The Aggregation Principle and the Future of Fourth Amendment Jurisprudence

Shaun B. Spencer*

Data aggregation has played a role in three recent cases implicating one's reasonable expectation of privacy under the Fourth Amendment.[1] Although the cases involve disparate doctrines, they all focus on aggregation as a reason to depart from prior law.[2]

For example, in *United States v. Jones*,[3] five Supreme Court Justices relied on aggregation to depart from the public exposure doctrine. In *Jones*, the Court considered a defendant's claim that law enforcement violated the Fourth Amendment by gathering Global Positioning System (GPS) data from a tracking device attached to his vehicle for thirty days.[4] The government relied on the public exposure doctrine[5] to argue that one lacks any expectation of privacy while traveling in public places. Five Justices relied on the thirty-day aggregation of data to depart from the public exposure doctrine, and to hold that long-term, warrantless GPS tracking violated a reasonable expectation of privacy.[6]

Similarly, in *Commonwealth v Augustine*,[7] the Supreme Judicial Court of Massachusetts (SJC) relied on aggregation to depart from the third-party

---

* Assistant Professor, University of Massachusetts School of Law – Dartmouth.

1. *See* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945 (2012); Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2013).

2. *See Riley*, 134 S. Ct. at 2473; *Jones*, 132 S. Ct. at 945; *Augustine*, 4 N.E.3d at 846.

3. *See Jones*, 132 S. Ct. at 964.

4. *See id.* at 948.

5. *See* United States v. Knotts, 460 U.S. 276, 281-82 (1983) (holding that law enforcement's use of beeper to track the defendant's vehicle was not a Fourth Amendment search because one has no expectation of locational privacy while on a public road).

6. *Jones*, 132 S. Ct. at 956 (Alito, J., concurring) (noting that long-term tracking "secretly monitor and catalogue every single movement of an individual's car for a very long period"); *id.* at 964 (Sotomayor, J., concurring) (people do not "reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on . . . .").

7. *Augustine*, 4 N.E.3d at 865-66.

doctrine. In *Augustine*, the SJC considered a defendant's argument that the Commonwealth violated the Fourth Amendment by obtaining two weeks of cell site location information (CSLI) from the defendant's cell service provider without a warrant.[8] The Commonwealth argued that CSLI enjoyed no Fourth Amendment protection because it was obtained from the cell phone provider, and therefore fell within the third-party doctrine.[9] The SJC declined to apply the third-party doctrine because of the portrait that long-term CSLI tracking can paint of a person's affairs.[10]

Finally, in *Riley v. California*,[11] a unanimous Supreme Court relied on aggregation to depart from the search incident to arrest exception to the warrant requirement. In *Riley*, the Court considered the arrestees' arguments that the government violated the Fourth Amendment by searching the contents of a cell phone and a smart phone incident to arrest.[12] The government argued that the search incident to arrest exception permitted the warrantless search.[13] The Court declined to apply the search incident to arrest exception because of the aggregated data that law enforcement can gather from cell phones and smart phones.[14]

In each of these cases, the courts relied on data aggregation to carve out an "exception to an exception." This essay considers several questions about where this aggregation principle will take us next.

I. CELL SITE LOCATION INFORMATION

Lower courts have reached conflicting decisions over whether the Fourth Amendment protects CSLI, or whether CSLI falls within the third-party doctrine. *Jones* did not consider that question, because the police gathered location information from a device planted on the suspect's vehicle, not

8. *Id.* at 849.

9. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that defendant had no reasonable expectation of privacy in the numbers that he dialed).

10. *Augustine*, 4 N.E.3d at 863 ("[E]ven CSLI limited to the cell site locations of telephone calls made and received may yield a treasure trove of very detailed and extensive information about the individual's 'comings and goings' in both public and private places."). The SJC also distinguished CLSI records from the telephone numbers dialed in *Smith* because individuals do not voluntarily transmit their location information to the cell service provider when making a call and because location information bears no relation to the communicative purpose of the call. *Id.* at 862-63.

11. *See* Riley v. California, 134 S. Ct. 2473, 2481 (2014).

12. *See id.* at 2480.

13. *Id.* at 2481.

14. *Id.* at 2491 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is . . . .").

from a third party, like a cell service provider.[15] However, just as aggregation led five Justices in *Jones* to depart from the public exposure doctrine, and led the *Riley* Court to depart from the search incident to arrest exception, courts could rely on the aggregation principle to exclude long-term collection of CLSI from the third-party doctrine. Indeed, the SJC relied on aggregation to do precisely that in *Augustine*.[16]

We may be seeing just such a development in the post-*Jones* CSLI cases. Prior to *Jones*, courts were divided on whether CSLI should enjoy Fourth Amendment protection, but a substantial majority of courts held that it was not protected.[17] In the wake of *Jones*, however, decisions in state and federal appellate courts are equally divided.[18] Even one of the federal cir-

15. Indeed, several appellate courts have disregarded *Jones* for just that reason. *See In re* United States Application for Historical Cell Site Data, 724 F.3d 600, 611-12 (5th Cir. 2013) (distinguishing *Jones* because the government has neither "required [n]or persuaded" providers to keep historical cell site records) (quoting *Jones*, 132 S. Ct. at 961 (Alito, J., concurring)); Ford v. State, 444 S.W.3d 171, 187-88 (Tex. Ct. App. 2014) (distinguishing *Jones* because the cell provider gathered the information, not the state).

16. Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2013).

17. "The majority of courts to consider this issue have ruled that the acquisition of historic CSLI pursuant to a 2703(d) order does not implicate the Fourth Amendment because it is a business record held by a third party." United States v. Caraballo, No. 5:12-cr-105, 2013 U.S. Dist. LEXIS 112739, *53 (D. Vt. Aug. 7, 2013); United States v. Rigmaiden, No. 08-814-PHX-DGC, 2013 U.S. Dist. LEXIS 65633, *32-33 (D. Ariz. May 8, 2013); United States v. Wilson, NO. 1:11-CR-53-TCB-ECS-3, 2013 U.S. Dist. LEXIS 37783, *17 (N.D. Ga. Feb. 20, 2013); United States v. Steve Ruby, NO. 12CR1073 WQH, 2013 U.S. Dist. LEXIS 18997, *17 (S.D. Cal. Feb. 12, 2013); United States v. Madison, No. 11-60285, 2012 U.S. Dist. LEXIS 105527, *29-30 (S.D. Fla. July 30, 2012); *In re* Application of United States for Order Pursuant to 18 U.S.C. 2703(d), 849 F. Supp. 2d 177, 179 (D. Mass. 2012); United States v. Dye, No. 10CR221, 2011 U.S. Dist. LEXIS 47287, *24-25 (N.D. *33 Ohio Apr. 27, 2011); United States v. Velasquez, No. 08-730-WHA, 2010 U.S. Dist. LEXIS 118045, *17-18 (N.D. Cal. Oct. 22, 2010); United States v. Benford, No. 09 CR 86, 2010 U.S. Dist. LEXIS 29453, *7-8 (N.D. Ind. Mar. 26, 2010); United States v. Suarez-Blanca, No. 07-023-MHS/AJB, 2008 U.S. Dist. LEXIS 111622, *27-28 (N.D. Ga. Mar. 26, 2008). In contrast, the Commonwealth's brief cited far fewer cases supporting the minority position. *Id.* (citing *In re* Application of the United States of America for an Order Authorizing Release of Historical Cell-Site Information, 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011); *In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578, 579 (E.D.N.Y 2010)); Brief and Appendix for the Commonwealth at 32, Commonwealth v. Augustine, No. SJC-11482, 2013 WL 5052093, Aug. 19, 2013 (citing *In re*: Application of the United States of America for Historical Cell Site Data, No. 11-20884, 2013 U.S. App. LEXIS 15510 (5th Cir. July 30, 2013)).

18. For cases denying CSLI Fourth Amendment protection, *see In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611–15 (5th Cir. 2013); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012) (holding that defendant had no reasonable expectation of privacy in the location data given off from his cell phone's GPS, thus no

cuits that applied the third-party doctrine recognized that the Supreme Court may ultimately reconsider *Smith v. Maryland* as applied to CSLI.[19] Since *Jones*, two of the three state supreme courts that have exempted CSLI from the third-party doctrine have relied on their state constitutions.[20] Ultimately, it may be the state courts that turn the national tide on this question.[21]

II. SHORT-TERM VERSUS LONG-TERM LOCATION TRACKING

Jones and *Augustine* did not prohibit all warrantless location tracking. Instead, they distinguished short-term tracking (acceptable) from long-term tracking (unacceptable). This raises an obvious question for future cases—how long is too long? Although this may seem a somewhat pedantic exercise in line-drawing, it remains an important exercise for litigants who have been subjected to GPS or CSLI tracking.

Looking purely at the numbers, there is a relatively small window for debate. The *Jones* Court established the outer limit by holding that thirty days of GPS tracking was too long. The *Augustine* court adopted a shorter

---

search occurred when Skinner voluntarily used his cell phone while traveling on public roads), *cert. denied*, 133 S. Ct. 2851 (2013); *Ford*, 444 S.W.3d at 190-91 (concluding that *Riley* "does not concern the third-party doctrine espoused" in *Smith v. Maryland* and is "otherwise inapplicable to the present situation involving a court order to obtain . . . business records of [defendant's] use of its cell tower network."). For cases granting CLSI Fourth Amendment protection, *see Tracey*, at *19 (dealing only with real-time CSLI, as opposed to historical CSLI); *Augustine*, 4 N.E.3d at 846; State v. Earls, 70 A.3d 630, (N.J. 2013) (refusing to apply the third-party doctrine because people do not use cell phones in order to be tracked, and because most people are unaware of the extent of their cell provider's tracking ability); *see also* United States v. Cooper, No. 13–cr–00693–SI–1, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015) (holding that the Fourth Amendment prohibited warrantless access to 60 days of CSLI, but refusing to suppress CSLI because of good faith exception); United States v. Davis, 754 F.3d 1205, 1215 (11th Cir. 2014) (holding that collection of CSLI violated reasonable expectation of privacy, but finding no reversible error because of good faith exception), *vacated pending rehearing en banc*, 573 Fed. Appx. 925 (11th Cir. 2014).

19. *See* United States v. Guerrero, 768 F.3d 351, 360-61 (5th Cir. 2014) (recognizing the concerns about location tracking and data aggregation may lead the Supreme Court to revisit the third-party doctrine, but holding that *Riley v. California* did not "unequivocally" overrule earlier Fifth Circuit precedent or *Smith v. Maryland*).

20. *Compare Augustine*, 4 N.E.3d at 846 (Massachusetts Constitution), *and Earls*, 70 A.3d at 644, (New Jersey Constitution), *with* Tracey v. State, No. SC11-2254, 2014 WL 5285929, at *19 (Fla. Oct. 16, 2014) (Federal Constitution).

21. *See generally* Lawrence M. Friedman, *Reactive and Incompletely Theorized State Constitutional Decision-making*, 77 MISS. L.J. 265 (2007); Lawrence M. Friedman, *Unexamined Reliance on Federal Precedent in State Constitutional Interpretation: The Potential Intra-State Effect*, 33 RUTGERS L.J. 1031 (2002) (discussing the role of state constitutional law).

threshold by holding that two weeks of CSLI tracking constituted long-term surveillance. On the other end of the spectrum, the *Augustine* court observed in dicta that six hours would be acceptable as short-term, warrantless tracking.[22] And the Sixth Circuit in *Skinner* held that, even if the reasoning of the five concurring Justices in *Jones* were applicable to CSLI, three days of warrantless CSLI tracking was permissible.

To render this line-drawing exercise less hollow, courts should consider how the duration of the tracking implicates the two policy concerns identified in the *Jones* concurrences. First, courts should consider how long surveillance would have to last before painting an impermissibly intimate picture of an individual's affairs.[23] And second, courts should consider how long digital surveillance would have to last to render it impractical by traditional law enforcement means.[24]

These policy concerns favor an extremely limited exception to allow short-term, warrantless tracking. Even the three-day tracking that the Sixth Circuit approved in *Skinner* seems unreasonably long when you envision law enforcement tracking you for three straight days.[25] Monitoring one's movements twenty-four hours a day, for three straight days, may paint an intimate portrait of his or her daily patterns, habits, and associations. And financial and personnel limitations make three days of round-the-clock surveillance prohibitively expensive in most law enforcement investigations. For these reasons, courts should draw the line between short-term and long-term location tracking at one day at most. In fact, the high courts in New Jersey and Florida have held CSLI to be protected under the Fourth Amendment without regard to the duration of the tracking.[26]

III. SHORT-TERM BUT LARGE-SCALE LOCATION TRACKING

The decisions described above have emphasized the intrusive nature of aggregating large amounts of data about one person. But do similar concerns apply to aggregating small amounts of data about many people?

---

22. *Augustine*, 4 N.E.3d at 863.

23. *See* United States v. Jones, 132 S. Ct. 945, 955-57 (2012) (Sotomayor, J., concurring) (reasoning that location tracking allows the government to cheaply obtain an intimate portrait of one's personal affairs in an easily obtainable, searchable, and storable format).

24. *See id.* at 963-64 (Alito, J., concurring) (reasoning that a reasonable person would not expect law enforcement to engage in long-term tracking because of the cost and resource demands of traditional surveillance techniques).

25. United States v. Skinner, 690 F.3d 772, 779 (6th Cir. 2012).

26. State v. Earls, 70 A.3d 630, 643-44 (N.J. 2013) (distinguishing *Smith v. Maryland* because people do not buy cell phones to be tracked and do not realize the extent of tracking possible with CSLI); Tracey v. State, No. SC11-2254, 2014 WL 5285929, at *19 (Fla. Oct. 16, 2014) (rejecting the use of duration to decide whether a warrant is required because that would require after-the-fact, case-by-case determinations).

Courts must confront this question when considering the constitutionality of so called "tower dumps." In a tower dump, law enforcement obtains information about hundreds or even thousands of cell phone users whose phones communicated with a given cell tower or set of cell towers.[27] The surveillance windows are short, ranging from a few minutes or hours to perhaps a day or two.[28] The information gathered can include each cell phone's location when it connected to the tower, identifying information about each cell phone, and in some cases the internet addresses and even search terms entered in the cell phone.[29] In 2012, cell service providers reported over 9000 law enforcement requests for cell tower dumps.[30]

Only a few cases have considered whether warrantless tower dumps violate the Fourth Amendment.[31] The two United States Magistrate Judges who have considered the issue so far have reached conflicting results. Magistrate Judge Owsley of the Southern District of Texas, held that tower dumps constitute Fourth Amendment searches and therefore require a warrant.[32] Magistrate Judge Owsley reasoned that the government was seeking a "broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment." In contrast, Magistrate Judge Francis, of the Southern District of New York, held that tower dumps are not pro-

---

27. *See, e.g.*, Ellen Nakashima, *Agencies collected data on Americans' cellphone use in thousands of* '*tower dumps*,' WASH. POST (Dec. 9, 2013), http://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html.

28. *Id.*

29. *Id.*

30. *Id.*

31. Courts are divided on whether the Stored Communications Act, 18 U.S.C. § 2703(d), allows government to request tower dumps. *Compare In re* United States *ex rel.* Order Pursuant to 18 U.S.C. Section 2703(d), 930 F. Supp. 2d 698, 701-02 (S.D. Tx. 2012) (holding that tower dumps must be supported by probable cause and must involve a protocol for handling protected information of innocents), *with In re* Application of the United States for an Order Pursuant to 18 U.S.C. Sections 2703(c)-(d), No. M. 50, 2014 WL 4388397, at *6 (S.D.N.Y. May 20, 2014) (holding that no warrant was required to obtain tower dump, but requiring government to provide additional justification for the time period of the tower dump, and a protocol to handle "the private information of innocent third-parties whose data is retrieved"). For a discussion of the statutory authority or lack thereof for cell tower dumps, *see* 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 (2013) (arguing that 18 U.S.C. § 2703(d) does not authorize courts to issue orders requiring cell tower dumps).

32. *In re* United States *ex rel.* Order Pursuant to 18 U.S.C. Section 2703(d), 930 F. Supp. 2d 698, 701-02 (S.D. Tex. 2012) (holding that tower dumps must be supported by probable cause and must involve a protocol for handling protected information of innocents).

tected by the Fourth Amendment.[33] Magistrate Judge Francis reasoned that there was no long-term tracking of any individual's movements, and relied on both the third party and public exposure doctrines.

If the court considers only the duration of the data tracking, then tower dumps seem an easy case. Tracking for a few minutes or hours, or perhaps even days, seems like the short-term tracking that should not overcome the third party or public exposure doctrines. This approach, however, considers only one dimension of the aggregation—the aggregation going forward in time, which I call "vertical" aggregation. Yet there is another dimension—the aggregation that captures data on the many innocent cell phone users who pass near the cell towers under surveillance, which I call "horizontal" integration.

The question, then, is whether horizontal integration matters for Fourth Amendment purposes. In the GPS and CSLI cases discussed above, the doctrinal starting point was that location information was unprotected by the Fourth Amendment because of the public exposure doctrine or the third-party doctrine. In those cases, the intimate portrait that vertical integration could paint led the courts to depart from the public exposure and third-party doctrines, and grant the location information Fourth Amendment protection. Should purely horizontal integration lead to the same result?

Admittedly, tower dumps may gather vast amounts of information about innocents with no reasonable suspicion whatsoever, but horizontal integration does not paint a portrait of any individual's affairs. Instead, it takes a snapshot of many innocent 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.[34] Although 99.9% of the data will relate to innocents, that alone does not justify departing from the third-party and public exposure doctrines. Video surveillance of a suspect's travels in public would also capture images of many innocent pedestrians, but that would not convert the surveillance into a search for Fourth Amendment purposes. There may be compelling policy arguments to restrict how law enforcement stores and shares the information about innocent people's locations.[35] However, short-

33. *In re* Application of the United States for an Order Pursuant to 18 U.S.C. Sections 2703(c)-(d), No. M. 50, 2014 WL 4388397, at *6 (May 30, 2014) (holding that no warrant was required to obtain tower dump, but requiring government to provide additional justification for the time period of the tower dump, and a protocol to handle "the private information of innocent third-parties whose data is retrieved.").

34. The collection of search terms and other communication's content, of course, would raise a different constitutional question.

35. For cases discussing the need for a protocol to govern handling of innocent people's data, *see* Riley v. California, 134 S. Ct. 2473, 2481 (2014).

term horizontal aggregation will probably be insufficient to remove tower dumps from the third party and public exposure doctrines.

IV. OTHER TYPES OF LOCATION TRACKING TECHNOLOGIES

So far, aggregation has played a role in how courts handled two types of location tracking: GPS and CSLI. Yet nothing about the aggregation principle limits itself to these technologies. As technology creates new ways to track people's movements, courts may have to decide whether they enjoy Fourth Amendment protection.

For example, police departments nationwide have deployed automatic license plate reading systems, and California has become the first state to adopt digital license plates.[36] License plate readers are a combination of hardware and software. The hardware uses high-speed video cameras to capture digital images of each passing vehicle.[37] The software then analyzes the images to extract the license plate number.[38] The software can also store the license plate number along with the date, time, and location of the image, and alert the operator if the system encounters a number on a preloaded "hot list."[39] License plate readers can be mounted in fixed locations like bridges or overpasses, or on vehicles like patrol cars.[40]

Looking a bit further into the future, facial recognition could eventually be used as a tracking technology. Facial recognition technology converts images of faces into sets of measurements, and then compares those measurements against an existing database of measurements to try to find a matching face.[41] The database of facial images can be already in the government's possession, or can be drawn from publicly available websites such as social networking sites.[42] As of 2013, a Department of Homeland

---

36. *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, AM. CIV. LIBERTIES UNION (July 17, 2013), *available at* https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf (reporting on the proliferation of governmental and private industry use of license plate readers to collect and store hundreds of millions of datapoints that include location information about Americans' vehicles).

37. *Id.* at 4-5.

38. *Id.*

39. *Id.*

40. *Id.*

41. Adam Schwartz, *Chicago's Video Surveillance Cameras: A Pervasive and Poorly-Regulated Threat to Our Privacy*, 11 NW. J. TECH. & INTELL. PROP. 47, ¶ 17 (2013).

42. *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing before the United States S., Comm. on the Judiciary, Subcomm. on Privacy, Tech., and the Law* (July 18, 2012) (testimony of Alessandro Acquisti, Associate Professor, Heinz College, Carnegie Mellon University) *available at* http://www.judiciary.senate.gov/download/testimony-of-alessandro-acquisti-pdf.

Security facial recognition program called Biometric Optical Surveillance System (BOSS) was unable to achieve its goal of recognizing faces from 100 meters with 80% to 90% accuracy, and lacked sufficient processing power to compare images against a database quickly enough for security purposes. Yet project researchers predicted that obstacles will fall away as computer processing speed increases. An independent expert estimated that the effort was still at least five years from achieving its goals.[43]

Whether the aggregation principle supports Fourth Amendment protection for new technologies may depend upon the precision with which each technology tracks location. In the early stages of these technologies, license plate or facial recognition tracking will likely yield far less information than CSLI tracking because the collection points will be less densely concentrated than cell towers. The government, therefore, could successfully argue that license plate reader records do not paint a sufficiently intimate portrait of a given individual's affairs.[44]

But either technology could come into far more widespread use. License plate readers could eventually be deployed in dense networks, especially in urban areas.[45] Similarly, facial recognition technology could someday be applied to networks of public and private video surveillance cameras[46] or networks of drones.[47] If these technologies became sufficiently widespread

---

43. Charlie Savage, *Facial Scanning Is Making Gains in Surveillance*, N.Y. TIMES, Aug. 21, 2013, at A1.

44. Chief Justice Gants advanced a similar argument in *Commonwealth v. Augustine*, where he distinguished the CSLI gained from telephone calls from GPS tracking because tracking the location of episodic telephone calls did not create a sufficiently detailed record of the defendant's travels to merit Fourth Amendment protection. Commonwealth v. Augustine, 4 N.E.3d 846, 873 (Mass. 2013) (Gants, C.J., dissenting) ("Telephone call CSLI is episodic, not continuous, and therefore its location points are not a continuous or continual line, but simply a patchwork of points. The extent to which that patchwork can reveal an intelligible picture of where the user goes and whom the user visits, and therefore the degree of intrusion on privacy, will depend both on the frequency of telephone calls and the duration of the CSLI request.").

45. For example, as of 2013, New York City operated a network of nearly 4,000 surveillance cameras and license plate readers in lower Manhattan alone. Amanda Davis, *Smile, You're Probably on Camera: High-tech surveillance networks are getting bigger and smarter*, IEEE ROUNDUP (May 22, 2013), http://theinstitute.ieee.org/ieee-roundup/opinions/ieee-roundup/smile-youre-probably-on-camera-.

46. *See* Schwartz, *supra* note 41, ¶ 17 (discussing Chicago's proposal to add facial recognition to public surveillance cameras). Researchers are now working on techniques to reliably track subjects as they pass from the view of one camera to the next. Kevin Hartnett, *Watching You Between Surveillance Cameras*, BOS. GLOBE, Feb. 3, 2013; Riccardo Mazzon & Andrea Cavallaro, *Multi-camera tracking using a Multi-Goal Social Force Model*, NEUROCOMPUTING, Vol. 100, Jan. 16, 2013, at 41-50, *available at* http://www.sciencedirect.com/science/article/pii/S092523121200327X.

47. Yochi J. Dreazen, *From Pakistan, With Love: The technology used to monitor the*

that they approach the same tracking precision as cell towers, long-term location tracking using license plate readers and facial recognition should receive the same Fourth Amendment treatment as GPS or CSLI tracking.[48]

V. AGGREGATION OF NON-LOCATION INFORMATION

As of December 2014, three federal circuits had heard arguments in surveillance cases involving massive aggregation of non-location data.[49] These cases challenge the NSA's warrantless collection of telephone metadata under section 215 of the USA Patriot Act. Since 2006 the government has relied on section 215 of the USA Patriot Act to collect telephone metadata on telephone calls made to or from telephone numbers in the United States.[50] This metadata includes the originating and terminating telephone number as well as each call's time and duration, but does not include the call's contents.[51] The program stored metadata on United States phone calls for five years.[52]

---

skies over Waziristan is coming to your hometown, NAT'L J., March 10, 2011, *available at* http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313; Ellen Nakashima and Craig Whitlock, *With Air Force's Gorgon Drone 'We Can See Everything'*, WASH. POST, Jan. 2, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html.

48. Facial recognition could be even more precise than CSLI, depending on how densely distributed the collection network was, because we cannot turn off our faces or leave them behind.

49. Oral Argument, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-3994), *available at* http://www.c-span.org/video/?321163-1/aclu-v-clapper-oral-argument-phone-record-surveillance; Oral Argument, Klayman v. Obama, 2013 WL 6598728, at *17-24 (D.D.C. Dec. 16, 2013) (No. 13-0851), *available at* http://www.c-span.org/video/?322507-1/klayman-v-obama-oral-argument-audio; Oral Argument, Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014) (No. 2:13–CV–257–BLW), *available at* https://www.youtube.com/watch?v=fXfKsZVsPtM&feature=youtu.be&t=38m50s (9th Cir. oral argument Dec. 8, 2014).

50. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 141 (2014), *available at* http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf. The bulk telephone metadata program began in 2001, after the September 11 terrorist attacks. From 2001 through 2006 the program proceeded pursuant to presidential authorization. *Id.* at 37.

51. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13–109, 2013 WL 5741573 at *1 n.2 (Foreign Intelligence Surveillance Ct. Aug. 29, 2013) (Eagan, J.). The Foreign Intelligence Surveillance Court noted that the "sole purpose of this production is to obtain foreign intelligence information in support of [redacted] individual authorized investigations to protect against international terrorism and concerning various international terrorist organizations." *Id.* at *1.

52. Scott Shane, *N.S.A. Violated Rules on Use of Phone Logs, Intelligence Court*

The program's challengers have argued that the third-party doctrine should not apply because of the program's massive aggregation of metadata. Lower courts have split on this question. In *Klayman v. Obama*, Judge Leon of the District of Columbia held that the third-party doctrine did not apply, and that the plaintiff's Fourth Amendment claim was likely to succeed on the merits.[53] Judge Leon distinguished *Smith v. Maryland* because of "the evolution in the government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies." Judge Leon relied in part on the massive aggregation of data that the bulk collection program involved. He drew a parallel to the aggregation principle in the concurrences in *United States v. Jones*, and relied on that aggregation to distinguish the bulk telephone metadata collection program from the pen register used for one day in *Smith v. Maryland*.[54]

On the other hand, the Southern District of New York and the Foreign Intelligence Surveillance Court have held that the third-party doctrine shields the bulk metadata collection program from Fourth Amendment scrutiny.[55] In *ACLU v. Clapper*, Judge Pauley of the Southern District of New York held that the NSA's bulk metadata collection was analogous to the pen register in *Smith v. Maryland*.[56] Judge Pauley rejected the idea that building a massive database of every American's telephone records for the past five years changed the analysis: "The collection of breathtaking amounts of information unprotected from the Fourth Amendment does not

---

Found in 2009, N.Y. TIMES, Sept. 11, 2013, at A1. Although the program collected "closer to 100%" of all call records in 2006, as time passed the percentage of phone records collected fell below 30% because the NSA could not keep up with cellphone use. *See also* Ellen Nakashima, *NSA Is Collecting Less Than 30 Percent of U.S. Call Data, Officials Say*, WASH. POST, Feb. 7, 2014, http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html. According to "current and former U.S. officials," the NSA was unable to keep up with expanding cellphone use for several reasons. First, the NSA must prepare its database to handle cellphone data, which contain different data than land-line calls and often contain geolocation data, which the NSA may not receive. And second, NSA resources have been diverted from preparing its databases during 2009 by review and compliance issues arising from breaches documented by the FISC, and from responses to Congressional inquiries in the wake of the Snowden disclosures. Nevertheless, the officials indicated that the government is attempting to restore collection to previous levels. *Id.*

53. Klayman v. Obama, No. 13-0851, 2013 WL 6598728, at *17-24 (D.D.C. Dec. 16, 2013) (Leon, J.).

54. *Id.* at *19.

55. ACLU v. Clapper, 959 F. Supp. 2d 724, 724 (S.D.N.Y. 2013); *see In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *3 (U.S. Foreign Intelligence Surveillance Ct. Aug. 29, 2013).

56. *Clapper*, 959 F. Supp. 2d at 750.

transform that sweep into a Fourth Amendment search."[57] Judge Pauley also rejected the ACLU's argument that the database provided the government with a rich mosaic of each person's life.[58] According to Judge Pauley, because the government cannot query the database without tying that query to an approved target, and the results of the query simply tell the government who has had telephone calls with the target—but not who uses those telephone numbers.[59] The Foreign Intelligence Surveillance Court engaged in a similar analysis of the issue when it approved a production order under the Section 215 bulk telephone metadata collection program.[60] And in *Smith v. Obama*, Judge Winmill of the District of Idaho rejected the Fourth Amendment challenge and reasoned that the case was controlled by *Smith v. Maryland*, even though she recognized that the Supreme Court could eventually take a different view.[61]

If the circuit courts reach the Fourth Amendment argument,[62] they will have to decide whether the third-party doctrine applies. In so doing, they will have to consider whether to distinguish the section 215 program, which collects the times, durations, and incoming and outgoing numbers for most Americans' phone calls over a five-year period, from the pen register in *Smith v. Maryland*, which collected only a one-day record of the numbers dialed, and did not reflect the duration of the call or even whether each call connected.

---

57. *Id.*; *see generally* United States v. Jones, 132 S. Ct. 945, 957, 964 (2012) (stating that short-term tracking of one's public movements did not trigger the Fourth Amendment, but long-term tracking of those same movements did).

58. *Clapper*, 959 F. Supp. 2d. at 750.

59. *Id.*

60. *See, e.g.*, *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *2-3 (Foreign Intelligence Surveillance Ct. Aug. 29, 2013) (Eagan, J.).

61. Smith v. Obama, 24 F. Supp. 3d 1005, 1009-10 (D. Idaho 2014) ("Judge Leon's decision should serve as a template for a Supreme Court opinion. And it might yet. Justice Sotomayor is inclined to reconsider *Smith*, finding it 'ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.' (Citation omitted.) The Fourth Amendment, in her view, should not 'treat secrecy as a prerequisite for privacy.' (Citation omitted.) But *Smith* was not overruled, and it continues—along with the Circuit decisions discussed above—to bind this Court.").

62. The circuit courts could avoid the constitutional question by holding that the text of Section 215 does not authorize bulk collection of all data because nearly all of the data collected would not be "relevant to an authorized investigation" to obtain foreign intelligence information or protect against terrorism or clandestine intelligence activities. 50 U.S.C. § 1861(b)(2)(A). The courts may have an additional incentive to avoid the constitutional question because Section 215 will sunset in 2015. *See* P.L. 112-14 (extending sunset provision until June 1, 2015).

These courts would be justified in extending the aggregation principle to the section 215 program, because the aggregation principle is not limited to the location-specific nature of the data. The *Jones* concurrences relied on the fact that long-term tracking was unexpected and impractical, and painted an intimate portrait of one's affairs. These two rationales apply equally in the case of telephone metadata. Ordinary citizens may expect (at least according to *Smith v. Maryland*) that the government may engage in warrantless collection of telephone numbers dialed for a short period of time, but it strains credulity to suggest that they expect the government to collect and save the metadata about every one of their telephone calls for five years. Similarly, while collecting telephone metadata for a few hours may not tell the government much about the subject, a record of every call that the subject placed, including when and for how long, can paint a startlingly revealing image of that subject's values, beliefs, and associations. A record of the numbers that I call, and that call me, can be even more revealing than a dossier showing where I traveled. For example, driving up to a particular office building or hotel may reveal some information about my affairs, but knowing whom I called in that office building or hotel reveals far more. For those reasons, courts should apply the aggregation principle and reject the government's argument that warrantless collection of long-term telephone metadata is protected by the third-party doctrine.

VI. CONCLUSION

The third party and public exposure doctrines emerged at a time when modern surveillance capabilities were beyond imagination. Today, these previously unimaginable technologies are not merely law enforcement tools; they are essential parts of our daily lives. The GPS tracking and cell phone cases have forced courts to consider how the ongoing digital revolution affects the reasonable expectation of privacy under the Fourth Amendment. Courts have begun to recognize the intrusive potential of long-term aggregation of location data. This aggregation principle, however, will be increasingly tested as emerging technologies share our location and other metadata from our vehicles, our household devices, and even our eyeglasses, watches, and other wearable technologies. This essay has previewed several ways in which this aggregation principle may be tested in the near future. To navigate a principled way forward, courts must rely on the concerns underlying the aggregation principle to adapt long-settled Fourth Amendment doctrines to emerging technologies.