Beyond Mosaic Theory: Understanding Privacy Harms in Smart Cities Through a Complexity Theory Lens

Jesse Woo[*]

Professor Andrew Ferguson's *Structural Sensor Surveillance*[1] comes at a pivotal moment for urbanism in the United States. The country is emerging from a global pandemic that in many instances has hit cities especially hard, altering patterns of living and working in ways that are still in flux. COVID-19 may have accelerated a trend of large, expensive cities losing population to suburbs and smaller urban centers as white-collar workers were freed to seek more space and lower costs of living by the shift to remote work.[2] As the country emerges from the Pandemic, legislators on both sides of the aisle have recognized the pressing need to rebuild American infrastructure

[*] Jesse Woo (J.D. University of Washington 2013) is an attorney and researcher with expertise in smart cities, artificial intelligence and robotics, and cross-border data transfers. He is currently pursuing an M.S. in computer science at Columbia University.

[1] Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47 (2020).

[2] William H. Frey, *America's Largest Cities Saw the Sharpest Population Losses During the Pandemic, New Census Data Shows*, BROOKINGS (June 8, 2021), https://www.brookings.edu/research/the-largest-cities-saw-the-sharpest-population-losses-during-the-pandemic-new-census-data-shows [https://perma.cc/L4C7-9NPY] (analyzing census data to show that the Pandemic accelerated a trend of slowing population loss and depopulation in American cities, with the sharpest losses in the largest and most expensive cities). *But see* Howard Schneider, *Pandemic-Led Decline of U.S. Cities May be Reversing*, REUTERS (May 4, 2021, 9:19 AM), https://www.reuters.com/world/the-great-reboot/pandemic-led-decline-us-cities-may-be-reversing-2021-05-04 [https://perma.cc/PXS9-RMAB].

and technological competitiveness.[3] Further, a rise in violent crime rates in some cities has many Americans increasingly concerned about the issue and in search of new approaches to tackle public safety.[4]

In the middle of these shifting sands, many cities are continuing a movement that began before the Pandemic to become "smart." That is, to integrate digital technologies, and particularly Internet of Things ("IoT")[5] sensors, into their built environments, infrastructure, and municipal governance. Professor Ferguson and others have documented the privacy implications of building ubiquitous, pervasive sensor networks into urban public spaces for years.[6] While the Fourth Amendment has long stood as the principal constitutional mechanism for protecting individual privacy against government intrusion, until recently, the third-party doctrine[7] left a large hole in the Fourth Amendment protections for data collected on individuals in public spaces, and thus smart cities had a privacy problem.[8]

The Supreme Court's embrace of the mosaic theory of privacy[9] in *Carpenter v. United States* has the potential to dramatically change the level of constitutional protection of data in the smart city context.[10] This is an exciting

[3] *See The U.S. Innovation and Competition Act: Senate Passes Sweeping $250 Billion Bill to Bolster Scientific Innovation and Compete with China*, SIDLEY (June 16, 2021), https://www.sidley.com/en/insights/newsupdates/2021/06/an-overview-of-the-united-states-innovation-and-competition-act [https://perma.cc/N993-8RDR]; Jonathan Weisman, Emily Cochrane & Jim Tankersley, *Biden and Senators Reach Broad Infrastructure Deal*, N.Y. TIMES (July 1, 2021), https://www.nytimes.com/2021/06/24/us/politics/biden-bipartisan-infrastructure.html [https://perma.cc/2NK2-3VUK].

[4] Cleve R. Wootson, Jr. & Scott Clement, *Concern Over Crime is Growing — but Americans Don't Just Want More Police, Post-ABC Poll Shows*, WASH. POST (July 2, 2021, 6:00 AM), https://www.washingtonpost.com/politics/poll-crime-police-discrimination/2021/07/01/85be64b6-da79-11eb-9bbb-37c30dcf9363_story.html [https://perma.cc/NT2U-Q76R].

[5] The Internet of Things refers to physical objects with embedded digital technologies that allow them to be networked (connected to the Internet and other devices) and often also allows some amount of sensing or digital interface. IoT devices are often referred to as "smart," such as a smart streetlight or a smart refrigerator. For further explanation see Matt Burgess, *What is the Internet of Things? WIRED Explains*, WIRED (Feb. 16, 2018, 12:40 PM), https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot [https://perma.cc/RFS5-2L84].

[6] *See generally* Ferguson, *supra* note 1 (discussing the effects of smart sensor networks in city environments); Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581 (2014) (discussing the privacy implications of smart cities and their development).

[7] The third-party doctrine, created by the Supreme Court in *United States v. Miller*, dictates that the Fourth Amendment's protections do not extend to information that a person voluntarily discloses to a third-party. United States v. Miller, 425 U.S. 435, 443 (1976).

[8] *See* Jesse W. Woo, *Smart Cities Pose Privacy Risks and Other Problems, but that Doesn't Mean We Shouldn't Build Them*, 85 UMKC L. REV. 953, 953 (2017).

[9] The mosaic theory of privacy posits that privacy harms may arise when multiple pieces of public information are combined to reveal private information about an individual, even though knowing the individual data points by themselves would not constitute a harm because the information is public. It is an attempt to rebalance constitutional privacy protections in a time when people leave highly revealing digital traces in public spaces. For more discussion of mosaic theory, see generally David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381 (2013).

[10] In *Carpenter*, the Court held that accessing cell-site location information from a phone carrier to reconstruct a historical record of a suspect's physical location over several days, without

and necessary development in the Court's Fourth Amendment jurisprudence. The implications of the *Carpenter* decision are potentially quite far reaching,[11] and Professor Ferguson's article adds to a growing and comprehensive body of work exploring its effects in a number of different contexts.

In Part I of this brief Response, I delve a little more deeply into three important takeaways from Professor Ferguson's reading of *Carpenter* and other cases that laid the groundwork for the Court's embrace of mosaic theory: These takeaways constitute a sound analysis of the Court's reasoning, but also highlight what I view as a blind spot in the *Carpenter* decision and the broader academic conversation around the mosaic theory of privacy. The first, most salient point of *Structural Sensor Surveillance* is right there in the title: Smart city surveillance will be part of the structural or built environment rather than purely digital or human-based.[12] This increased use of surveillance technologies in the built environment will result in aggregations of large amounts of data that will pose constitutional challenges for smart cities under *Carpenter*. The second takeaway is his formulation of a three-factor test based on *Carpenter* and other mosaic theory cases for a warrant requirement on public but aggregated data on individuals. The third is the call for a positive law model of smart city privacy.

In Part II, I discuss my ultimate critique of the mosaic theory—that it is a one-dimensional analysis of a multidimensional problem. Both the Court in *Carpenter* and scholarly commentators have emphasized the revealing nature of mass *collection* of data as the primary privacy issue facing mosaic theory. I myself have taken this tack.[13] While I believe that the amount of data collected is a necessary component of the analysis, in this Response I refocus on the distinction and interplay between data collection, collation, and re-use in a data-rich environment that gives rise to privacy harms in such cases. Smart cities are an ideal test case to understand these concepts because of the breadth of data they can collect and that data's relationship to an individual's physical presence in public spaces. I conclude that concepts borrowed from complexity theory, a young scientific discipline characterized by an analysis of network connections and emergent behavior, can be instructive in this area.

a warrant, violated the individual's Fourth Amendment rights. "[T]ime-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). This is despite the fact that the suspect's movements had been in public, and the data was held by a third party, and prior to *Carpenter* the data would have been exempt from the warrant requirement based on the third-party doctrine.

[11] For a discussion of the full implications of *Carpenter*, see generally Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357 (2019).

[12] By "human-based" I mean analogue techniques such as reliance on informants or observation by a human.

[13] *See* Woo, *supra* note 8, at 954–58.

I. SMART CITIES THROUGH THE LENS OF MASS DATA COLLECTION

A. *SENSORS EVERYWHERE RESULT IN MORE DATA THAN EVER BEFORE*

The first vital point Professor Ferguson makes in his article is that the physically embodied nature of smart city surveillance data in quantities is massive enough to trigger Constitutional scrutiny under a mosaic theory of the Fourth Amendment. In some ways, the primary goal of the "smart city" movement has been to transform a largely physical space with new utility using digital technologies.[14] Professor Ferguson refers to this as the "digital layer" of the smart city,[15] but the point is that the digital and physical are inseparable. This integration is part of the challenge that embedded sensor networks present to privacy; when the digital and physical are permanently integrated, it becomes practically impossible to hide one's digital trace in the public sphere.

Professor Ferguson astutely points out that city planners, policy makers, and the firms they contract with will face numerous design choices that will impact personal privacy in a smart city.[16] I read his concern to mainly be with the sheer volume collected by physically embedded smart city sensors. For instance, he emphasizes how city planners and policy makers will make design choices about where and how sensors are deployed in cities because this will impact how *much* data they collect.[17] Mass sensor deployment presents greater challenges for privacy than a single or few sensors because of the breadth of the data collected.[18] This is the central concern of mosaic theory: that connecting a large number of data points will reveal information about an individual even when a single data point would not be considered revealing or privacy-invasive.[19]

Professor Ferguson also highlights a few of what he calls "aggregation problems." The first is the potential to re-identify anonymized data, thereby exposing personal information that was previously thought to be safe.[20] This is a particular problem in smart cities that embed sensors in the physical infrastructure because of massive amounts of data that will then be subject to collect. The second aggregation problem arises from platform creep. As more city services become convenient through a digital platform, the city will have access to more and broader sets of information about residents.[21] His final design axis he calls a choice of localization. Essentially, storing and processing data locally on a device (say a "smart" streetlight equipped with a camera) is

[14] There are some smart city projects that are more purely digital of course, such as the movement to open municipal data.

[15] *See* Ferguson, *supra* note 1, at 64–67.

[16] *Id.* at 53–54.

[17] *See id.* at 54, 67.

[18] *See id.* at 54.

[19] *See* Gray & Citron, *supra* note 9, at 398–99.

[20] *See* Ferguson, *supra* note 1, at 67–68.

[21] *See id.*

more privacy protective than storing and processing centrally.[22] Again, his main concern appears to be the amount of data collected and stored together. Using a local or distributed system avoids the problem of "collecting" large amounts of data in a central repository.

While Professor Ferguson characterizes each of these issues as potential harms flowing from mass collection, I believe he is glossing over an important nuance. For example, though he characterizes re-identification as an aggregation problem, the risk of exposing personal information in re-identification is generally not from collecting large amounts of data from one dataset (say smart utilities), but from joining multiple datasets together.[23] So the risk is not just from mass collection alone, but from using or processing different datasets together. The connection of different datasets and what is done with them is what matters. Compare this to the mosaic theory as expressed in *Carpenter*, where the issue was collecting records of one dataset, cell-site location information ("CSLI"), over an extended period of time.[24]

B. The Carpenter *Test*

The second important takeaway from Professor Ferguson's article is his three-factor based test for a warrant requirement on public but aggregated data on individuals. Professor Ferguson's emphasis on data collection flows from the Court's own analysis in the *Carpenter* decision and is echoed in the reading of other prominent scholars. Professor Ferguson derives three principles from *Carpenter* and related cases for a warrant requirement under the mosaic theory. The first is that "Digital is Different."[25] Fourth Amendment questions regarding digital technologies cannot be easily resolved by comparing them to an analogue counterpart.[26] The digital location tracking by CSLI data is so much more powerful than an analogue technique that the digital case requires different analysis.[27] The second principle is that the Court disfavors arbitrary and "too permeating police surveillance."[28] This refers to surveillance that is overly broad, sweeping up behavior that is unrelated to a criminal investigation for example, and overly deep, tracking individuals with extremely fine granularity.[29] The third principle is that "[a]ggregating and [p]ermanent [t]racking [t]echnologies [r]aise Fourth Amendment

[22] *See id.* at 86

[23] Re-identification by joining public datasets is the approach taken by the founder of the discipline. *See e.g.*, Latanya Sweeney, *Only You, Your Doctor, and Many Others May Know*, TECH. SCI. (Sept. 28, 2015), https://techscience.org/a/2015092903 [https://perma.cc/6VVX-Z278] (demonstrating a technique to re-identify anonymized health data by joining them with public news reports of hospital visits).

[24] *See* Carpenter v. United States, 138 S. Ct. 2206, 2211–13 (2018).

[25] Ferguson, *supra* note 1, at 75.

[26] *Id.*

[27] *Carpenter*, 138 S. Ct. at 2216 (describing CSLI data as "qualitatively different" from telephone and bank records at issue in prior third-party doctrine cases).

[28] Ferguson, *supra* note 1, at 77 (quoting *Carpenter*, 138 S. Ct. at 2214).

[29] *Id.* at 76–77.

[c]oncerns."[30] Professor Ferguson highlights the potential for digital surveillance to aggregate enough data on an individual's activities and movements over time, "creat[ing] a 'time-machine' problem."[31] A related concern is "the ability to collect personal data for one purpose but then have it available to search for" a different purpose later.[32]

Professor Ferguson's three Constitutional principles are similar to the three-part test articulated in Professor Paul Ohm's reading of *Carpenter*. Professor Ohm believes that under *Carpenter*, the government must obtain a warrant when it seeks a category of information that "(1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection."[33] He also highlights the embrace of technological exceptionalism in *Carpenter*, and the rejection of simple analogies to analogue methods of investigation.[34] This focus on the problem of mass collection of data makes sense given the issue presented to the Court. It was addressing whether large amounts of digital data of one parameter (cellphone tower location) triggered a Constitutional search.[35] However, smart cities will face this problem in a much more complicated design space, with more parameters than the Court ever contemplated in *Carpenter*.

C. *POSITIVE PRIVACY LAW AT THE LOCAL LEVEL*

The third important takeaway from Professor Ferguson's article is his call for a positive law model of smart city privacy. Professor Ferguson concludes by calling for a positive law model for Fourth Amendment privacy in smart cities to be implemented through municipal legislation that he calls the "legal layer," as well as through Privacy-by-Design principles.[36] He begins by examining Justice Gorsuch's dissent in *Carpenter*, which explored a property-based positive law model for digital privacy rights vis-à-vis the Fourth Amendment.[37] He then moves on to other non-property-based positive law models such as the California Consumer Privacy Act ("CCPA") and Europe's General Data Protection Regulation ("GDPR") as examples.[38] The CCPA is essentially a notice and consent-based model,[39] while the GDPR is based on human rights principles like those in the Charter of Fundamental Rights of

[30] *Id.* at 77.

[31] *Id.* at 78 (quoting Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 939 (2016)).

[32] *Id.* at 79.

[33] Ohm, *supra* note 11, at 378.

[34] *Id.* at 385–99.

[35] Carpenter v. United States, 138 S. Ct. 2206, 2211–13 (2018).

[36] Ferguson, *supra* note 1, at 102.

[37] *Id.* at 102–04.

[38] *Id.* at 106–07.

[39] *See* California Consumer Privacy Act of 2018 § 3, CAL. CIV. CODE §§ 1798.100–105 (West 2020).

the European Union.[40] Professor Ferguson concludes that a combination of Privacy-by-Design principles governing technical architecture and municipal legislation governing data at the point of collection is the best way to maintain a constitutional floor for Fourth Amendment privacy as cities implement all-encompassing surveillance nets in the name of becoming "smart."[41] He argues that one way to minimize Fourth Amendment problems for smart cities is equipping every sensor in a smart city with "a legal judgment about the use, access, retention, expectations, and security of data to go along with it."[42]

II. Understanding Smart Cities as Distributed Systems

In Part I of this Response, I distilled Professor Ferguson's analysis into three main points: 1) an emphasis on the urban-built environment's role in mass data collection; 2) a formulation of multi-pronged test for Fourth Amendment mosaic theory cases based on Carpenter and antecedent cases; and 3) a call for a positive law for smart city privacy. I believe Professor Ferguson is correct in his emphasis on these three issues as a strict legal analysis of *Carpenter* (and others that he examines but I do not address). However, with respect to the first point, I noted that a narrow focus on the amount of data collected is incomplete. In Part II, I seek to build this point into a critique of the narrowness of mosaic theory, which itself emerged as a response to an overly restrictive view of the Fourth Amendment's constitutional privacy protections. I propose that an approach grounded in an emerging science called complexity theory, or complex adaptive systems, can address this problem and the needs articulated in Professor Ferguson's other two points as well. In essence, I see Professor Ferguson's application of *Carpenter* to the smart city context as an opportunity to rethink and reshape the mosaic theory in its early stages of development, before it ossifies into established doctrine. There is a classic puzzle from ancient Greek philosophy called the Sorites Paradox, or the Paradox of the Heap, that illustrates what I believe to be the problem with the mosaic theory of privacy as it is commonly framed. The paradox goes something like this:

- 1 grain of sand is not a heap
- If 1 grain is not a heap, then adding 1 additional grain of sand does not make a heap, so 2 grains is not a heap
- If 2 grains is not a heap, then adding 1 additional grain of sand does not make a heap, so 3 grains is not a heap
- …

[40] *See* Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) 1.

[41] Ferguson, *supra* note 1, at 111–12.

[42] *Id.* at 111.

- If 999,999 grains is not a heap, then adding grain of sand does not make a heap, so 1 million grains is not a heap
- Therefore 1 million grains of sand is not a heap[43]

This is clearly an absurd result, but this same sort of faulty reasoning can easily infect our thinking about data collection. Collecting one data point of publicly available information is not revealing, nor is two, etc. etc., therefore a million data points is not revealing. The mosaic theory of privacy seeks to reverse this absurd result by pointing out that actually, collecting many publicly available data points on an individual *can* reveal sensitive information, even if each individual datum is considered "safe" for privacy. However, mosaic theory's opponents also have a point: Law enforcement requires clear, predictable lines in order to operate effectively, and this is difficult when the answer to "how much data is too much?" is "a large amount."[44] The *Carpenter* decision has begun to offer some guidance to this question, but judge-made law is typically incremental and slow to take shape. The Court in *Carpenter* and most academic commentators have focused on the "how much data is too much?" question and come up with various multi-factor tests. Time will tell if this approach proves workable for both privacy and public safety.

The issues facing personal privacy in a smart city setting invite us to broaden the scope of the inquiry beyond simply "how much data is too much?" to "what combinations and uses of data are problematic?" Under the Stored Communications Act ("SCA"), law enforcement may access an individual's telephone call records,[45] their bank records,[46] the content of their emails older than 180 days,[47] and their social media posts[48] using only a subpoena. They may also use other techniques like purchasing location data or employing facial recognition with even less transparency and fewer safeguards.[49] There are currently no safeguards when combining these publicly disclosed data sets to form an intimate picture of a suspect's movements and private life beyond the SCA. In fact, the *Carpenter* majority

[43] Dominic Hyde, *Sorites Paradox*, STAN. ENCYCLOPEDIA OF PHIL. (Mar. 26, 2018), https://plato.stanford.edu/entries/sorites-paradox [https://perma.cc/F4DE-4FB6].

[44] *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (arguing against the adoption of the mosaic theory).

[45] 18 U.S.C. § 3121 (2018); *see also* Smith v. Maryland, 442 U.S. 735, 736–37 (1979).

[46] United States v. Miller, 425 U.S. 435, 444–47 (1976).

[47] 18 U.S.C. § 2703. *But see* United States v. Warshak, 631 F.3d 266, 274–75 (6th Cir. 2010) (holding that accessing the content of 27,000 emails from a suspect's internet service provider using a SCA subpoena violated their Fourth Amendment rights).

[48] *See generally* Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 HOW. L.J. 523 (2018) (describing how social media information is used by law enforcement).

[49] Sara Morrison, *A Surprising Number of Government Agencies Buy Cellphone Location Data. Lawmakers Want to Know Why*, VOX (Dec. 2, 2020, 4:25 PM), https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel [https://perma.cc/AP9S-YNCP]; Rebecca Heilweil, *The World's Scariest Facial Recognition Company, Explained*, VOX (May 8, 2020, 11:51 AM), https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement [https://perma.cc/ZA8P-A55N].

took pains to limit the scope of their decision and not to "disturb the application of *Smith* and *Miller*."[50] Because it is the practice of the Court to consider issues narrowly, they are much more likely to examine law enforcement investigation tools and techniques in isolation: pen registers; wiretaps; or even CSLI. But the joining of data sets could slip through the cracks of Fourth Amendment protection with such an approach. One of the chief privacy concerns that I and other commentators have about smart cities is the sheer *variety* of data on an individual's movements and activities that will be collected by a widespread, urban sensor net.[51] It is the combinations of data or the porting from one context to another that need some form of constitutional safeguard, not just the *volume* of data collected by a single type of sensor.

Of course, this is not to say that all joining of public data sets should require a warrant. After all what is a police investigation if not the combining of information to reach a conclusion about the commission of a crime? I am merely asserting that the Court's current approach to a nascent mosaic theory may leave a constitutional blind spot for activity that is significantly privacy-invasive. The solution is to build on *Carpenter*, not jettison it entirely. For instance, I believe that the technological exceptionalism identified by both Professor Ferguson and Professor Ohm will remain relevant.

For these reasons, I prefer not to think about smart city privacy as a web, rather than a heap, where the connections are the most salient feature.[52] I draw this web analogy from complexity theory, or the study of complex adaptive systems ("CAS").[53] Computer scientist and leading CAS scholar Melanie Mitchell defines a complex system as "a system in which large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution."[54] Central to CAS as a new science is the study of network theory, which focuses on the relationship or interaction "between entities rather than the entities themselves."[55] If we understand a city as a complex system, then surveillance (or the ability to recreate fine-grain traces of an individual's movements) is an emergent property of the distributed sensor network that makes a smart city "smart." This shift in thinking allows us to graduate from a law of line-drawing (how

[50] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[51] *See e.g.*, Wajeeha Ahmad & Elizabeth Dethy, *Preventing Surveillance Cities: Developing a Set of Fundamental Privacy Provisions*, 15 J. SCI. POL'Y & GOVERNANCE, no. 1, 2019; Liesbet van Zoonen, *Privacy Concerns in Smart Cities*, 33 GOV'T INFO. Q. 472, 473–74 (2016).

[52] This analogy is a favorite of field of complexity science, which in short is the science of emergent behavior in complex systems. *See* John R. Turner & Rose M. Baker, *Complexity Theory: An Overview with Potential Applications for the Social Sciences*, 7 SYSTEMS, no. 1, 2019, at 1, 11–14.

[53] MELANIE MITCHELL, COMPLEXITY: A GUIDED TOUR 12–14 (2009).

[54] *Id.* at 13. Cities do have a central controller (a government), but nonetheless are comprised of many independent and distributed actors sufficient to warrant a CAS approach. *See e.g.*, ROGER WHITE, GUY ENGELEN & INGE ULJEE, MODELING CITIES AND REGIONS AS COMPLEX SYSTEMS: FROM THEORY TO PLANNING APPLICATIONS 1 (2015).

[55] MITCHELL, *supra* note 53, at 233.

many grains of sand constitute a heap) to a law of effects: Which connections between datasets reveal private or intimate information, and how can the law mediate those connections. Understanding the salient connections should also inform the design choices that will govern data "node by node," as Professor Ferguson calls for.[56] Techniques from complexity theory such as the study of emergent behavior and network theory could be instructive in defining the contours of such a law. Although an exhaustive analysis of complexity theory and its application to privacy is beyond the scope of this brief Response, thinking about a city as a CAS does offer some useful lessons for the design of the "legal layer."

Complexity theory invites us to view cities not as a binary (smart or not) but as an ecology that is evolving. A CAS approach looks at a system as a design space where agents and their environments interact dynamically (i.e., with feedback loops going both ways).[57] Through this lens, a city is a place where constitutional safeguards for privacy can find their level via an iterative design process. I have written elsewhere about how cities are suitable testbeds for IoT technologies in public spaces and their attendant privacy impacts. This is because cities allow for iterative experimentation and innovation while being politically accountable to residents—the people who will experience the privacy effects most acutely.[58] This "nearness" to the citizenry hopefully makes cities more responsive to political safeguards that are necessary for robust privacy protections for data gathered in public. The privacy localism[59] movement has studied how local governments build organizational capacity to govern data and address privacy harms.[60] Understanding cities as design spaces highlights the power they have to guide how and when sensors are used, and also how data from those sensors is governed.

When considering the appropriate positive law model for smart city privacy, the complexity inherent in a smart city suggests that an administrative approach is necessary to handle the dynamism of the system. Such an approach will achieve Professor Ferguson's aim for a review of privacy issues and sensor deployment on the front-end. Decisions about how to design the technical and legal layers of a smart city will depend on both a nuanced understanding of the technical implementation of sensors and a political responsiveness to local privacy concerns. I believe this could take the form of a type of municipal administrative law, where a legislatively empowered

[56] Ferguson, *supra* note 1, at 102.

[57] Julia C. Bendul & Henning Blunck, *The Design Space of Production Planning and Control for Industry 4.0*, 105 COMPUTS. INDUS. 260, 260–62 (2019).

[58] *See* Jesse Woo, Jan Whittington & Ronald Arkin, *Urban Robotics: Achieving Autonomy in Design and Regulation of Robots and Cities*, 52 CONN. L. REV. 319, 376 (2020). *See generally* Jan Whittington et al., *Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government*, 30 BERKELEY TECH. L.J. 1899 (2015) (reviewing Seattle's Open Data Initiative and with a combination of ethnographic interviews of municipal staff and legal analysis of relevant technology vendor contracts).

[59] "Privacy Localism" refers to "privacy regulation at the local level." Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961, 1961 (2018).

[60] *Id.* at 1963–68.

organization or office within the city implements privacy protections at the legal layer.[61] The privacy localism movement has experimented with these types of organizations with some success. We see it in the rise to prominence of municipal surveillance ordinances and the Chief Privacy Officer role in local governments.[62] The cities of Seattle and Oakland, among others, have empowered citizen oversight boards to review the implementation of new surveillance technologies.[63] Municipal privacy officers have had a direct hand in shaping the collection and use of smart city data through their power to review contracts and other government programs for privacy risks.[64] With additional powers (and safeguards) these roles could be even more impactful.

* * *

This Response is making a subtle point about the narrow frame with which the Court in *Carpenter* and commenters like Professor Ferguson have approached the implications of the mosaic theory and the digitization of urban public spaces. As I have mentioned, I find Professor Ferguson persuasive on many points, particularly the three identified in Part I: 1) an emphasis on the urban built environment's role in mass data collection; 2) a formulation of multi-pronged test for Fourth Amendment mosaic theory cases based on *Carpenter* and antecedent cases; and 3) a call for a positive law for smart city privacy. However, in Part II I have argued that focusing on the surveillance implications of individual technologies in isolation as *Carpenter* does will leave a gap in constitutional protections. A CAS based approach would work with and build upon what I see as Professor Ferguson's main points while covering a potential constitutional gap. This shift in perspective may seem a small thing, but as Shannon Mattern thoroughly documents in her book *A City is Not a Computer: Other Urban Intelligences*,[65] the metaphors and framing that we use to think about cities can have profound policy implications. As long privacy is framed around issues with aggregation without also considering combination, discussions about privacy will be mired in line-drawing exercises. While advocates attempt to draw the lines to accommodate a myriad competing interests, governments and firms will continue to collect, collate, and process ever-growing stockpiles of personal data. This will be particularly true in smart cities, but hardly limited to that context. While I believe that data minimization (the opposite of aggregation) is an important part of the privacy conversation, it is past time for privacy advocates and academics to broaden their scope to account for the complex ways that data

[61] Concerns about regulatory capture are always salient when creating new regulatory bodies, which is why appropriate democratic safeguards must be carefully considered.

[62] Rubinstein, *supra* note 59, at 1966.

[63] *See* Meg Young, Michael Katell & P. M. Krafft, *Municipal Surveillance Regulation and Algorithmic Accountability*, BIG DATA & SOC'Y, July–Sept. 2019, at 1, 10.

[64] *See, e.g.*, PRIV. OFF., SEATTLE INFO. TECH. DEP'T, 2018 PRIVACY PROGRAM ANNUAL REPORT 5–6 (2018).

[65] SHANNON MATTERN, A CITY IS NOT A COMPUTER: OTHER URBAN INTELLIGENCES 10–15 (2021).

is used. Complexity theory, with its emphasis on emergent behavior in design ecologies and network connections, offers a way forward.