tower dumps are distinguishable from CSLI, reasoning that they capture [data] not for one targeted individual for an extended time, chronicling that individual's private life for days, but rather . . . for a particular place at a limited time. In this manner, the privacy concerns underpinning the court's holding in Carpenter do not come into play here, where the search for data focuses not on "the whole of [an individual's] physical movements" but rather on the data that was left behind at a particular time and place by virtue of cell phone tower locations.[63]

Given these differences, the Court believed that "Carpenter does not apply with equal force in the context of a tower dump request."[64] The court went even further in finding "no basis for attaching a Fourth Amendment interest to [tower dumps]" before concluding that, therefore, the Government may obtain a court order under § 2703(d).[65]

While *Carpenter*'s imposition of a per se warrant requirement for long-term individualized CSLI data was undeniably a victory for privacy advocates, such a victory is unlikely to be repeated with tower dumps. At least not by treading the same path.

VI. BEYOND *CARPENTER*

Simply because tower dumps do not fall within the scope of *Carpenter* does not mean they are without their own troubling privacy implications. Instead of the singular acute intrusion presented by long-term CSLI

individual's affairs. Instead, it takes a snapshot of many individuals' locations during a brief window of time. To the extent that the aggregated snapshot paints any picture, that picture merely shows everyone who was near the location of the alleged crime. Although 99.9 percent of the data will relate to innocents, that alone should not justify departing from the third-party and public exposure doctrines. Video surveillance of a suspect's travels in public also would capture snapshots of many passersby, but that would not convert the surveillance into a Fourth Amendment search. There may be compelling policy arguments to restrict how law enforcement stores and shares the information about innocent people's locations. *However, short-term horizontal aggregation will probably be insufficient to remove tower dumps from the third-party and public exposure doctrines.*") (emphasis added) (footnotes omitted).

[63] United States v. Walker, No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *8 (E.D.N.C. July 20, 2020) (second alteration in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)).

[64] *Id.* at *7 (internal quotation marks omitted).

[65] *Id.* at *8.

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

collection, a tower dump can result in thousands of invasions of privacy, almost all of which are inflicted upon innocent (and unaware) third parties.[66] In addition, while these invasions may seem minor now, advances in technology allowing our mobile devices to measure, catalogue, and broadcast increasingly sensitive information will inevitably make them more severe.[67]

The warrant requirement imposed by *Carpenter* works to protect the privacy interest in CSLI of the *subject* of a government investigation. The third parties whose information is caught up in the wide net of a tower dump are, by definition, not subjects of any investigation. Therefore, a probable cause requirement would do little to protect their interests beyond making it marginally more difficult for the Government to obtain a tower dump in the first place. The probable cause determination, being focused on the individual (known or unknown) who is the target of the Government's investigation, contains within it no room for the consideration of third parties.[68]

VII. THE EXISTING JUDICIAL REMEDY

Despite holding that CSLI *could* be obtained with a showing less-than probable cause, the Third Circuit has found the language of the Stored Communications Act to be permissive, allowing for a scenario in which a judge, despite the Government's fulfilment of § 2703's statutory requirements, could refuse to issue a court order allowing the collection of CSLI, and instead require probable cause before issuing a warrant.[69] Note

---

[66] *See supra* note 8.

[67] Dalmacio V. Posadas, Jr., *Commentary, Regardless of the Outcome in* United States v. Carpenter, *The Stored Communications Act is Problematic*, HARV. J.L. & TECH. JOLT DIG. (2018), https://jolt.law.harvard.edu/digest/regardless-of-the-outcome-in-united-states-v-carpenter-the-stored-communications-act-is-problematic ("However, what happens when, and yes, very likely a question of when, the data or historical CSLI that is retrieved during cell tower dumps includes far more pervasive and intimate details than at present. Technology is exponentially advancing and if the Courts do not address these issues with the future in mind, then the laws will surely being playing catch up for the foreseeable future.").

[68] *Cf. id.* (Warning that, even where the Government has probable cause "there are still potentially hundreds of thousands of innocent cellular subscribers who lose Fourth Amendment protection from a single cell tower dump in order to further the government's criminal investigation" and acknowledging that it is tempting ignore this "because the infringement seems innocuous enough, or even that the third-party doctrine removes the innocent cellular subscribers' protection under the Fourth Amendment.").

[69] *See In re* Third Cir. Application, 620 F.3d at 319.

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

that this approach was not universal, with other jurisdictions explicitly denying the existence of such judicial discretion.[70]

For requests involving CSLI, *Carpenter* has foreclosed a judge's use of discretion in favor of defaulting to a higher standard, but that case's letter and spirit do not seem to disturb the existing ability (in the Third Circuit anyway) of a judge to exercise this discretion when reviewing tower dump requests. However, the Third Circuit rather narrowly proscribed that discretion[71] and *Carpenter* does not offer much support for expanding a judge's ability to include requiring probable cause for *all* tower dumps, both because of the express limitation of its holding[72] as well as the substantive difference between the 127 days of CSLI collected in that case and the rather narrow cross section of information involved in a typical tower dump.[73]

Looking beyond the warrant requirement, some courts have used their inherent power to attach conditions to court orders issued under § 2703(d), and in doing so have sought to minimize the threat tower dumps present to the privacy of innocent third parties.

In 2014, the Southern District of New York furnished an illustrative pre-*Carpenter* example.[74] There, a magistrate judge agreed to issue an order authorizing a tower dump under § 2703(d), provided that the Government "justifies the time period for which the cell tower records are requested and [] provides a plan to address the protection of private information of innocent third parties whose data is disclosed to the Government."[75] Also of note is that, even while imposing restrictions, the court acknowledged a difference

---

[70] *See In re* Fifth Cir. Application, 724 F.3d at 607 ("Reading the provision as a whole, we conclude that the 'may be issued' language is permissive—it grants a court the authority to issue the order—and the 'shall issue' term directs the court to issue the order if all the necessary conditions in the statute are met.") (quoting the Stored Communications Act § 2703(d) and 615 ("[A]s long as the Government meets the statutory requirements, the SCA does not give the magistrate judge discretion to deny the Government's application for such an order.").

[71] *In re* Third Cir. Application, 620 F.3d at 319 ("[I]t is an option to be used sparingly . . . . [S]hould the MJ conclude that a warrant is required rather than a § 2703(d) order, on remand it is imperative that the MJ make fact findings and give a full explanation that balances the Government's need (not merely desire) for the information with the privacy interests of cell phone users.").

[72] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("We do not express a view on . . . 'tower dumps' . . . .").

[73] *See* Section V, *supra*.

[74] *In re* S.D.N.Y. Application, 42 F. Supp. 3d 511.

[75] *Id.* at 519–20.

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

between tower dumps and CSLI.[76] In making that distinction, the court cited an E.D.N.Y. decision requiring a warrant for retrieval of CSLI.[77]

Similarly, a Southern District of Texas magistrate judge, acknowledging the Fifth Circuit's controlling precedent,[78] nevertheless exercised discretion over the issuance of a court order for a tower dump, requiring that the Government narrow its request from one hour to ten minutes.[79]

In 2017, after the Supreme Court had heard arguments in *Carpenter*, but before its decision had been handed down, a magistrate judge in the Eastern District of Michigan refused to issue an order authorizing a tower dump, citing concerns over the privacy of innocent third parties, and allowing for resubmission once those concerns had been addressed in a similar manner as in the preceding cases.[80]

Perhaps most illuminating of all is a 2015 memorandum opinion and order[81] from a Northern District of Illinois magistrate judge outlining a series of best practices[82] for limiting warrants authorizing the use of a cell-site simulator (commonly referred to as a stingray device). A cell-site simulator essentially poses as a cell tower, which causes all operational mobile devices in the vicinity to "ping" it, yielding the same kind of information involved in

---

[76] *Id.* at 515 ("[tracking an individual's movements over time] is not at issue here. Rather, the Government seeks to retrieve phone numbers used during a particular time period in a particular area . . . .").

[77] *See In re* Application of the U.S. for an Ord. Authorizing the Release of Hist. Cell–Site Info., 809 F. Supp. 2d 113 (E.D.N.Y. 2011). In other words, without conflating long-term CSLI and tower dumps, and acknowledging the more acute nature of the former, the Court *still* was willing to curtail tower dumps.

[78] *In re* Fifth Cir. Application, 724 F.3d 600 (regarding a magistrate judge's then-inability to require a warrant for CSLI).

[79] *In re* S.D. Tex. Records, 90 F. Supp. 3d at 677 ("To be sure, the court has inherent power to limit the scope of the tower dump based on Fourth Amendment privacy concerns, but again, the Fifth Circuit has found no reasonable expectation of privacy in cell site records. A court could also limit the temporal scope of the tower dump based on the Government's threshold showing of the 'specific and articulable facts' required by § 2703(d). For that very reason, I have reduced the relevant time window here from one hour to ten minutes.") (footnote omitted).

[80] *In re* E.D. Mich. Application, 2017 WL 6368665 at *2 ("Any order for mass production of cell site data requires protections for third parties who are not subjects of the investigation. . . . [T]he present application is DENIED WITHOUT PREJUDICE. The government may resubmit an application and proposed order consistent with this Opinion and Order.").

[81] *In re* Application of the U.S. for an Order Relating to Tel. Used by Suppressed, No. 15 M 0021, 2015 WL 6871289 (N.D. Ill. Nov. 9, 2015) [hereinafter *In re* N.D. Ill. Application].

[82] *See infra*, note 85.

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

both CSLI and tower dumps.[83] The court cautioned that, even coupled with a warrant, the usage of a cell-site simulator inevitably creates a concerning intrusion into the privacy of innocent third parties.[84]

In an effort to mitigate these intrusions, the court outlined three requirements for the Government when using a cell-site simulator,[85] the first two of which are readily applicable to tower dumps. The first requires the Government to make reasonable efforts to avoid obtaining the information of individuals other than those who are the target of investigation.[86] The second requires the immediate destruction of all data not related to the target, to occur no later than 48 hours after its acquisition, with evidence of this destruction furnished to the court.[87] The court also observed that "to date, the requirements outlined in this opinion have not interfered with effective law enforcement."[88]

While a cell-site simulator—with its portability, and ability to affirmatively seek information—seems somewhat more insidious than a tower dump, concerns with regard to innocent third parties are substantially similar. Limiting a tower dump's temporal duration to a reasonable extent while mandating prompt destruction of extraneous data would significantly protect the privacy interests of innocent third parties.

---

[83] *In re* N.D. Ill. Application, 2015 WL 6871289 at *2.

[84] *Id.* at *4 (Noting that "concern over the collection of innocent third parties' information is not theoretical. It has been reported that the federal government collects telephone numbers, maintains those numbers in a database and then is very reluctant to disclose this information.").

[85] *Id.* at *3, *4 (the Court summarized its conclusion as follows: "Accordingly, this Court requires that the order granting the application must contain a provision that reads as follows: 'The Federal Bureau of Investigation, and other authorized law enforcement officials, may employ electronic investigative techniques to capture and analyze signals emitted by any and all cellular telephones used by [the target] for a period of 30 days. Officials of the Federal Bureau of Investigation and other authorized law enforcement officials (a) must make reasonable efforts to minimize the capture of signals emitted from cellular telephones used by people other than [the target], (b) must immediately destroy all data other than the data identifying the cellular telephones used by [the target] (such destruction must occur within forty-eight (48) hours after the data is captured, and the destruction must be evidenced by a verification provided to the Court with the return of the warrant), and (c) are prohibited from using the data acquired beyond that necessary to determine the cellular telephones used by [the target].'").

[86] *Id.*

[87] *Id.*

[88] *Id.* at *1.

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

VIII. A LEGISLATIVE REMEDY

Through their foresight and ingenuity, U.S. magistrate judges have provided a strong framework for protecting third-party privacy interests whenever a tower dump is executed. However, full-scale implementation of this framework can be best accomplished through the political process, via an amendment to the SCA.

It is no critique of the previously-discussed "judicial remedy" to say that it is merely a guidepost toward a permanent solution. Magistrate judges, whose statutory authority permits them to[89] issue orders and warrants,[90] represent a critical first line of defense against governmental overreach. However, as of 2019, there were 541 full-time magistrate judges authorized by statute,[91] and as evidenced by what little case law exists on the issue, there isn't exactly universal consensus among them.[92] Given that no statute directly addresses tower dumps, and that *Carpenter* expressed no opinion, some judges are likely unaware of the issue to begin with.[93]

Aside from this logistical hurdle, an inconsistent and ad hoc judicial solution is simply inappropriate for an issue of this magnitude.[94] Legislative action strikes a middle ground between direct constitutional protection (assuming tower dumps are never recognized as Fourth Amendment searches) and asking individual magistrate judges to defend the privacy of

---

[89] (among many other things)

[90] 28 U.S.C. § 636(a).

[91] *Just the Facts: Magistrate Judges Reach the Half Century Mark*, U.S. CTS. (Feb. 20, 2019, 9:09 PM), https://www.uscourts.gov/news/2019/02/20/just-facts-magistrate-judges-reach-half-century-mark.

[92] *See supra* Section IV.

[93] *See* Owsley, *supra* note 8, at 17–18 ("Cell tower dumps have not garnered much attention in the media. Indeed, the government does not like to draw attention to this electronic surveillance method. Interestingly, in my own informal survey of magistrate judges nationwide, many have informed me that they were unfamiliar with cell tower dumps. After coming to an understanding of the procedure, numerous had concerns or reservations about them.").

[94] Simon M. Baker, *Unfriending the Stored Communications Act: How Technological Advancement and Legislative Inaction Have Rendered Its Protections Obsolete*, 22 DEPAUL J. ART TECH. & INTELL. PROP. L. 75, 116 (2011) ("It is not the courts' place to overhaul this area. Such a complex and immense task falls clearly on the shoulders of the legislature.").

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

innocent citizens from increasingly sophisticated and commonplace[95] surveillance techniques.[96]

The Fifth Circuit may have hinted at this when it ruled on the issue, acknowledging that while it sympathized with the *desire* of cell phone users[97] to have a degree of privacy in their location information, such a desire couldn't become a reasonable *expectation*[98] without more: namely, statutory protection.[99] The Court further supported a legislative remedy by quoting Justice Alito, who, while concurring in *United States v. Jones*,[100] said that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[101]

The Court also characterized its ruling as being deferential to the "balancing of privacy and safety" Congress already completed in enacting the SCA.[102] Such deference to the will of the people—as expressed through the democratic process—sounds great in theory.[103] But the SCA is now 35

---

[95] Joh, *supra* note 52, at 285 ("The police today enjoy a surfeit of data that can be collected, stored, mined, and sifted through easily and cheaply: license plate data, social media posts, social networks, and soon our own faces.").

[96] Surely the privacy of innocent third parties is too important to be shielded solely by judicial discretion at the lowest level of the federal court system. Nearly a decade before *Carpenter*, one commentator, in discussing a potential warrant requirement for GPS-enabled location tracking, thought the issue was too important to rely on intervention at that system's *highest* level. *See* Kimberly C. Smith, *Hiding in Plain Sight: Protection From GPS Technology Requires Congressional Action, Not a Stretch of the Fourth Amendment*, 62 MERCER L. REV. 1243, 1267 (2010) ("[T]his Author opines that the appropriate solution to protect this important privacy right should not be in limbo until a future determination by the Supreme Court.").

[97] 97% of adult Americans own a cellphone. *Mobile Fact Sheet*, PEW RES. CTR. (Sept. 22, 2021, 9:43 PM), https://www.pewresearch.org/internet/fact-sheet/mobile/.

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

[99] *In re* Fifth Cir. Application, 724 F.3d at 615 ("[T]he recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections."). *Cf.* Smith, *supra* note 96, at 1276 ("The [Supreme] Court has long acknowledged Congress's ability, through direct legislation, to provide privacy protections beyond the Fourth Amendment.").

[100] 565 U.S. 400 (2012) (holding that attachment of a GPS device to a vehicle, together with the subsequent tracking of its movements, constituted a search under the Fourth Amendment).

[101] United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

[102] *In re* Fifth Circuit Application, 724 F.3d at 615 ("We decline to create a new rule to hold that Congress's balancing of privacy and safety is unconstitutional.").

[103] Similar reasoning was given *In re* Third Cir. Application, 620 F.3d at 319 ("Congress would, of course, be aware that such a statute mandating the issuance of a § 2703(d) order without requiring probable

years old,[104] which makes its continued application to contemporary technologies[105] anachronistic at best. Critique of the SCA as unfit to handle the modern paradigm far predates even Judge Owsley's 2013[106] article: Professor (and privacy law luminary) Orin Kerr's exhaustive critique dates all the way to 2004, and contains *zero* references to cell-phones.[107] It also expressed little concern about § 2703(d), which, given the state of technology at the time, was significantly less potent than it is now.[108]

Legislative action would relieve courts of the impossible task of trying to reconcile old law with new problems. This is particularly important because the privacy implications of tower dumps are something of a moving target, in that advancing technology will only make them more severe. The SCA distinguishes between the disclosure of content and non-content records, with more stringent processes required to obtain the former.[109] In a pre-digital world, this made a lot of sense: the contents of a letter are intuitively more "private" than the addressee, written on the exterior of the envelope. The CSLI at issue in *Carpenter*, obtained with a § 2703(d) order, was non-content too, yet its acquisition worked such an intrusion into the suspect's privacy that the Court recognized it as a Fourth Amendment

cause and based only on the Government's word may evoke protests by cell phone users concerned about their privacy. The considerations for and against such a requirement would be for Congress to balance. A court is not the appropriate forum for such balancing, and we decline to take a step as to which Congress is silent.").

[104] Originating in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat 1848 (1986).

[105] And their broad implications. *See* quote accompanying *supra* note 96.

[106] Owsley, *supra* note 8.

[107] *See generally* Kerr, *supra* note 55.

[108] Due to the ubiquity of cell phone ownership coupled with the proliferation of cell towers themselves. *See supra* note 98; Owsley, *supra* note 8, at 33 ("[I]mproving technology enables the recipients of cell site location information to pinpoint a cell phone within about one hundred feet or less. At the end of 1986, the year Congress enacted the Electronic Communications Privacy Act, there were only 1531 cell sites throughout the United States. At the end of 2011, there were 283,385 cell sites throughout the United States, up from 127,540 at the end of 2001. As the number of cell towers increases, the accuracy of the tracking of a specific cell phone (and the cell phone's user) vastly improves.") (footnotes omitted).

[109] Stored Communications Act 18 U.S.C. § 2703(d). *See* Kerr, *supra* note 55, at 1218–20.

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

search.[110] Such a distinction no longer accomplishes much,[111] especially given the increasing sophistication of artificial intelligence. As an example: datasets derived from *existing* non-content surveillance methods, like tower dumps, can be analyzed, cross-referenced, and continually monitored to yield information that was once impossible to ascertain[112] even from *content*.[113]

Congress may efficiently protect third-party privacy interests from intrusions by court-ordered tower dumps by amending the SCA. This amendment should require, as a prerequisite to any court order issued for a tower dump under § 2703(d), the prophylactic measures already being used by some magistrate judges. First amongst these should be limiting to a reasonable degree the temporal scope of a tower dump, which will minimize the collection of third-party data in the first place. Second, any data provided to law enforcement by a carrier should be preemptively anonymized by the carrier.[114] Finally, the party requesting data should be required to supply the court with proof of non-retention.

This last factor is perhaps the most important. That the government knows where you were on a given day may seem unimportant when you are not the person they're after. But if the Government is allowed to continue to retain the contents of every tower dump it compels, that data will constitute

---

[110] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.").

[111] *See* Carlos Aguilar, *Privy or Private: A New Age Look at Old School Privacy Laws*, 53 CAL. W.L. REV. 85, 104 (2016) ("In essence, cell site location data is treated as metadata information. Given that cell site location data constitutes non-content information, the SCA does not require a warrant. Yet, like emails, cellphones are prevalent in contemporary society.").

[112] See the now-seminal example of Target analyzing customers' purchases to determine if they were pregnant, Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 8:49 PM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did.

[113] Joh, *supra* note 52, at 284–85 ("The availability of massive amounts of data, leaps in computing power, and increasingly sophisticated algorithms have begun to change policing as well. We might define the use of AI in policing as the growing use of technologies that apply algorithms to large sets of data to either assist human police work or to replace it. And assistance is something of a misnomer. Artificial intelligence has begun to change the capabilities of the police by permitting them to do what was once nearly impossible or impracticable.") (footnote omitted).

[114] For example, carriers could identify each mobile device that connected to a tower during the requested time period with a randomly generated signifier. Law enforcement could then conduct whatever cross-referencing necessary, and return to the carrier to request the "true identity" of only the signifier they deemed to be relevant. This measure alone would render most third-party privacy concerns moot.

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu

an increasingly detailed historical record of *everyone's* whereabouts. Such a record could, and may already be, abused in a myriad of ways.

IX. CONCLUSION

Admittedly, the SCA is a complex statute[115] whose implications are increasingly muddled with time. The amendment proposed in this Article is merely a single piece in a much larger puzzle.[116] Voluntary, rather than compelled disclosure, is another pernicious issue that merits examination,[117] particularly where carriers are compensated for the data they provide,[118] and changes in technology may make tower dumps obsolete before they have time to do much more harm. In any event, attention must be paid to how we as a people—through our elected officials—respond to emerging Government intrusions.

Where a statute is hopelessly out of date, judicial prose of a similar vintage may prove more evergreen: "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[119] That time is now.

---

[115] Kerr, *supra* note 55, at 1208 (the SCA "remains poorly understood" and "is dense and confusing").

[116] A mosaic, if you will.

[117] For a timely example that implicates this and other nuances discussed here, see Commonwealth v. Dunkins, 229 A.3d 622, 625 (Pa. Super. 2020), *appeal granted*, 237 A.3d 415 (Pa. 2020).

[118] Owsley, *supra* note 8, at 19–20 ("For some providers, cell phone surveillance, including cell tower dumps, generates revenue. For example, in 2011, Verizon report[ed] that it had been reimbursed approximately three to five million dollars in each of the last five years for the data it provided to law enforcement. Similarly, AT&T collected $8.3 million in fees, up from $2.8 million in 2007. Although Sprint declined to provide any information about how much it collects in fees, commentators have estimated that it could be as high as $26 million, but probably at least $10 million. Even U.S. Cellular, a small provider, reported earning $460,000 in fees from providing data in response to law enforcement requests. This interest in increasing revenue creates an incentive to cooperate with law enforcement that invariably leads to a loss of privacy by some innocent third parties.") (footnotes and internal quotation marks omitted).

[119] United States v. Knotts, 460 U.S. 276, 284 (1983).

Vol. 40, No. 1 (2021) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2021.222 ● http://jlc.law.pitt.edu