

American University Washington College of Law

Digital Commons @ American University Washington College of Law

Articles in Law Reviews & Other Academic Journals

Scholarship & Research

11-1-2020

Structural Sensor Surveillance

Andrew Guthrie Ferguson

American University Faculty Account, ferguson@wcl.american.edu

Follow this and additional works at: https://digitalcommons.wcl.american.edu/facsch_lawrev



Part of the [Criminal Law Commons](#), and the [Criminal Procedure Commons](#)

Recommended Citation

Andrew G. Ferguson, *Structural Sensor Surveillance*, 106 Iowa Law Review 47 (2020).

Available at: https://digitalcommons.wcl.american.edu/facsch_lawrev/1983

This Article is brought to you for free and open access by the Scholarship & Research at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in Articles in Law Reviews & Other Academic Journals by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.

American University Washington College of Law

Digital Commons @ American University Washington College of Law

Articles in Law Reviews & Other Academic Journals

Scholarship & Research

11-1-2020

Structural Sensor Surveillance

Andrew Ferguson

Follow this and additional works at: https://digitalcommons.wcl.american.edu/facsch_lawrev



Part of the [Criminal Law Commons](#), and the [Criminal Procedure Commons](#)

Structural Sensor Surveillance

Andrew Guthrie Ferguson*

ABSTRACT: City infrastructure is getting smarter. Embedded smart sensors in roads, lampposts, and electrical grids offer the government a way to regulate municipal resources and the police a new power to monitor citizens. This structural sensor surveillance, however, raises a difficult constitutional question: Does the creation of continuously-recording, aggregated, long-term data collection systems violate the Fourth Amendment? After all, recent Supreme Court cases suggest that technologies that allow police to monitor location, reveal personal patterns, and track personal details for long periods of time are Fourth Amendment searches which require a probable cause warrant.

This Article uses the innovation of smart city structural design as a way to rethink current Fourth Amendment theory. This Article examines the Fourth Amendment search questions that may render structural surveillance unconstitutional, and then offers a legal and practical design solution. The Article argues that Fourth Amendment principles must be built into the blueprints of urban design. At a micro-level, privacy rules must be embedded alongside data collection rules. At a macro-level, a comprehensive legal framework must be integrated with digital design choices. Only by thinking about municipal code and computer code simultaneously can smart cities avoid emerging Fourth Amendment challenges.

I.	INTRODUCTION.....	49
II.	STRUCTURAL SENSOR SURVEILLANCE	52
	A. SMART SENSOR DESIGN.....	54
	1. Built Environment.....	55
	2. Utilities	58
	3. Public Safety	60

* Professor of Law, American University Washington College of Law. Thank you to Steve Bellovin, Marc Blitz, Danielle Citron, Andrew Crespo, David Gray, Stephen Henderson, Orin Kerr, Mary Leary, Cynthia Lee, Ron Lee, Rebecca Lipman, Wayne Logan, Richard Re, Andrew Selbst, Katherine Strandburg, Matt Tokson, Kate Weisburd, Jordan Woods, and the University of Maryland School of Law Legal Theory Workshop participants, the AALS/ABA Criminal Justice Section workshop, and friends at the Privacy Law Scholars Conference for reading an earlier version of this Article.

4.	City-Wide Application Programming Interface	64
B.	SMART SENSOR PRIVACY	67
III.	THE FOURTH AMENDMENT & SMART SENSORS IN PUBLIC	70
A.	A DIGITAL REASONABLE EXPECTATION OF PRIVACY TEST IN PUBLIC	70
1.	Reasonable Expectation of Privacy Principles	72
i.	Principle #1: Digital is Different	75
ii.	Principle #2: The Court Disfavors Arbitrary and “Too Permeating” Surveillance	76
iii.	Principle #3: Aggregating and Permanent Tracking Technologies Raise Fourth Amendment Concerns	77
2.	Fourth Amendment Principles for Structural Surveillance	79
B.	THE FOURTH AMENDMENT APPLIED TO SMART SENSORS	79
1.	Integrated Data Collection Systems: API	80
2.	Visual Surveillance & Object Recognition	82
3.	Public Utilities	84
4.	Smart Streetlights	86
C.	RESPONSES TO THE REASONABLE EXPECTATION OF PRIVACY PUZZLE	87
1.	Public Exposure	87
2.	Consent–Assumption of Risk	88
3.	Type of Data	90
4.	Acquisition of Data	90
D.	CONCLUSION: REASONABLY SMART EXPECTATIONS OF PRIVACY IN PUBLIC	91
IV.	THE FOURTH AMENDMENT & SMART SENSORS AS TRESPASS SEARCHES	91
V.	FOURTH AMENDMENT IN THE DIGITAL CITY: EXCEPTIONS?	95
A.	SPECIAL NEEDS EXCEPTION	95
B.	REASONABLENESS	97
VI.	A DIGITAL PRIVACY-FOCUSED POSITIVE LAW	100
A.	THE POSITIVE LAW MODEL	102
B.	DIGITAL PROPERTY: FOURTH AMENDMENT PROTECTIONS THROUGH PROPERTY RIGHTS	104
C.	POSITIVE LAW: FOURTH AMENDMENT PROTECTIONS THROUGH LAW	106
D.	DIGITAL PRIVACY RIGHTS: FOURTH AMENDMENT EXPECTATIONS THROUGH COMPUTER CODE	108

E.	DESIGNING THE “LEGAL LAYER”	111
VII.	CONCLUSION	112

I. INTRODUCTION

Sensors are now embedded in the infrastructure of American cities. Smart roads, smart streetlights, smart homes, and smart electrical grids offer entirely new means of monitoring citizens living in “smart cities.”¹ This municipal data collection involves state actors surveilling citizens, literally tagging them, touching them, and tracking them—all the while aggregating personal data for government purposes over long periods of time.

Unfortunately, and a bit awkwardly, these digital contacts collide with Fourth Amendment “search”² principles because the modern Fourth Amendment turns on issues such as tracking, touch, aggregated personal data collection, and “too permeating police surveillance.”³ Physical intrusion,⁴ expectations of privacy,⁵ and a fear of arbitrary surveillance⁶ rest at the core of Fourth Amendment search cases.

This Article asks the question of what happens when the architecture of a digital future is built on an analog Fourth Amendment framework. Are smart city sensors unconstitutional because they inadvertently allow for aggregated government collection of personal data without a probable-cause search warrant? Will smart cities become Fourth Amendment-free zones with ubiquitous tracking and no expectations of privacy? Or can design principles

1. See, e.g., BEN GREEN, *THE SMART ENOUGH CITY: PUTTING TECHNOLOGY IN ITS PLACE TO RECLAIM OUR URBAN FUTURE* 1–14 (2019).

2. The Fourth Amendment provides that

[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

3. *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)); see *id.* at 2211–20.

4. *United States v. Jones*, 565 U.S. 400, 404–05 (2012) (finding that “[t]he Government[’s] physically occup[ying] private property for the purpose of obtaining information” was a search for Fourth Amendment purposes).

5. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (“My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”).

6. See *United States v. Martinez-Fuerte*, 428 U.S. 543, 554 (1976) (articulating that the purpose of the Fourth Amendment is to protect against “arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals”).

be created using smart sensor technology to respond to these Fourth Amendment concerns?

The short answer is that under current Supreme Court doctrine, automated, continuous, aggregated, long-term acquisition of personal data by smart sensors triggers Fourth Amendment scrutiny and thus could violate the Constitution.⁷ The longer answer recognizes the need for a new theory of how the Fourth Amendment can fit the digital age as well as new design rules for smart sensor technologies.⁸

This Article uses the innovation of smart sensor structural design as a way to rethink current Fourth Amendment doctrine. It argues that Fourth Amendment principles must be built into the blueprints of urban planning. At a micro-level, privacy rules must be embedded alongside data collection rules. At a macro-level, a comprehensive legal framework must be integrated with digital design choices. This is not a simple process because the technologies vary in terms of scope, scale, connectivity, and purpose. But it is important because the smart design rules developed today will shape the privacy expectations of tomorrow.

Imagine what the smart sensor-enabled city of the future can do. It can monitor where citizens walk, drive, live, play, eat, what medical services they need, what they buy, what they like, who they visit and associate with, and who they love.⁹ The city becomes the platform for data collection.¹⁰ The data is potentially available at a granular level to track individuals, at an associational level to map networks of contacts, and at a pattern level to monitor the number of people involved in any activity. This “sensorveillance” data is tied to geography, time, and date, and can be visualized across days, weeks, or years.¹¹

7. See *infra* Part III (discussing the Fourth Amendment analysis of smart cities).

8. See *infra* Part VI (detailing a digital positive law to address the shortcomings of existing Fourth Amendment doctrine).

9. See *infra* Part II (detailing the rise of smart city technology); Jan Whittington, *Remembering the Public in the Race to Become Smart Cities*, 85 UMKC L. REV. 925, 927 (2017) (“Though the intended consequence of smart city technology may be efficiency, the unintended consequence may be surveillance.”); see also Janine S. Hiller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309, 314–15 (2017) (discussing the vast variety and scope of “big data” collected in smart cities).

10. Andrew Guthrie Ferguson, *When Citizens Become the Product*, PRAWFSBLAWG (Apr. 11, 2018, 3:03 PM), <https://prawfsblawg.blogs.com/prawfsblawg/2018/04/when-citizens-become-the-product.html> [<https://perma.cc/7CVH-D6SB>] (describing the problem of selling public data to private companies in exchange for public services and benefits).

11. I coined the term sensorveillance in *The “Smart” Fourth Amendment*. See Andrew Guthrie Ferguson, *The “Smart” Fourth Amendment*, 102 CORNELL L. REV. 547, 551 n.15 (2017) [hereinafter Ferguson, “*Smart” Fourth*]. (“The term ‘sensorveillance’ owes its inspiration to the term ‘dataveillance.’” (quoting M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN. ST. L. REV. 809, 822 (2010))); see also Justin Jouvenal, *Commit a Crime? Your Fitbit, Key Fob or Pacemaker Could Snitch on You.*, WASH. POST (Oct. 9, 2017), https://www.washingtonpost.com/local/public-safety/commit-a-crime-your-fitbit-key-fob-or-pacemaker-could-snitch-on-you/2017/10/09/f35a4f30-8f50-11e7-8df5-c2e5cf46c1e2_story.html [<https://>

And then think about what police wish to do in the name of public safety. Using data, police can monitor individuals thought to be involved in criminal activities, associated groups involved in networks of crime, and places of criminal risk.¹² They can seek to understand points of environmental vulnerability, victims most at risk, and patterns of crime.¹³ They can seek to understand crime data in terms of geography, time, people, and patterns, and visualize it across the days, weeks, or years.¹⁴ Using smart sensor technologies, police will possess a powerful investigative “time machine.”¹⁵ Crimes can be investigated by rolling back the digital trails to see who might have been near the scene, what they did, and how they acted. Police response time will improve, witnesses will be found more quickly, and the raw material of investigative clues will be memorialized in digital form.¹⁶ Depending on the level of granularity and the anonymity protections baked into the system, this capability will change how police do their jobs and how citizens act. Depending on how the sensors are configured, these city environments can either create a Fourth Amendment search problem or avoid one.

Intriguingly, the flexibility of the technology may also hint at a solution to the Fourth Amendment puzzle. Because the digital architecture must be built from scratch, digital property rights and social expectations of privacy can be written into code—both legal code and computer code. This moment of physical and digital construction opens the possibility for a legal reconstruction of privacy, potentially offering more protections, more transparency, and more democratic engagement about the balance between

perma.cc/48JZ-C7N7] (using the term *sensorveillance* to describe surveillance among the Internet of Things).

12. See generally Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOCIO. REV. 977 (2017) (analyzing the impact of big data analytics on the Los Angeles Police Department’s surveillance practices); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015) (analyzing the impact of big data policing on the Fourth Amendment “reasonable suspicion” standard); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014) (discussing the Fourth Amendment implications of big data-driven predictive policing, mass surveillance systems, and DNA databanks); Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109 (2017) (discussing the discriminatory effects of predictive policing and proposing the use of “algorithmic impact statements” for early and transparent consideration of these effects); Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947 (suggesting strategies for fair and effective use of algorithms in predictive policing).

13. See sources cited *supra* note 12.

14. See sources cited *supra* note 12.

15. Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 937 (2016) (coining the “time machine” metaphor in the Fourth Amendment context).

16. See Sidney Fussell, *Kentucky Is Turning to Drones to Fix Its Unsolved-Murder Crisis*, ATLANTIC (Nov. 6, 2018), <https://www.theatlantic.com/technology/archive/2018/11/police-drone-shots-potter-kentucky-gun-911-ai/574723> [<https://perma.cc/VgKT-LQJU>]; Jouvenal, *supra* note 11 (describing “how Internet-connected, data-collecting smart devices such as fitness trackers, digital home assistants, thermostats, TVs and even pill bottles are beginning to transform criminal justice”).

security and liberty in urban spaces.¹⁷ In many ways, the design of smart sensors in urban infrastructure offers an opportunity to redesign Fourth Amendment protections by creating a digital positive law that can reshape existing Fourth Amendment theory and also, where appropriate, forbid certain privacy-invading practices.

Part II of this Article addresses the rise of structural surveillance in city environments, examining how smart sensors are being embedded in the built environment, regulating utilities, augmenting public safety, and connecting denizens through a networked digital layer. The next three Parts examine how the Fourth Amendment addresses this world of smart sensors. Part III offers a new theory of Fourth Amendment privacy in public arising from recent Supreme Court cases involving digital technologies, which collectively establish what this Article calls a “digital reasonable expectation of privacy test in public.” These recent Supreme Court cases offer a fractured, but functional new framework to address the different privacy issues arising from smart sensor technologies in public. Part IV examines the recently rediscovered Fourth Amendment “trespass” test as applied to smart city technologies. This test supplements the reasonable expectation of privacy test and presents novel problems in the context of smart infrastructure. Part V addresses possible rejoinders to these arguments and possible exceptions to the Fourth Amendment. Finally, Part VI suggests an alternative Fourth Amendment theory tied to a quasi-positive law approach built around digital rights.

II. STRUCTURAL SENSOR SURVEILLANCE

To speak of sensor surveillance is to speak of both present capabilities and future plans. Smart sensors currently exist in streetlights, cars, and homes, but entire industries are being designed to capitalize (monetarily and technologically) on sensor-driven efficiencies in the built urban environment.¹⁸

A “smart sensor” is a generic term for a device that can take inputs from the physical environment, collect data, and share it with other similarly connected devices.¹⁹ For example, a smart pollution sensor might sample water or air quality from the physical environment and convert it to a readable score, and then share that information with a collecting sensor.²⁰ Smart

17. See *infra* Part VI (describing how to reimagine smart cities with more privacy protection).

18. See Joe Carmichael, *Amazon Previews Its Autonomous “Just Walk Out” Grocery Stores*, INVERSE (Dec. 5, 2016, 11:33 AM), <https://www.inverse.com/article/24730-amazon-go-grocery-shopping> [<https://perma.cc/SPBD-YDLT>]; Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1924–25, 1939 (2017) [hereinafter *Walls*]; Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 WAKE FOREST J.L. & POL’Y 339, 345 (2015).

19. See Dalmacio V. Posadas, Jr., *After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 75–77 (2017) (describing the role of smart sensors in the Internet of Things).

20. See Kelly Kennedy, Note, *19th Century Farming and 21st Century Technology: The Path to Cleaner Water*, 47 ARIZ. ST. L.J. 1385, 1408–09 (2015) (discussing the use of sensors to monitor

sensors tend to be small, low cost, wireless, energy efficient, and can be combined with other devices and networked together.²¹ So, for example, a single smart pollution sensor could be combined with thousands of other sensors to offer a reading of air quality for an entire city.²² The network of smart sensors allows physical devices to communicate with other sensors. The result is the potential to track almost anything that can be reduced to its digital signature.

These smart sensors promise a new form of “algorithmic governance”²³—to more efficiently provide scarce resources like electricity and water and to monitor public safety or emergency situations.²⁴ To work as planned, cities must collect sensor data of all types of inputs, analyze it, record it, and act on it as quickly as possible. The data sources can be built into the architecture and infrastructure of the city buildings or streets. Sensors can be set to automatically and continuously record and communicate with other sensors. Of course, this data-driven governmental control comes at the expense of traditional notions of privacy and a hands-off approach to government.²⁵

The next Section examines structural surveillance capabilities focusing on design choices that might be relevant to city planners or citizens thinking about how to evaluate digital sensors in their cities.

water pollutants and environmental contamination); Skip Descant, *California's Bay Area to Measure Air Quality Block-by-Block*, GOV'T TECH. (Jan. 17, 2020), <https://www.govtech.com/analytics/Californias-Bay-Area-to-Measure-Air-Quality-Block-by-Block.html> [<https://perma.cc/LAQ7-YNXG>]; Solomon Serwanjja, *Kenya Pollution: How Air Sensors Are Helping People Fight Pollution*, BBC NEWS (Dec. 5, 2019), <https://www.bbc.com/news/world-africa-50647465> [<https://perma.cc/FV8C-MS44>].

21. See, e.g., FED. TRADE COMM'N, *INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD* 5–6 (2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> [<https://perma.cc/WSYD-SGAg>].

22. See Liesbet van Zoonen, *Privacy Concerns in Smart Cities*, 33 GOV'T INFO. Q. 472, 472 (2016) (discussing pollution sensors in the city of Rotterdam).

23. Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 114 (2018) (“Use of big data and predictive algorithms is a form of governance—that is, a way for authorities to manage individual behavior and allocate resources. Implementation of algorithms at the local level is part of a broader move towards data-driven decision making, and must be understood in the context of the ‘smart city’ agenda.” (footnote omitted)).

24. Hiller & Blanke, *supra* note 9, at 311 (“Government agencies, quasi-governmental utilities, commercial interests, and others will trace, analyze, and predict the movements, needs, and scarcities of citizens in the city in order to manage resources and protect the community most effectively.”); Saraju P. Mohanty, Uma Choppali & Elias Kougiannos, *Everything You Wanted to Know About Smart Cities: The Internet of Things Is the Backbone*, IEEE CONSUMER ELECS. MAG., July 2016, at 60, 60 (“As a simplistic explanation, a smart city is a place where traditional networks and services are made more flexible, efficient, and sustainable with the use of information, digital, and telecommunication technologies to improve the city’s operations for the benefit of its inhabitants.”).

25. Hiller & Blanke, *supra* note 9, at 312 (“The smart city’s pervasive use of sensors and citizen surveillance threatens to create a society that ignores boundaries for individual privacy.”).

A. SMART SENSOR DESIGN

Integrated smart sensors are shaped by choices in engineering and design. Sensors can be localized or networked together. Data can be stored and de-anonymized at the source, or aggregated in a centralized location. The sensors can be place-based, person-based, thing-based, or all three. Each design choice offers an important moment to restrict or expand the scope and scale of data being collected by the government.

Such design choices can directly impact the usefulness of the data collected. For example, a single sensor can identify how many automobiles drive past a particular street. Data can be stored—or “siloe”—on the device and collected monthly to determine traffic density at a particular place over that specific time period. Or thousands of such sensors can be networked together to provide a city-wide reading of traffic patterns.²⁶ These sensors again can be siloe or aggregated depending on how the data is collected. If integration were the goal, each of the sensors could provide real-time outputs of traffic patterns. The sensors could be placed in city infrastructure (e.g., curbs or streetlights), or on cars (i.e., license plates), or even captured by video surveillance and digitally converted into traffic density readings. A single sensor on a single street may not seem a significant privacy concern, but a city-wide aggregated sensor system may suggest a new type of surveillance capacity.

Choices also arise about the capacity to track individual objects within the system. One could set up a traffic system to anonymize all the cars that pass by, treating them as undifferentiated physical objects.²⁷ Or one could provide a unique identifier for each car, albeit not associated with a particular person (like an IP address in the computer context).²⁸ Or one could identify a

26. Whittington, *supra* note 9, at 928 (“Smart technologies offer the promise of real-time data with remarkably thick flows of information. . . . Instead of traffic counts estimated from travel diary surveys and the occasional placement of cables that record the numbers of cars as they roll across each cable, traffic operations personnel can have the real-time traces of persons through the road networks of the city, sent in continuous signals from their automobiles, phones, and computers to networked Wi-Fi and Bluetooth sensors.”).

27. See Jonathan M. Gitlin, *Concerned About Connected Car Privacy? Bluetooth Sensors Used to Track Traffic*, ARS TECHNICA (July 24, 2017, 10:20 AM), <https://arstechnica.com/cars/2017/07/a-danish-town-has-been-using-bluetooth-sensors-to-track-traffic-patterns> [<https://perma.cc/96MF-YTXC>] (describing the process behind Bluetooth tracking of real-time traffic patterns); OTONOMO, A PRIVACY PLAYBOOK FOR CONNECTED CAR DATA 15–16 (2019), <https://fpf.org/wp-content/uploads/2020/01/OtonomoPrivacyPaper.pdf> [<https://perma.cc/7MRV-F52D>] (explaining how car data can be used while still retaining privacy).

28. See Klaus Philipsen, *How Will Technology Change Cities?*, 7 U. BALT. J. LAND & DEV. 91, 94–95 (2018) (“Traffic signals can be equipped with sensors as well to coordinate traffic with sophisticated programs which respond to volume not only at one intersection, but within an entire network of roads and could successfully optimize traffic flow and even differentiate between cars and transit.”). *But see* John R. Quain, *Cars Suck up Data About You. Where Does It All Go?*, N.Y. TIMES (July 27, 2017), <https://www.nytimes.com/2017/07/27/automobiles/wheels/car-data-tracking.html> [<https://perma.cc/ZFY6-R7GR>] (noting that “radar sensors, diagnostic

particular car allowing for a tracking capacity that might be useful for toll collection, mileage taxes, or parking enforcement tied to individual driving use.²⁹ Those collection mechanisms could also remain siloed and isolated, or aggregated and trackable. The result, again, turns on how the system is designed at the outset.

As a simplified example of the future challenges with smart sensor design, the following are possible uses of smart sensor technology, focusing on the overlapping categories of (1) the built environment (infrastructure); (2) utilities (services); (3) public safety (security); and (4) a city-wide networked digital interface (application program interface) that has the potential to connect all of the above.

1. Built Environment

Traditional cities are built with concrete, steel, asphalt, and glass. Yet smart cities can reimagine this physical reality as a data collection system by placing digital sensors within the built environment.³⁰ These sensors will continually collect data about physical structures, residents, and the natural world in order to more efficiently provide basic government services and monitor civic activity.

Longstanding urban fixtures like streetlights, curbs, smart signs, and sidewalks are being equipped with sensors or visual tracking technologies to count the number of cars or people who pass by.³¹ This information can be very helpful to ease traffic congestion, including providing real-time information on blocked traffic lanes³² or dangerous potholes.³³ Sensors can

systems, in-dash navigation systems and built-in cellular connections” in cars can record sensitive data, and “[t]he United States generally does not ensure that companies strip out names or other personal details [from that data]”).

29. See James Doubek, *Digital License Plates Roll Out in California*, NPR (June 1, 2018, 8:14 AM), <https://www.npr.org/sections/thetwo-way/2018/06/01/616043976/digital-license-plates-roll-out-in-california> [<https://perma.cc/3P4V-X78S>].

30. Mohanty et al., *supra* note 24, at 62 (“The infrastructure of the smart city includes physical aspects, ICT [information communication technology], and services. The physical infrastructure is the real physical or structural entity of the smart city, including buildings, roads, railway tracks, power supply lines, and water supply system.”).

31. MIKE BARLOW & CORNEALIA LEVY-BENCHETON, *SMART CITIES, SMART FUTURE: SHOWCASING TOMORROW* 51–72 (2018).

32. 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, 955 (2017) (“[I]n Kansas City, Sensity’s LED streetlights . . . have visual sensors that can track when a vehicle is blocking the path of the new streetcar and alert authorities to have it ticketed and removed.”).

33. Mickey McCarter, *Smart Cities Connect 2018: Cameras, Sensors Turn City Vehicles into Smart Assets*, STATETECH (Mar. 28, 2018), <https://statetechmagazine.com/article/2018/03/smart-cities-connect-2018-cameras-sensors-turn-city-vehicles-smart-assets> [<https://perma.cc/2SBN-2WAG>] (showing how city vehicle “data can be used to identify potholes, locate damaged traffic signs, and discover other problems”).

also ease toll collection and parking enforcement.³⁴ For instance, Santander, Spain installed 12,000 sensors under the streets or on street lamps to assist with parking and save electricity.³⁵ Santander residents can use smartphone apps to find open parking spots, road closures, and learn about other city services.³⁶

Smart cars will not only be able to drive themselves, but will also be able to provide real time information about paths and patterns of the automobiles around them.³⁷ Car services like Lyft or Uber already provide the same type of informational awareness for those in the sharing economy, mapping not only their routes but the entire city's traffic patterns.³⁸ Bike and scooter services similarly reveal local community travel habits.³⁹ These transportation technologies do not just offer convenience and flexibility, but volumes of data about travel patterns, preferences, and urban space all collected by smart sensors. Similarly, smart subway cards, bus passes, and road tolls provide measurable data on the number of people using public transport or roads at any given time and across all time.⁴⁰

34. Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 ME. L. REV. 397, 404–10 (2014) (describing states' use of Automated License Plate Readers ("ALPR") for law enforcement and toll revenue collection).

35. Hiller & Blanke, *supra* note 9, at 317–18.

36. *Id.*

37. See Alexander B. Lemann, *Coercive Insurance and the Soul of Tort Law*, 105 GEO. L.J. 55, 56 (2016) ("[A modern telematics device] collects data for wireless transmission to an insurance company, including how fast your car is moving, when, for how long, and in some cases where you drive, and the g-forces your car experiences as it accelerates, brakes, or maneuvers around turns.").

38. Hemant Bhargava, David S. Evans & Deepa Mani, *The Move to Smart Mobile Platforms: Implications for Antitrust Analysis of Online Markets in Developed and Developing Countries*, 16 U.C. DAVIS BUS. L.J. 157, 164 (2016) ("[R]ide sharing services such as Uber use large amounts of historical data (such as traffic patterns and sharing patterns) as well as real-time data (such as traffic conditions and the location and preferences of riders) as the fuel for intelligent algorithmic search and optimization programs that produce ride-sharing allocations in real-time."); Matt McFarland, *Uber and Lyft Battle Los Angeles over the Future of Transportation*, CNN BUS. (May 23, 2019, 9:58 AM), <https://www.cnn.com/2019/05/23/tech/uber-lyft-cities-data/index.html> [<https://perma.cc/D28Q-G6DB>].

39. See Benjamin Schneider, *Why Little Vehicles Will Conquer the City*, BLOOMBERG CITYLAB (June 21, 2018, 2:18 PM), <https://www.bloomberg.com/news/articles/2018-06-21/a-guide-to-little-vehicles-the-future-of-urban-mobility> [<https://perma.cc/3EKZ-A95U>]; David Zipper, *Cities Can See Where You're Taking that Scooter*, SLATE (Apr. 2, 2019, 5:45 AM), <https://slate.com/business/2019/04/scooter-data-cities-mds-uber-lyft-los-angeles.html> [<https://perma.cc/68PY-D28H>].

40. Colin Harrison & Ian Abbott Donnelly, *A Theory of Smart Cities*, PROC. 55TH ANN. MEETING INT'L SOC'Y SYS. SCIS., July 2011, at 1, 3 ("A road tolling system, for example, provides large amounts of precise, 'real-time' information about the movement of vehicles through toll gates. Offline analysis of historical traffic data can find patterns that can be leading indicators of the risk of congestion occurring in specific city districts. When such patterns are then found in 'real-time' data, they provide a warning period that enables managers to adjust the traffic management system to prevent such congestion occurring."); see also Kelsey Finch & Omer

Built along smart roads, smart homes and apartments will be filled with communication-enabled devices. Living in those homes will be people with all sorts of smart, data-generating gadgets. Even in a non-smart city, digital natives leave a revealing data trail of their habits. Personal patterns are exposed by smart alarm systems, ovens, coffee makers, toothbrushes, and Amazon Echo commands that track daily life.⁴¹ Wi-Fi-enabled computers and tablets reveal times at work and time off for play, along with Internet queries, news preferences, and entertainment choices.⁴² Biometric devices reveal our health and exercise habits.⁴³ Internet Service Providers (“ISPs”) track every search we make and every show we watch.⁴⁴ Smart security services monitor our homes and report on suspicious people.⁴⁵ New consumer-friendly products like video-enabled Ring doorbells offer “surveillance as a service” that can turn a home into a networked neighborhood security network.⁴⁶ Simply put, our structural physical environment is digitally exposed like never before—an attractive target for smart city designers seeking to sell smart apartments, and smarter lifestyles.

Tene, *Welcome to the Metropicon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1586 (2014) (“Electronic toll collection systems have become the norm in both urban and non-urban spaces, using RFID tags and video cameras so that drivers can prepay tolls, eliminating the need to stop at toll plazas.”).

41. See Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 88–90, 101, 135 (2014); see also *id.* at 120 (“The technical problem created by the Internet of Things is that sensor data tend to combine in unexpected ways, giving rise to powerful inferences from seemingly innocuous data sources. Put simply, in a world of connected sensors, ‘everything may reveal everything.’ Sensor data are so rich, accurate, and fine-grained that data from any given sensor context may be valuable in a variety of—and perhaps all—other economic or information contexts.”).

42. See John Herrman, *Google Knows Where You’ve Been, but Does It Know Who You Are?*, N.Y. TIMES MAG. (Sept. 12, 2018), <https://www.nytimes.com/2018/09/12/magazine/google-maps-location-data-privacy.html> [<https://perma.cc/TPB6-L3XZ>].

43. Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, FORBES (June 19, 2014, 1:26 PM), <https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance> [<https://perma.cc/M828-VFPN>].

44. See, e.g., Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1420, 1437–39; Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707, 1769 (2013).

45. Krystal Rogers-Nelson, *Robotic Monitoring and AI-Powered Surveillance Are Changing Home Security*, VENTUREBEAT (Oct. 12, 2017, 2:10 PM), <https://venturebeat.com/2017/10/12/robotic-monitoring-and-ai-powered-surveillance-are-changing-home-security> [<https://perma.cc/UTAg-AFBS>].

46. Alison Griswold, *Amazon Wants to Sell “Surveillance as a Service,”* QUARTZ (June 20, 2019), <https://qz.com/1648875/amazon-receives-us-patent-for-surveillance-as-a-service> [<https://perma.cc/2MKE-VV3N>]; *Amazon’s Ring Doorbell Camera Is Pretty Much the Trojan Horse of Home Privacy*, MARKETPLACE TECH (Nov. 22, 2019), <https://www.marketplace.org/shows/marketplace-tech/amazons-ring-doorbell-camera-is-pretty-much-the-trojan-horse-of-home-privacy> [<https://perma.cc/BXT8-BX3M>]; Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019, 5:53 PM), <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach> [<https://perma.cc/L3W4-GCRA>].

2. Utilities

In smart cities, finite resources like water, electricity, and gas can be regulated through sensor data. For example, cities are looking into smart energy grids to predict the fluctuating level of energy consumption at different times of the year (or even times of day).⁴⁷ Regulating water use, waste, and other necessary services can be managed more responsibly with better data. For example, instead of having streetlights that stay on all night, smart streetlights might only turn on in response to the presence of a person or vehicle.⁴⁸ Or, instead of having a weekly trash day, trash receptacles might automatically alert the need for disposal, and trash trucks would find the most optimal routes for pick-up.⁴⁹ The city-state of Singapore, for example, has experimented with sensors to track energy usage and personal waste.⁵⁰ Songdo, South Korea, an urban center inspired by smart cities, uses a vast camera system to monitor traffic and crime⁵¹ and even has “[a] citywide

47. See Finch & Tene, *supra* note 40, at 1588 (“One of the most visible ‘smart’ infrastructure systems today is the smart grid, which allows utilities, users, and other third parties to monitor and control electricity use.”). See generally ANN CAVOUKIAN & JULES POLONETSKY, *PRIVACY BY DESIGN AND THIRD PARTY ACCESS TO CUSTOMER ENERGY USAGE DATA* (Jan. 2013) [hereinafter CAVOUKIAN & POLONETSKY, *THIRD PARTY ACCESS*], <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-thirdparty-CEUD.pdf> [<https://perma.cc/LD58-KHR3>] (discussing third-party aggregation of customer energy information and related privacy issues); INFO. & PRIV. COMM’R OF ONT., *PRIVACY BY DESIGN: ACHIEVING THE GOLD STANDARD IN DATA PROTECTION FOR THE SMART GRID* (2010) [hereinafter INFO. & PRIV. COMM’R OF ONT., *GOLD STANDARD*], https://www.smartgrid.gov/document/privacy_design_achieving_gold_standard_data_protection_smart_grid [<https://perma.cc/REW5-QRWX>] (discussing the development of Ontario’s Smart Grid and related privacy issues).

48. See Luis Gomez, *Thousands of San Diego Street Lights Are Equipped with Sensors and Cameras. Here’s What They Record*, SAN DIEGO UNION-TRIB. (Mar. 18, 2019, 5:20 PM), <https://www.sandiegouniontribune.com/opinion/the-conversation/sd-san-diego-street-light-sensors-how-they-work-20190318.htmlstory.html> [<https://perma.cc/Z9M8-XAX8>].

49. Nathalie Vergoulas, *Smart Cities: Is Cutting-Edge Technology the Method to Achieving Global Sustainable Goals?*, 32 J. ENV’T L. & LITIG. 271, 283 (2017) (“Sensors utilize radio frequency and Wi-Fi, which provides data to a central system that advises sanitation workers of the trash level to then prepare an optimal trash removal route.”); see also Patience Haggin, *How a ‘Smart’ Trash Bin Can Transform City Garbage Collection*, WALL ST. J. (May 21, 2019, 11:26 AM), <https://www.wsj.com/articles/how-a-smart-trash-bin-can-transform-city-garbage-collection-11558452400> [<https://perma.cc/24LZ-2LHS>] (“Tests conducted by the [smart trash] bin makers and several city waste departments have shown that emptying trash containers before they are full tends to make collecting waste much more efficient.”); Colin Campbell, *Notice New ‘Smart’ Trash Cans in South Baltimore? They’re Part of a Citywide Upgrade*, BALT. SUN (Sept. 18, 2018, 2:35 PM), <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-smart-trash-cans-20180918-story.html> (discussing Baltimore’s first smart trash cans).

50. Nick Summers, *Inside Google’s Plan to Build a Smart Neighborhood in Toronto*, ENGADGET (Mar. 16, 2018), <https://www.engadget.com/2018/03/16/alphabet-google-sidewalk-labs-toronto-quayside> [<https://perma.cc/QFB8-YC74>].

51. See Ross Arbes & Charles Bethea, *Songdo, South Korea: City of the Future?*, ATLANTIC (Sept. 27, 2014), <http://www.theatlantic.com/international/archive/2014/09/songdo-south-korea-the-city-of-the-future/380849> [<https://perma.cc/44EG-UC98>].

pneumatic refuse system [that] sucks garbage below the surface and into a remote sorting center, eliminating the need for dirty garbage trucks.”⁵²

Environmental data can also be collected, monitoring air quality, pollution, and even the perceived “happiness” of a particular community. “In the Dutch city of Rotterdam, . . . the regional environment agency produces hourly data about air quality from sensors across greater Rotterdam resulting in over 175,000 observations per year.”⁵³ In Chicago, the city government rolled out an “‘Array of Things’ network . . . already labeled ‘Your Big (Friendly) Brother,’ . . . consist[ing] of ‘highly visible, aesthetically pleasing, one-foot-square boxes mounted on light poles that track environmental conditions around them.’”⁵⁴ In London, a virtual city dashboard displays city traffic cameras.⁵⁵ Collected, this type of sensor data can allow cities to better use resources and respond to quality-of-life problems. Because the networked data can be centrally analyzed and acted upon in close to real time,⁵⁶ it can help city planners design a more inclusive, efficient, and livable city.⁵⁷ But, of course, it also traps citizens who cannot escape the digital collection all around them.⁵⁸ After all, it is almost impossible to opt out of basic services like electrical services or trash collection.

52. Summers, *supra* note 50.

53. van Zoonen, *supra* note 22, at 472.

54. Finch & Tene, *supra* note 40, at 1589–90 (quoting Susan Crawford, *Chicago Is Your Big (Friendly) Brother*, BLOOMBERG (June 19, 2014, 2:48 PM), <https://www.bloomberg.com/opinion/articles/2014-06-19/chicago-is-your-big-friendly-brother> [<https://perma.cc/2KYY-ZVJ7>]).

55. See London, CITYDASHBOARD, <http://citydashboard.org/london> [<https://perma.cc/L9QQ-Y6Y2>].

56. See Rob Kitchin, *The Real-Time City? Big Data and Smart Urbanism*, 79 GEOJOURNAL 1, 5–6 (2014) (“For example, the Centro De Operacoes Prefeitura Do Rio in Rio de Janeiro, Brazil, a partnership between the city government and IBM, have created a citywide instrumented system that draws together data streams from thirty agencies, including traffic and public transport, municipal and utility services, emergency services, weather feeds, and information sent in by employees and the public via phone, internet and radio, into a single data analytics centre.” (citations omitted)).

57. See Mohanty et al., *supra* note 24, at 63 (“[I]n the context of smart cities, anything physical, electrical, and digital that is the backbone of the smart city can be considered as its infrastructure. There are many examples, including a rapid transit system, waste management system, road network, railway network, communication system, traffic light system, street light system, office space, water supply system, gas supply system, power supply system, firefighting system, hospital system, bridges, apartment homes, hotels, digital library, law enforcement, and economy system.”).

58. See Finch & Tene, *supra* note 40, at 1596 (“Cities will have only one smart grid, one subway system, and one set of emergency services available to the public. Public services have captive populations who cannot opt out of information collection without paying a steep price in safety, convenience, and quality of life.”).

3. Public Safety

Smart cities are surveillance cities with powerful capabilities to track, predict, and record potential criminal actions or civil disorder.⁵⁹ Many urban cities already have adopted powerful visual surveillance technologies involving digital camera systems. The Domain Awareness System in lower Manhattan links more than 9,000 cameras to a centralized command center where police can observe the streets in real time.⁶⁰ The cameras record the public space and store the data for a month.⁶¹ The existing system includes automated alerts for suspicious behaviors (e.g., abandoning a bag) and the capacity to search for a particular object in the footage (e.g., a sports logo or particular colored shirt).⁶² The Chicago Police Department invested in a network of over 30,000 digital cameras, all recording high-risk neighborhoods.⁶³ Hartford, Connecticut installed a series of artificially intelligent digital cameras that allow police to run object recognition software to identify cars, license plates, and suspicious activities.⁶⁴ Detroit, Michigan also has a similar camera system

59. Whittington, *supra* note 9, at 927; Kitcin, *supra* note 56, at 11 (“It is now possible to track and trace individuals and their actions, interactions and transactions in minute detail across a number of domains (work, travel, consumption, etc.). This level of monitoring has been driven by a growing ‘culture of control’ that desires ‘security, orderliness, risk management and the taming of chance.’”). For an international perspective, see Simon Denyer, *China’s Watchful Eye: Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, WASH. POST (Jan. 7, 2018), <https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance> [<https://perma.cc/TWL6-YRQ6>]; *Chinese Man Caught by Facial Recognition at Pop Concert*, BBC NEWS (Apr. 13, 2018), <https://www.bbc.com/news/world-asia-china-43751276> [<https://perma.cc/46JF-B5SH>]; Paul Mozur, *Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> [<https://perma.cc/ABqJ-8DT4>] (“China has an estimated 200 million surveillance cameras . . .”); and Lily Hay Newman, *Facial Recognition Tech Is Creepy When It Works—and Creepier When It Doesn’t*, WIRED (May 9, 2018, 2:51 PM), <https://www.wired.com/story/facial-recognition-tech-creepy-works-or-not> [<https://perma.cc/6VBN-J2CZ>].

60. See Thomas H. Davenport, *How Big Data Is Helping the NYPD Solve Crimes Faster*, FORTUNE (July 17, 2016, 9:00 AM), <http://fortune.com/2016/07/17/big-data-nypd-situational-awareness> [<https://perma.cc/TgPW-W2KN>].

61. See TalkPolitiX, *New York City—Domain Awareness*, YOUTUBE (June 7, 2013), <https://www.youtube.com/watch?v=ozUHOHAAhzg> [<https://perma.cc/63YH-NX7J>] (posting an excerpt from NOVA, *Manhunt—Boston Bombers*, PUB. BROAD. SERV. (May 29, 2013)).

62. *Id.*

63. See Timothy Williams, *Can 30,000 Cameras Help Solve Chicago’s Crime Problem?*, N.Y. TIMES (May 26, 2018), <https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html> [<https://perma.cc/8GSA-2VWS>].

64. See Eoin Higgins, *Pre-Crime Policing Is Closer than You Think, and It’s Freaking People Out*, VICE (June 12, 2018, 2:47 PM), https://www.vice.com/en_us/article/7xmmvy/why-does-hartford-have-so-many-cameras-precime [<https://perma.cc/9AHC-F35Z>]; Milestone Systems, *Hartford Crime Center Expands Surveillance*, YOUTUBE (Dec. 12, 2017), <https://www.youtube.com/watch?v=OIGxTITe6dE> [<https://perma.cc/7F8W-T6DW>].

with facial recognition capabilities.⁶⁵ Some cities have even piloted smart cameras with automated alert systems that instantaneously deploy a police response based on algorithmic suspicion of criminal activity.⁶⁶

In addition to fixed surveillance video, cities have begun incorporating police-worn body camera footage and patrol car footage, and are considering drones with video and video analytics capabilities.⁶⁷ As digital cameras become cheaper and as machine learning technologies are embedded in video feeds, the ability to track, identify, and monitor the streets will become all-encompassing.⁶⁸

American police forces have partnered with private companies to offer facial recognition technology on a pilot basis.⁶⁹ More tellingly, the companies themselves have begun investing heavily in developing facial recognition and

65. Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues over Racial Bias*, N.Y. TIMES (July 8, 2019), <https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html> [<https://perma.cc/Q2UG-Y72F>] (“Facial recognition, the Detroit police stress, has indeed helped lead to arrests. In late May, for instance, officers ran a video image through facial recognition after survivors of a shooting directed police officers to a gas station equipped with Green Light cameras where they had met with a man now charged with three counts of first-degree murder and two counts of assault. The lead generated by the software matched the description provided by the witnesses.”); *see also* Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 3:19 AM), <https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251> [<https://perma.cc/APK9-NFNA>] (discussing the role of facial recognition software in law enforcement).

66. Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 876–79 (2016); AOL, *Digisensory Technologies Avista Smart Sensors*, YOUTUBE (Sept. 14, 2012), <https://www.youtube.com/watch?v=JamGobiS5wg> [<https://perma.cc/X75C-UE2L>]; *NJ City Leading Way in Crime-Fighting Tech*, CBS NEWS (June 19, 2010, 9:30 AM), <https://www.cbsnews.com/news/nj-city-leading-way-in-crime-fighting-tech> [<https://perma.cc/M4FG-JEW9>].

67. Fussell, *supra* note 16; Chaim Gartenberg, *DJI Is Partnering with Axon to Sell Video-Capable Drones Directly to Cops*, VERGE (June 5, 2018, 2:13 PM), <https://www.theverge.com/2018/6/5/17429908/dji-axon-air-taser-drones-police-officers-program-sale> [<https://perma.cc/TE58-HR5C>].

68. *See* Finch & Tene, *supra* note 40, at 1601 (“Face and object detectors are already widely deployed throughout urban landscapes, both as safety measures (the police in lower Manhattan can track cars and people moving south of Canal Street and even detect unattended packages) and as energy conservation tools (motion sensors on smart streetlights can save an additional twenty to thirty percent on energy by dimming lights during hours of low activity, as well as tracking noise and pollution levels).” (footnote omitted)).

69. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), <https://www.flawedfacedata.com> [<https://perma.cc/S98H-PEES>]; Drew Harwell, *Oregon Became a Testing Ground for Amazon's Facial-Recognition Policing. But What if Rekognition Gets It Wrong?*, WASH. POST (Apr. 30, 2019, 5:19 PM), https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/?noredirect=on&utm_term=.10b8818b5bea [<https://perma.cc/6R6A-8SGU>].

object recognition capabilities.⁷⁰ Companies are selling AI facial recognition technology to schools in an effort to promote safety and to airports for transportation security.⁷¹ Once improved beyond existing technical limitations, cameras will be able to identify people, cars, objects, things, and kinetic movements.⁷² The ubiquity of Automated License Plate Readers (“ALPRs”), which collect millions of recorded license plate images every day, demonstrates the scale at which this type of digital recognition surveillance can grow.⁷³

Video surveillance is but one of the capabilities that can be built into the monitoring capacities of a smart city.⁷⁴ Most obviously, in a wired city marked by digital connecting points, police will be able to track the digital trails of the people using city services or merely just passing by. As Jesse Woo writes, “[i]f smart city sensors are deployed in public areas (which is kind of the point), they potentially introduce government surveillance technology into the public square at an unprecedented level.”⁷⁵

Sensor evidence from the Internet of Things has already started to find its way into criminal cases.⁷⁶ Cell-site locational data, internet browser searches, and smartphone data offer circumstantial evidence of guilt.⁷⁷ Smart

70. See Sidney Fussell, *The New Tech that Could Turn Police Body Cams into Nightmare Surveillance Tools*, GIZMODO (Mar. 9, 2017, 10:09 AM), <https://gizmodo.com/new-ai-could-turn-police-body-cams-into-nightmare-surveillance-1792224538> [<https://perma.cc/8LSD-QH9A>].

71. Drew Harwell, *Unproven Facial-Recognition Companies Target Schools, Promising an End to Shootings*, WASH. POST (June 7, 2018, 7:26 PM), https://www.washingtonpost.com/business/economy/unproven-facial-recognition-companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637_story.html [<https://perma.cc/9MTU-A9U6>]; Lori Aratani, *Your Face is Your Boarding Pass at This Airport*, WASH. POST (Dec. 4, 2018, 1:25 PM), <https://www.washingtonpost.com/nation/2018/12/04/your-face-is-your-boarding-pass-this-airport/> [<https://perma.cc/KR4R-K6PS>] (“An increasing number of airports are using biometrics to process passengers as they move through the system. Dulles International Airport recently unveiled a system that uses iPads to scan passengers’ faces before they board flights. U.S. Customs and Border Protection has been using biometrics to track passengers entering the U.S.”).

72. JAY STANLEY, ACLU, *THE DAWN OF ROBOT SURVEILLANCE: AI, VIDEO ANALYTICS, AND PRIVACY* 17–21 (2019), https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf [<https://perma.cc/G2WG-DEFL>].

73. See Randy L. Dryer & S. Shane Stroud, *Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother’s Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action*, 55 JURIMETRICS 225, 234–35 (2015).

74. JOHN S. HOLLYWOOD, MICHAEL J.D. VERMEER, DULANI WOODS, SEAN E. GOODISON & BRIAN A. JACKSON, *USING VIDEO ANALYTICS AND SENSOR FUSION IN LAW ENFORCEMENT* 4 (RAND Corp. 2018); STANLEY, *supra* note 72, at 37–38.

75. Woo, *supra* note 32, at 956.

76. Jouvenal, *supra* note 11 (detailing biometric evidence used in criminal investigations).

77. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html> [<https://perma.cc/4SR7-K93S>]; Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> [<https://perma.cc/4WAK-HYJD>] (noting

cars literally report individuals suspected of crimes.⁷⁸ Algorithmic financial systems report potential fraud.⁷⁹ Finally, digital tools like Stingray (International Mobile Subscriber Identity catchers) can find a particular cell phone signal in a particular location and, if configured correctly, even intercept some of the content in the transmission.⁸⁰ As cities, homes, cars, and people become more connected, the Internet of Things eventually will become the “Internet of Evidence.”⁸¹

Other criminal patterns will emerge from mass surveillance technologies embedded in smart city sensors. Sometimes the evidence will be generalized, like the ability of wastewater systems to identify an increase in illegal narcotics from the sewage system.⁸² Other times it will be more individualized, like the ability of smart electrical meters to identify suspiciously high home electricity usage (consistent with growing marijuana).⁸³ And other times it will be accidental, like the consequences of installing smart streetlights with audio

that many apps collect users’ location data); Deanna Paul, *Google Refused an Order to Release Huge Amounts of Data. Will Other Companies Bow Under Pressure?*, WASH. POST (Aug. 18, 2018, 9:23 AM), <https://www.washingtonpost.com/technology/2018/08/18/google-refused-an-order-release-huge-amounts-data-will-other-companies-bow-under-pressure> [https://perma.cc/C8A9-H36N] (describing how Google searches are being used in criminal prosecutions to reveal location and other incriminating clues).

78. See Alex Hern, *Florida Woman Arrested for Hit-and-Run After Her Car Calls Police*, GUARDIAN (Dec. 7, 2015, 10:33 AM), <http://www.theguardian.com/technology/2015/dec/07/florida-woman-arrested-hit-and-run-car-calls-police> [https://perma.cc/MH8U-LF7Z].

79. See Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1164 (2017) (“[A]cademic researchers have demonstrated how machine-learning algorithms can be used to predict cases of financial statement fraud . . .” (citing Johan Perols, *Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms*, 30 AUDITING 19 (2011))).

80. Bert-Jaap Koops, Bryce Clayton Newell & Ivan Škorvánek, *Location Tracking by Police: The Regulation of ‘Tireless and Absolute Surveillance,’* 9 U.C. IRVINE L. REV. 635, 669–70 (2019); Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 146 (2013); see also Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015), <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html> (discussing the use of nondisclosure agreements between the FBI and police departments regarding stingray operations); Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 24, 2015, 7:51 AM), <https://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181> [https://perma.cc/8EV3-MH8W] (“In one case after another, . . . police in Baltimore and other cities used the phone tracker, commonly known as a stingray, to locate the perpetrators of routine street crimes and frequently concealed that fact from the suspects, their lawyers and even judges. In the process, they quietly transformed a form of surveillance billed as a tool to hunt terrorists and kidnappers into a staple of everyday policing.”).

81. Also the title of a future law review article I really should write.

82. Christopher L. Hering, Note, *Flushing the Fourth Amendment Down the Toilet: How Community Urinalysis Threatens Individual Privacy*, 51 ARIZ. L. REV. 741, 741–44 (2009).

83. *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 526 (7th Cir. 2018).

sensor capabilities that will be able to record gunshots and (inadvertently) record human conversations.⁸⁴

Beyond people and patterns, police can also target particular areas to find all the people who might frequent a known drug house, intersection, or gang territory.⁸⁵ Cell data, wireless data, Bluetooth, and even Radio-Frequency Identification (“RFID”) sensors might all be designed to reveal locational data which could be useful in police investigations trying to identify suspects at a particular location or involved in a suspicious pattern of activity.⁸⁶

4. City-Wide Application Programming Interface

The digital layer of a truly smart city could have a very public face: the Application Programming Interface (“API”).⁸⁷ A shared API could allow government services and third-party providers to share a software platform which can communicate with the end user. As an early version of a smart city prototype advertised, the goal is to design a “neighborhood built from the internet up.”⁸⁸

84. Sarah Holder, *The Shadowy Side of LED Streetlights*, BLOOMBERG CITYLAB (Mar. 8, 2018, 9:44 AM), <https://www.citylab.com/equity/2018/03/their-lights-were-watching-odd/554696> [<https://perma.cc/4S4Z-BJ2Z>] (“San Diego’s deputy chief operating officer told IEEE Spectrum that the city’s new sensor-enabled lights could eventually be hooked up to the city’s ShotSpotter network, helping to identify the source of gunfire and ‘automatically alert police to dangerous situations’ by picking up audio from the ground. The sounds of violence are defined as breaking glass and shots fired, but it’s not hard to imagine that raised voices could be linked to real people, and draw similar scrutiny.”).

85. Jake Laperruque, *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance*, 51 U. RICH. L. REV. 705, 717 (2017) (“[T]he tracking technology, BriefCam, allows law enforcement to overlay hours of video and then isolate individuals based on certain factors so monitors can view all applicable targets with hours of time reduced to minutes. This can be used to isolate all individuals or cars that are a particular color, or traveling on a specific route. With such technologies, police could ‘reverse-engineer’ location tracking, picking a route they want to monitor, then use BriefCam to immediately isolate and identify everyone who used it over the course of several hours.” (footnotes omitted)).

86. See Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 812 (2016) (describing the rise of Internet of Things technology as surveillance); *I Know What You’ll Do Next Summer: More Data and Surveillance Are Transforming Justice*, ECONOMIST: TECH. Q. (June 2, 2018), <https://www.economist.com/technology-quarterly/2018-05-02/justice> [<https://perma.cc/7XMV-RRM8>]; Valentino-DeVries et al., *supra* note 77.

87. An Application Programming Interface is essentially an operating system that allows developers to program on a shared digital platform. See Petr Gazarov, *What Is an API? In English, Please.*, FREECODECAMP (Dec. 19, 2019), <https://medium.freecodecamp.org/what-is-an-api-in-english-please-b880a3214a82> [<https://perma.cc/9CKF-EKJM>].

88. Laura Bliss, *How Smart Should a City Be? Toronto Is Finding Out*, BLOOMBERG CITYLAB (Sept. 7, 2018, 9:19 AM), <https://www.citylab.com/design/2018/09/how-smart-should-a-city-be-toronto-is-finding-out/569116> [<https://perma.cc/ML44-ZN9S>].

To build a city “from the internet up,” one must design a city that includes a digital layer.⁸⁹ So, in addition to a physically visible public street level and a hidden underground layer for utilities, a truly “smart” city would integrate a city-wide digital layer.⁹⁰

The digital layer will include a set of APIs, creating a stable and well-designed canvas on which developers can build applications to reimagine and reinvent how the city works. In much the same way that software platforms like Apple’s App Store, the Google Play Store, and Amazon Web Services have stimulated creativity on the web and in personal devices, the digital layer provides a set of APIs, with documentation and developer support that will inspire the same creativity in the city. APIs include regulated access to city data and the ability to interact with the city infrastructure in ways that are safe and consistent with other uses.⁹¹

The idea is that the city could become a digital smart platform akin to a smartphone platform with government services and third-party services available through shared applications.⁹² The city would make its platform available to developers to invent additional consumer conveniences for residents.⁹³ If the city becomes the platform, then the API is the key to the city.

The goal of this digital layer is three-fold. First, it would allow flexibility to ensure the city can update its technology and capacity.⁹⁴ Since technology must upgrade to avoid becoming obsolete, so must a smart city. In addition, the sensor data collected allows city administrators to create predictive models based on real city data, so that municipal officials can build a digital replica

89. Nancy Scola, *Google Is Building a City of the Future in Toronto. Would Anyone Want to Live There?*, POLITICO MAG. (July/Aug. 2018), <https://www.politico.com/magazine/story/2018/06/29/google-city-technology-toronto-canada-218841> [<https://perma.cc/TYB2-3K3W>].

90. Summers, *supra* note 50 (“At the highest level is the digital layer, which combines a network of sensors, a detailed map of the neighborhood, simulation software and a platform where citizens can log in and manage their public and private data.”).

91. SIDEWALK LABS, RFP NO. 2017-13 app. 70 (Oct. 2017), <https://www.passivehousecanada.com/wp-content/uploads/2017/12/TO-Sidewalk-Labs-Vision-Sections-of-RFP-Submission-sm.pdf> [<https://perma.cc/DBW5-UDCE>]. In 2020, Sidewalk Labs announced it would not be pursuing Waterfront Toronto as a smart city project. Andrew J. Hawkins, *Alphabet’s Sidewalk Labs Shuts Down Toronto Smart City Project*, VERGE (May 7, 2020, 11:56 AM), <https://www.theverge.com/2020/5/7/21250594/alphabet-sidewalk-labs-toronto-quayside-shutting-down> [<https://perma.cc/L2V6-77RD>].

92. Elizabeth Woyke, *A Smarter Smart City*, MIT TECH. REV. (Feb. 21, 2018), <https://www.technologyreview.com/s/610249/a-smarter-smart-city> [<https://perma.cc/A8QS-XP8R>].

93. *Id.* (“Details are still under discussion, but Sidewalk plans to let third parties access the data and technologies, just as developers can use Google’s and Apple’s software tools to craft apps. In fact, Sidewalk anticipates that 80 percent of the work on Quayside will involve these third parties.”).

94. SIDEWALK LABS, *supra* note 91, at 66.

of city services and game out possible future scenarios.⁹⁵ So, for example, instead of guessing how traffic patterns might change from a closed highway, city engineers can create a digital replica model of existing city usage to predict the impact.

Second, the digital layer allows the cost of municipal services to be quantified.⁹⁶ This involves understanding where people go, what they do, how they do it, and how they use government services, benefits, and infrastructure.⁹⁷ Everything from energy usage to pedestrian patterns can be measured and evaluated using sensors.⁹⁸ Public Wi-Fi spots can identify individuals from the phones in their pockets, and sophisticated cameras and overlapping sensors can monitor daily use of the public sphere.⁹⁹

Third, a digital layer allows for a host of innovations over existing urban design. For example, smart streets capable of directing traffic flow with embedded, ever-changing LED lights,¹⁰⁰ smart “[t]raffic signals . . . auto-calibrat[ing] to ease . . . congestion,”¹⁰¹ road tolls and parking that could be paid automatically,¹⁰² and smart sidewalks which could “sense movement, gather data, and send information back to a centralized map of the neighborhood.”¹⁰³

The tracking power of this shared digital interface could be quite powerful for surveillance purposes, especially if payments, government benefits, and financial transactions are mediated through this third-party records system.¹⁰⁴ Like Apple Pay, Lyft, or Uber, which do not work without a

95. *Id.* at 66–67 (“A Model component—in development by Sidewalk’s Model Lab—can simulate ‘what if’ scenarios for city operations and inform long-term planning decisions. A Map component collects location-based information about the infrastructure, buildings, and shared resources in the public realm.”).

96. *See Bliss, supra* note 88.

97. *See* SIDEWALK LABS, *supra* note 91, at 66–67 (“An Account component provides a highly secure, personalized portal through which each resident accesses public services and the public sector.”).

98. *See* Brian Barth, *The Fight Against Google’s Smart City*, WASH. POST (Aug. 8, 2018, 11:02 AM), <https://www.washingtonpost.com/news/theworldpost/wp/2018/08/08/sidewalk-labs> [<https://perma.cc/SW8G-8BP7>].

99. SIDEWALK LABS, *supra* note 91, at 70 (“The size of Quayside makes it feasible to deploy cameras with different capabilities covering the same spaces. This will help Sidewalk evaluate trade-offs in technology and cost with apples-to-apples detection tasks on the same region. Likewise, Quayside will have multiple overlapping communications networks—an opportunity to evaluate relative value.”).

100. *See Bliss, supra* note 88 (“Tiles capable of melting snow, absorbing stormwater, and directing traffic with LED lights would form the pavement underfoot.”).

101. Scola, *supra* note 89.

102. *See* Summers, *supra* note 50 (“The company is developing a platform with APIs that relate to road tolls, curbs and parking.”).

103. Bliss, *supra* note 88.

104. *See* Tomas Likar, *Your City Can’t Become ‘Smart’ Without Proper Payment Infrastructure*, SMARTCITIESDIVE (Aug. 29, 2018), <https://www.smartcitiesdive.com/news/your-city-cant->

smart device, the need for a trackable smart device may grow increasingly necessary. Many government benefits (e.g., disability benefits, food stamps) also may soon mandate some digital app and many private companies may target third-party development through a shared API.¹⁰⁵ These third-party entities are in the data business and citizens are the product.¹⁰⁶ The chosen smart device and its revealing third-party records will become necessary parts of life in a smart city.

B. SMART SENSOR PRIVACY

As might be evident, the scope and scale of sensors embedded in smart infrastructure can vary greatly. Simply by design choice, data can be shared or siloed. Engineers can also design smart sensor systems to avoid the direct collection of personal information.¹⁰⁷ Knowing how much electricity travels to homes in an affluent neighborhood may be useful without knowing which particular mansion wastes the most energy. Knowing how many cars pass by a smart street sign provides valuable traffic management information without knowing who owns each car.¹⁰⁸ Building smart transportation grids does not necessarily require revealing personally-identifiable information, because one can blind sensors to personally-identifiable information.

But technologies designed to anonymize data run into two basic problems. First, with enough information, individuals can de-anonymize the data, revealing the very information sought to be kept private.¹⁰⁹ In several studies, researchers have shown that reidentification is quite easy. Though the “smart road sensor” might only collect the number of vehicles travelling on it, the growth of surveillance tracking devices like the city’s license plate readers,

become-smart-without-proper-payment-infrastructure/531215 [https://perma.cc/VL6S-2BHH]; Woyke, *supra* note 92.

105. Barth, *supra* note 98. Much of the debate over Quayside has been about whether citizen data can or should be sold to third parties. See SIDEWALK LABS, DIGITAL GOVERNANCE PROPOSALS FOR DSAP CONSULTATION 12 (2018), https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES [https://perma.cc/EgCg-CS9S]; Sean McDonald, *Toronto, Civic Data, and Trust*, MEDIUM (Oct. 17, 2018), <https://medium.com/@McDapper/toronto-civic-data-and-trust-ee7ab928fb68> [https://perma.cc/BJ66-4ZG8]; Bianca Wylie & Sean McDonald, *What Is a Data Trust?*, CTR. FOR INT’L GOVERNANCE INNOVATION (Oct. 9, 2018), <https://www.cigionline.org/articles/what-data-trust> [https://perma.cc/FS5G-YKJR].

106. Ferguson, *supra* note 10.

107. Summers, *supra* note 50 (“We don’t need an image of you. . . . What we need is your outline, because then the computer can tell, ‘Oh, that’s a human. That’s a person walking.’ If all I do is outline your body and there’s no face, no color, no nothing, then there’s no way I can identify you. I’ve eliminated the privacy issue, but I’ve accomplished the goal.” (quoting Sidewalk Lab’s Head of Urban Systems, Rohit Aggarwala)).

108. See Finch & Tene, *supra* note 40, at 1612 (“While de-identification can no longer be treated as a ‘silver bullet,’ de-identified data sets still provide significant social utility with lowered privacy risks.”).

109. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716 (2010).

cameras, smart tolls, Wi-Fi sniffers, cell-signal technologies, etc., might undercut anonymity in practice.¹¹⁰ For example, considering the smart data from our homes, cars, and persons, all of these data points can be aggregated so that inferences can be drawn.¹¹¹ As privacy experts Kelsey Finch and Omer Tene write, “[s]mart city technologies thrive on constant, omnipresent data flows captured by cameras and sensors placed throughout the urban landscape. These devices pick up all sorts of behaviors, which can now be cheaply aggregated, stored, and analyzed to draw personal conclusions about city dwellers.”¹¹² And, though it has not been tried in a smart city setting, data experts have been able to re-identify de-identified datasets in other contexts.¹¹³ This aggregation problem will only grow with more connected city sensors allowing more individualized inferences to be drawn.

The second problem is largely one of consumer convenience. If smart devices and ubiquitous sensors can make some of the hassles of life easier, citizens will sync their lives to maximize these efficiencies. If you can buy coffee with your smartphone, pay tolls without quarters, access your building’s security without a key, or get your trash picked up seamlessly, why would you

110. Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL’Y FOR INFO. SOC’Y 425, 511 (2011) (“As data aggregation continues, as linkages among different data sets more [sic] extensive and as data mining analytics become more effective, predictive inferences about people will become more accurate. People will be less able to protect the secrecy of their information through concealment. Indirect inferences based on data analytics will reveal these facts with an acceptable level of certainty that people do not wish to reveal.”).

111. Hiller & Blanke, *supra* note 9, at 316 (“[T]he concepts of ‘data fusion’ or ‘sensor fusion’ refer to the phenomenon of data collected from a variety of different sources being combined to create more information and more powerful inferences than can be produced by the separate sources. This phenomenon will become even more important with the proliferation of the many varieties of sensors that will be connected in the smart cities.” (footnote omitted)).

112. Finch & Tene, *supra* note 40, at 1582.

113. Woo, *supra* note 32, at 961 (“True de-identification is quite difficult to accomplish because the prevalence of big data often allows determined actors to reverse the de-identification process and compromise a data subject’s privacy.”); see also Charlotte Jee, *You’re Very Easy to Track Down, Even when Your Data Has Been Anonymized*, MIT TECH. REV. (July 23, 2019), <https://www.technologyreview.com/2019/07/23/134090/youre-very-easy-to-track-down-even-when-your-data-has-been-anonymized> [<https://perma.cc/C7X8-TU98>] (“A paper back in 2007 showed that just a few movie ratings on Netflix can identify a person as easily as a Social Security number, for example.”); Kelsey Campbell-Dollaghan, *Sorry, Your Data Can Still Be Identified Even if It’s Anonymized*, FAST CO. (Dec. 10, 2018), <https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized> [<https://perma.cc/P85J-GGL4>] (describing a study by MIT Senseable City Lab in which researchers were able to match “two anonymized datasets . . . , one of mobile phone logs and the other of transit trips,” with 17 percent accuracy after one week and 95 percent accuracy after 11 weeks); Corin Faife, *The Safe Way to Build a Smart City*, BLOOMBERG CITYLAB (Oct. 2, 2017, 4:34 PM), <https://www.bloomberg.com/news/articles/2017-10-02/the-smart-safe-way-to-build-a-smart-city> [<https://perma.cc/P7NW-Y8VS>] (“In a widely cited study from 2000, Harvard professor Latanya Sweeney (then at Carnegie Mellon) found that 87 percent of Americans could be uniquely identified in a dataset by only gender, date of birth, and ZIP code. That can then be cross-referenced with voter records to identify each individual by name.”).

not take advantage of the convenience? The only real cost is your personal data, which you trade for better services.¹¹⁴ Smart sensors will thus likely evolve around an ever-increasing focus on consumer convenience connected by personally revealing information and Internet of Things devices.¹¹⁵ Landlords are already proposing facial recognition in apartments to keep out unwanted guests.¹¹⁶ Stores and services in a smart city may not be far behind in offering sales or discounts to customers they recognize through their smart devices (or biometrics).¹¹⁷ Once the city becomes the platform for digital existence, one can imagine hundreds of consumer-focused apps being developed. But, of course, all of this will only increase the government's ability to aggregate data and draw inferences about individuals.¹¹⁸

In addition to choices of anonymization, there is the choice of localization. Each of the technologies discussed can exist in a non-networked world. Each sensor could be engineered to retain data locally, eschewing centralized collection and analysis. This choice values privacy over some of the efficiencies and insights that could arise from mass data collection. But again, the temptation of efficiency and aggregated insight will be difficult to resist. The data is valuable, the convenience real, and the innovations helpful.

As will be discussed in the next several Parts, the design choices around smart sensors have constitutional consequences because of the way the Supreme Court has recently interpreted the Fourth Amendment in the context of digital surveillance technologies. These Parts proceed in three steps, first tracking the two dominant Fourth Amendment threshold search tests under current doctrine and then responding to some obvious objections. Part III will examine how smart sensors impact a reasonable expectation of privacy in public. Part IV will examine how the Supreme Court's recent

114. See Hiller & Blanke, *supra* note 9, at 323 ("Cities will often have no alternative but to collect personal or identifiable information if they are going to become 'smarter.'"); Carmichael, *supra* note 18; Walls, *supra* note 18, at 1924–25.

115. Mohanty et al., *supra* note 24, at 69 ("The use of the IoT can make smart cities feasible. Smartphones, smart meters, smart sensors, and RFID, in essence, form the IoT framework in smart cities.").

116. Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. TIMES (Mar. 28, 2019), <https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html> [<https://perma.cc/7KJN-2AHY>]; Alfred Ng, *Tenants Call for Better Laws After Stopping Facial Recognition from Moving In*, CNET (Nov. 22, 2019, 11:58 AM), <https://www.cnet.com/news/tenants-call-for-better-laws-after-stopping-facial-recognition-from-moving-in> [<https://perma.cc/RC96-KFBY>].

117. Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, N.Y.: INTELLIGENCER (Oct. 20, 2018), <http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html> [<https://perma.cc/3UKH-BF82>].

118. Mike Weston, *'Smart Cities' Will Know Everything About You*, WALL ST. J. (July 12, 2015, 6:36 PM), <http://www.wsj.com/articles/smart-cities-will-know-everything-about-you-1436740596> [<https://perma.cc/B2KV-RB84>] ("In a fully 'smart' city, every movement an individual makes can be tracked. The data will reveal where she works, how she commutes, her shopping habits, places she visits and her proximity to other people.").

“trespass test” would be applied to smart infrastructure. Finally, Part V looks at whether any of the traditional Fourth Amendment exceptions apply.

III. THE FOURTH AMENDMENT & SMART SENSORS IN PUBLIC

This Part seeks to untangle the doctrinal confusion that has emerged from the Supreme Court’s early forays into digital surveillance technologies and apply these insights to the equally unsettled world of structural sensor surveillance.

The Fourth Amendment protects against “unreasonable searches and seizures.”¹¹⁹ Yet, despite its centrality to criminal procedure, the definition of a “search” is still a contested issue. Over the years, different search tests have emerged with oddly drawn doctrinal lines. Terms of art like a “reasonable expectation of privacy,”¹²⁰ “trespass,”¹²¹ “protected interest[s],”¹²² and “reasonableness”¹²³ have created a constitutional muddle.¹²⁴ The introduction of powerful digital surveillance technologies has only added to the complications. Perhaps not surprisingly, an Amendment ratified in 1791 has failed to adapt to the twenty-first century.

Structural surveillance adds to this complexity because the type of sensors at issue may well determine the Fourth Amendment’s impact on individual privacy. This Part examines smart city sensors in public through the lens of Fourth Amendment law, exploring how background principles, emerging doctrinal themes, and precedent all suggest that some smart city innovations might run afoul of the Fourth Amendment search doctrine.

A. A DIGITAL REASONABLE EXPECTATION OF PRIVACY TEST IN PUBLIC

Like any city, a smart city requires public spaces for public activity. The difference, however, is that public activity can be more easily tracked and aggregated in a digitally monitored world. The open legal question is whether by designing smart sensors to ubiquitously track and collect personal data over

119. U.S. CONST. amend. IV.

120. *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

121. *United States v. Jones*, 565 U.S. 400, 405 (2012).

122. Jack Wade Nowlin, *The Warren Court’s House Built on Sand: From Security in Persons, Houses, Papers, and Effects to Mere Reasonableness in Fourth Amendment Doctrine*, 81 MISS. L.J. 1017, 1031–32 (2012) (“This traditional [protected interest] approach emphasized the interests specifically enumerated as protected in the text of the Fourth Amendment, ‘persons, houses, papers, and effects,’ and the common-law principles rooted in property law that formed the important broader legal context of the text.”).

123. *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (“[T]he ultimate touchstone of the Fourth Amendment is ‘reasonableness.’” (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006))).

124. See Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1293–95 (2014).

the long term, a smart city continually triggers Fourth Amendment concerns about aggregated, long-term tracking without a probable cause warrant.¹²⁵

To understand the problem, some background on the evolution of the Fourth Amendment is necessary. Since 1967, the Fourth Amendment threshold “search” inquiry has turned on whether the individual has a subjective expectation of privacy that society would consider objectively reasonable.¹²⁶ If such a reasonable expectation of privacy is violated, the Court finds that a Fourth Amendment search occurred.¹²⁷ If such a search occurs without a probable cause warrant or an applicable exception to the warrant requirement, the search may violate the Fourth Amendment. The doctrine has been called confused, and many scholars and a few Justices have criticized its use.¹²⁸ Nevertheless, it remains the controlling law for both the physical and digital worlds.¹²⁹

Structural surveillance involves two types of potential public exposure. First, there is the traditional physical exposure of people and things. Police in smart cities, like in normal cities, can observe what police can observe using traditional human means and are governed by existing Fourth Amendment rules.¹³⁰ The second type of exposure is digital—involving direct collection of tracking information of people living in those cities. The reality is that with enough digital clues—be they municipal, consumer, financial, cellular, or

125. The question remains open because both *Jones* and *Carpenter* only addressed longer-term surveillance: 28 days in *Jones* and at least seven days in *Carpenter*. *Jones*, 565 U.S. at 403; *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018).

126. *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

127. This is the traditional understanding subject to a few limited exceptions. See *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (“Consistent with our precedent, our analysis begins, as it should in every case addressing the reasonableness of a warrantless search, with the basic rule that ‘searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.’” (quoting *Katz*, 389 U.S. at 357)).

128. *Carpenter*, 138 S. Ct. at 2244 (Thomas, J., dissenting) (“[T]he *Katz* test also has proved unworkable in practice. Jurists and commentators tasked with deciphering our jurisprudence have described the *Katz* regime as ‘an unpredictable jumble,’ ‘a mass of contradictions and obscurities,’ ‘all over the map,’ ‘riddled with inconsistency and incoherence,’ ‘a series of inconsistent and bizarre results that [the Court] has left entirely undefended,’ ‘unstable,’ ‘chameleon-like,’ “‘notoriously unhelpful,’” ‘a conclusion rather than a starting point for analysis,’ ‘distressingly unmanageable,’ ‘a dismal failure,’ ‘flawed to the core,’ ‘unadorned fiat,’ and ‘inspired by the kind of logic that produced Rube Goldberg’s bizarre contraptions.’” (footnote omitted)); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (“The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable.”).

129. *Carpenter*, 138 S. Ct. at 2217 (“A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, ‘what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.’” (quoting *Katz*, 389 U.S. at 351–52)).

130. See *id.*; see also *California v. Greenwood*, 486 U.S. 35, 41 (1988) (“[T]he police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public.”).

biometric—individuals can be tracked through the aggregated nature of the information. If collected (and most data is designed to be collected), the digital trails of life can be studied to identify individual people. After all, you cannot enforce a trash tax if you do not know whose trash it is. This second level of digital exposure is the subject of this Section.

1. Reasonable Expectation of Privacy Principles

To understand how the “reasonable expectation of privacy” test works in a public space, one must piece together a series of Supreme Court decisions. To start, in *United States v. Jones*, five Justices agreed that 28 days of GPS surveillance of Antoine Jones’ car for a narcotics investigation was a Fourth Amendment search that violated his reasonable expectation of privacy.¹³¹ This was so even though the GPS tracking occurred in public (on public streets) and even though the satellite data only revealed the whereabouts of his car.¹³² The concurrences’ understanding of an expectation of privacy was later incorporated by reference in the majority decision in *Carpenter v. United States*.¹³³

Carpenter reaffirmed the Supreme Court’s commitment to digital privacy in an age of ubiquitous tracking. Timothy Carpenter was tracked down for a series of robberies because his cell phone signal revealed his location during the crimes.¹³⁴ Government agents requested seven days of cell-site tracking data from Carpenter’s cell phone company in an attempt to prove their case.¹³⁵ The Supreme Court held that acquiring a week’s worth of cell-site

131. *Carpenter*, 138 S. Ct. at 2220; see *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (“I would ask whether people 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. I do not regard as dispositive the fact that the government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.”); *id.* at 430 (Alito, J., concurring in judgment) (“Under this approach, relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.” (citation omitted)).

132. *Carpenter*, 138 S. Ct. at 2215 (“Since GPS monitoring of a vehicle tracks ‘every movement’ a person makes in that vehicle, the concurring Justices [in *Jones*] concluded that ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy’—regardless whether those movements were disclosed to the public at large.” (first quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment); and then quoting *id.* at 415 (Sotomayor, J., concurring))).

133. *Id.* at 2217 (first citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); and then citing *Jones*, 565 U.S. at 430 (Alito, J., concurring)) (“A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.”).

134. *Id.* at 2211–12.

135. *Id.* at 2212.

location data without a warrant violated the reasonable expectation of privacy.¹³⁶ This was so even though the digital records were collected by a private third party (the cell phone company) and held by that private company in largely unidentifiable form (raw unstructured data).¹³⁷ This was so even though all that was revealed was his location in public.¹³⁸ Like in *Jones*, the Court reasoned that the revealing nature of aggregated locational data required Fourth Amendment protection.

Finally, in *Riley v. California*, the Court recognized that access to stored data files (either on a smart phone or in the connected cloud) required a warrant even incident to a lawful arrest.¹³⁹ Police arrested David Riley and searched his smartphone's photos without a warrant, eventually recovering incriminating photographs.¹⁴⁰ The Court held that the quantity and qualitatively revealing nature of data on smartphone and digital devices was too great a privacy concern to obtain without a probable cause warrant.¹⁴¹ The Court reasoned that the collection of digital clues revealed too much about the privacies of life.

In *Carpenter*, the Justices focused on the personal, potentially sensitive nature of the collected locational data as part of the violation of privacy. In *Jones*, Justice Sonia Sotomayor similarly explained how "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."¹⁴² Justice Samuel Alito also envisioned a privacy-invading, prototype smart city environment filled with surveillance tracking technologies:

Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience.¹⁴³

136. *Id.* at 2220–23.

137. See Orin S. Kerr, *Initial Reactions to Carpenter v. United States* 16–17 (Univ. S. Cal. L. Legal Stud. Paper No. 18-14, 2018) [hereinafter Kerr, *Initial Reactions*].

138. *Carpenter*, 138 S. Ct. at 2200–23.

139. See *Riley v. California*, 134 S. Ct. 2473, 2493–95 (2014).

140. *Id.* at 2480–81.

141. *Id.* at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

142. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

143. *Id.* at 428 (Alito, J., concurring in judgment).

Similarly, the *Carpenter* Court repeatedly emphasized a concern with the revealing nature of private information coming from our digital trails:

A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. . . . [W]hen the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

....

. . . Yet this case is not about "using a phone" or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years.¹⁴⁴

In addition to the personal privacy harms of such tracking, the *Jones* Court recognized the potential chilling of associational and expressive conduct from digital monitoring.

Awareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."¹⁴⁵

This informational privacy harm connects back to the Court's concern in *Riley* about the revealing nature of digital information stored on our digital devices. As the Court recognized, our digital devices likely reveal more about our associations, interests, and beliefs than our homes.¹⁴⁶

Linking *Jones*, *Carpenter*, and *Riley* together, a few principles can be distilled as to when the Supreme Court will find a city-wide system of sensor surveillance to be a search for Fourth Amendment purposes. The purpose of this Section is to develop an analytical framework to show that city-wide systems of sensor surveillance could raise Fourth Amendment problems if

144. *Carpenter v. United States*, 138 S. Ct. 2206, 2218, 2220 (2018) (citations omitted).

145. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

146. *Riley*, 134 S. Ct. at 2491 ("Indeed, 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.").

designed carelessly. The next Section will apply these principles to some of the sensor technologies discussed in Part II.

i. Principle #1: Digital is Different

The first lesson to be learned from these recent cases is that “digital is different” when it comes to the Supreme Court’s analysis.¹⁴⁷ As evidenced in *Jones*, *Riley*, and *Carpenter*, analog precedent will not control the digital equivalent. The smartphone of *Riley* is not the equivalent container as the cigarette pack in *United States v. Robinson*.¹⁴⁸ The cell-site location records in *Carpenter* are not the same as bank records or landline phone records in *United States v. Miller* and *Smith v. Maryland*.¹⁴⁹ The GPS tracking in *Jones* is not the same thing as a team of police officers physically watching the same car in public over time.

If digital is different, then smart sensors capable of tracking digital signatures raise Fourth Amendment issues and will be evaluated with heightened care. In fact, one way to look at *Jones* and *Carpenter* is to see them as early smart sensor surveillance cases. The GPS device in *Jones* was a sensor-like device attached to a car, similar to many of the transportation innovations like digital license plates or toll collection readers.¹⁵⁰ Similarly, the cell-site signal in *Carpenter* is similar to a host of wireless connecting points that will be

147. Henderson, *supra* note 15, at 951 (“So, while *Riley* perhaps left things unanswered that it could have addressed, it made very clear that when it comes to the Fourth Amendment, digital is different.” (footnote omitted)); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 27 (2015); see also Jennifer Stisa Granick, *SCOTUS & Cell Phone Searches: Digital Is Different*, JUST SEC. (June 25, 2014), <https://www.justsecurity.org/12219/scotus-cell-phone-searches-digital> [http://perma.cc/94RH-42EV] (“The most important takeaway from today’s opinion is that Digital Is Different.”).

148. *Riley*, 134 S. Ct. at 2485 (“A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [prior precedents].”); see also *Carpenter*, 138 S. Ct. at 2214 (“[W]e rejected in *Kyllo* a ‘mechanical interpretation’ of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant’s home was a search.” (citation omitted)); *United States v. Robinson*, 414 U.S. 218, 236 (1973) (“Having in the course of a lawful search come upon the crumpled package of cigarettes, [Officer Jenks] was entitled to inspect it . . .”).

149. *Carpenter*, 138 S. Ct. at 2219 (“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.”); see also *United States v. Miller*, 425 U.S. 435, 442 (1976) (“The [bank] checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act . . .”); *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (“The [telephone] switching equipment that processed those [phone] numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy.”).

150. Doubek, *supra* note 29.

created in a city embedded with smart sensors. Like *Jones* and *Carpenter*, structural surveillance is a digital surveillance system that likely will receive a hard look by the Supreme Court.

ii. *Principle #2: The Court Disfavors Arbitrary and “Too Permeating” Surveillance*

The second lesson to be learned is that the Supreme Court is concerned with arbitrary and pervasive police surveillance. The former focuses on the potential to misuse police power to interfere with “the privacies of life,”¹⁵¹ and the latter focuses on the widespread systems created to facilitate that government interference. Smart sensors raise both concerns.

In *Carpenter*, Chief Justice John Roberts stated quite simply: “The ‘basic purpose of [the Fourth] Amendment,’ our cases have recognized, ‘is to safeguard the privacy and security of individuals against *arbitrary* invasions by governmental officials.’”¹⁵² This comment directly echoed Justice Sotomayor’s concurrence in *Jones* where in the context of GPS tracking she stated, “the Fourth Amendment’s goal [is] to curb *arbitrary* exercises of police power.”¹⁵³ In both cases, the check on arbitrariness would have been a probable cause warrant which would have limited police surveillance in an individualized and particularized manner. Without such a requirement, police could use GPS tracking or cell-site collection based on a lesser standard (or no standard), leading to a concern with arbitrary use.

The Supreme Court’s concern with such generalized police power evokes colonial history and the Founders’ fear of general warrants. Again, from *Carpenter*:

Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings “of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.” On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure “the privacies of life” against “*arbitrary* power.”¹⁵⁴

Sensors that literally collect data about all citizens going about their business in a smart city raise arbitrariness concerns. Depending on how they are designed and the limitations in place, the very same concerns articulated in *Carpenter* and *Jones* arise—only amplified across a city-scale.

151. *Riley*, 134 S. Ct. at 2495 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

152. *Carpenter*, 138 S. Ct. at 2213 (emphasis added) (quoting *Camara v. Mun. Ct. of S.F.*, 387 U.S. 523, 528 (1967)).

153. *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (emphasis added).

154. *Carpenter*, 138 S. Ct. at 2213–14 (alteration in original) (emphasis added) (footnote omitted) (citations omitted) (first quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925); and then quoting *Boyd*, 116 U.S. at 630).

Though the concern about arbitrary policing has to do with the overbroad and unparticularized nature of data collection, the Supreme Court was also concerned with setting up systemic surveillance. The language of *Carpenter* explicitly referenced that it was, “a central aim of the Framers . . . ‘to place obstacles in the way of a too permeating police surveillance.’”¹⁵⁵ In her *Jones* concurrence, Justice Sotomayor made a similar reference to “prevent[ing] ‘a too permeating police surveillance.’”¹⁵⁶

City sensors designed to capture, analyze, and use citizen data can, with little effort, become a permeating system of surveillance. In fact, depending on how they are configured, the proliferation of smart sensors might just be the definition of such a system. Worse, video systems with video analytics, object recognition, and face-tracking capabilities almost provide a worst-case version of “too permeating” surveillance.¹⁵⁷ Again, if the cell-site location system in *Carpenter* triggers Fourth Amendment concern, a city network where cell-site location is just one of numerous sensor collection efforts seems like a significant Fourth Amendment problem.

iii. Principle #3: Aggregating and Permanent Tracking Technologies Raise Fourth Amendment Concerns

The final lesson from the recent Supreme Court cases involves the nature of the privacy harm. Three related concerns surface in the Court’s opinions, involving tracking, aggregation, and permanence of the data collected.

First, in *Jones* and *Carpenter*, the Supreme Court was concerned with the tracking capabilities of new technology.¹⁵⁸ *Jones* was an individual GPS tracking case. *Carpenter* was a cell-site network tracking case. Any surveillance technology that allows long-term locational tracking will likely run squarely into this precedent.

Smart sensors raise tracking concerns as the sensors literally can track individuals across a city, revealing inferences drawn from locational details.¹⁵⁹

155. *Id.* at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

156. *Jones*, 565 U.S. at 416–17 (Sotomayor, J., concurring) (quoting *Di Re*, 332 U.S. at 595).

157. See Andrew Guthrie Ferguson, *The High-Definition, Artificially Intelligent, All-Seeing Future of Big Data Policing*, ACLU (Apr. 4, 2018, 3:00 PM), <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/high-definition-artificially-intelligent-all> [https://perma.cc/7H88-MZKS].

158. *Carpenter*, 138 S. Ct. at 2216 (“The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person’s past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.”); *id.* at 2217 (“As with GPS information, the time-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.’” (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring))).

159. See *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (“I would ask whether people 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,

If the GPS tracking in *Jones* violates a reasonable expectation of privacy, and acquisition of Timothy Carpenter's tracked cell-site signals violate an expectation of privacy, almost any person caught in a web of smart sensors with similar tracking capabilities will have a Fourth Amendment argument.¹⁶⁰

Second, in *Jones*, *Carpenter*, and *Riley*, the Court recognized that the aggregation of collected personal data created a distinct harm. In *Jones*, five Justices ruled that 28 days of tracking violated an expectation of privacy because of the aggregated locational details revealed.¹⁶¹ Similarly, in *Riley*, the Court recognized that the aggregation of information in a smartphone dwarfed a more limited collection of personal data.¹⁶² The *Riley* Court expressly addressed the qualitatively and quantitatively different nature of digital information collected on a smartphone-mini-computer. Finally, *Carpenter* echoed the dangers of aggregated locational collection through seven days of cell-site location data.¹⁶³

Smart sensors can be networked and aggregated to provide equivalent details about individuals. Though smart sensor data does not have to be aggregated or networked, the more it is collected and processed, the more it turns into a Fourth Amendment problem.¹⁶⁴

Finally, the Supreme Court expressed concern with a particular aspect of the collection and aggregation of tracking data, namely that it creates a backwards-looking permanent dataset which can be searched without legal justification. As was mentioned by Chief Justice Roberts, the collection of data created a "time-machine" problem.¹⁶⁵ As the Court stated in *Carpenter*:

sexual habits, and so on."); *id.* at 430 (Alito, J., concurring in judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

160. *Carpenter*, 138 S. Ct. at 2218 ("In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*.").

161. *Id.* at 2220; *Jones*, 565 U.S. at 403, 413, 415, 430.

162. *Riley v. California*, 134 S. Ct. 2473, 2489 (2014) ("The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.").

163. *Carpenter*, 138 S. Ct. at 2212, 2220.

164. See *infra* Section III.B.

165. Henderson, *supra* note 15, at 939.

Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI [Cell-Site Location Information], the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies [sic] of the wireless carriers, which currently maintain records for up to five years.¹⁶⁶

Like the revealing nature of information in David Riley's smartphone, the Court was concerned with the ability to collect personal data for one purpose but then have it available to search for any other purpose later on in time.

2. Fourth Amendment Principles for Structural Surveillance

The Supreme Court is still in the process of exploring how the Fourth Amendment fits the digital age. Yet, at least with surveillance technologies like smart sensors, its recent cases offer some clarity. Along the continuum of Fourth Amendment concerns, any surveillance system that (1) is arbitrarily applied; (2) is permeating in scope; (3) allows tracking; (4) aggregates personal details; and (5) can be permanently searched by government agents raises real Fourth Amendment concerns. City-wide smart sensors hit each of those concerns and, depending on how they are deployed, may face serious Fourth Amendment problems. At least when data is used against defendants in criminal cases,¹⁶⁷ the more centralized a system of sensor data collection, the more Fourth Amendment issues arise.

This Section seeks to apply this framework to four specific technologies discussed in Part II. Working backwards from the most centralized, aggregated, and networked to the least, this Section will address the Fourth Amendment implications of: (1) a city-wide API; (2) a networked video analytics system; (3) government-regulated utilities; and (4) smart sensor-enabled streetlights. As will be seen, the Fourth Amendment search analysis will depend on the design choices to keep data localized, networked, aggregated, and/or centralized.

B. THE FOURTH AMENDMENT APPLIED TO SMART SENSORS

As discussed in Part II, sensor data can be networked or isolated, aggregated or siloed. Further choices about tracking or anonymity can be built into the network's design specifications. As explained below, along the continuum of data collection available with smart sensors, the Fourth

¹⁶⁶. *Carpenter*, 138 S. Ct. at 2218.

¹⁶⁷. As will be discussed, there exists an open Fourth Amendment question about how to litigate concerns over generalized mass surveillance. Issues of standing and harm arise and might limit the impact of the Fourth Amendment. But, at least in terms of data used in criminal cases against criminal suspects, the Fourth Amendment harms will be justiciable.

Amendment is most concerned about arbitrary, permeating, aggregating, permanent, and individualized systems of surveillance.¹⁶⁸ The farther along the continuum, the more likely the acquisition of information would be a Fourth Amendment search.

1. Integrated Data Collection Systems: API

Smart things and smarter people will wander around a smart city.¹⁶⁹ These people could be connected by a digital layer that tracks various movements and actions.¹⁷⁰ This layer might involve an interconnected system of sensors which might include RFID chips, cellular connections, Wi-Fi, Bluetooth, or technologies not yet invented.¹⁷¹ In an API, the goal is to stream data back to either a central government monitoring service or private contractors to improve the functioning of city services. As the city becomes the digital platform, tracking technologies will link back to an identifiable object (e.g., car or person). This ubiquitous connection—collection through a digital layer—likely violates a reasonable expectation of privacy because it is doing exactly the type of aggregated, continuous personal data acquisition of locational data by government agents criticized by *Carpenter* and in *Jones* (in concurrence).¹⁷² At least when linked to an identifiable object (e.g., smartphone, smart car, smart home, biometric signature), this type of tracking is a Fourth Amendment search.

Under a reasonable expectation of privacy theory, are integrated, city-wide API systems unconstitutional if they continually acquire and aggregate this type of comprehensive personal data without a warrant? The answer is probably “yes,” at least for tracking of individuals in public over a period of time. The information is aggregated, building up the same type of informational harm as *Jones*’ GPS tracking.¹⁷³ The information is revealing,

168. Other scholars have addressed how the Fourth Amendment might be better considered in a systemic way. See Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1042 (2016) (“While our Fourth Amendment framework is transactional, then, surveillance is increasingly *programmatic*.”); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 92–97 (2016); Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident*, 82 U. CHI. L. REV. 159, 162 (2015). My argument here is different in that the system at issue is literally a system of surveillance, not just a conceptual way to think about police power.

169. See Mark Underwood, *Smart Car, Meet the Smart City*, DAILY BEAST (July 12, 2017, 7:37 PM), <https://www.thedailybeast.com/smart-car-meet-the-smart-city> [<https://perma.cc/C98Z-N52D>].

170. See *supra* notes 85–92 and accompanying text.

171. See *supra* notes 98–103 and accompanying text.

172. See *supra* Section III.A.1.

173. Ferguson, “*Smart*” *Fourth*, *supra* note 11, at 606 (“[W]hile Justice Scalia attempted to ground his *Jones* argument in property rights, the harm of affixing the GPS device was not in any real sense to physical property (the car was undamaged). The real harm was exposing the revealing personal data about the effect (car). . . . The ‘use’ in that case was the capturing of data trails via satellite transmissions communicated by cell phone to a government computer. By using

opening inferential clues about interests and activities like the *Carpenter* records.¹⁷⁴ The information is being acquired by state actors, at the direction of government officials (including law enforcement). As Paul Ohm has written, data that is “deeply revealing” and allows for a deep, broad, and comprehensive reach by automatic means is exactly the type of invasion the *Carpenter* Court found violated the Fourth Amendment.¹⁷⁵

Interestingly, this Fourth Amendment search occurs even if the system does not identify a person by name, but only a unique tracking number. From a Fourth Amendment perspective—similar to Timothy Carpenter’s cellphone and cell-site location tracking—the fact that the government is just collecting a digital identifier (not a name) does not avoid the Fourth Amendment problem.¹⁷⁶ In *Carpenter*, police “searched” when they acquired and gained access to the third-party data which could later be used to identify Timothy Carpenter’s location.¹⁷⁷ In the smart sensor context, whenever a government entity acquires any of these data trails (which could be every moment of the day through ever-present sensors), this act could run afoul of the reasonable expectation of privacy search test. Again, applying reasonable expectation of privacy in public principles, this type of aggregated collection of location is a warrantless search.¹⁷⁸

Also, the fact that sensors might be controlled by third-party vendors does not change the reach of the Fourth Amendment. First, the Supreme Court plainly stated that “the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection.”¹⁷⁹ The Fourth Amendment applies when “the Government employs its own surveillance technology . . . or leverages the technology of a [private company].”¹⁸⁰ As Justice Alito noted in his *Carpenter* dissent, “the Court effectively allows Carpenter to object to the ‘search’ of a third party’s property, not

the car to track its owner, the government invaded the informational security of the effect.” (footnotes omitted)).

174. *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (“[T]he Court has already rejected the proposition that ‘inference insulates a search.’” (quoting *Kyllo v. United States*, 533 U.S. 27, 35 (2001))).

175. Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 370 (2019) (quoting *Carpenter*, 138 S. Ct. at 2223).

176. In *Carpenter*, what was collected was a number associated with an identifier. The name Timothy Carpenter had to be linked via these digital identifiers. See *Carpenter*, 138 S. Ct. at 2211–12.

177. Orin Kerr, *When Does a Carpenter Search Start—and when Does It Stop?*, LAWFARE (July 6, 2018, 10:24 AM), <https://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop> [<https://perma.cc/E83X-LWKU>] (discussing the open questions after *Carpenter* of when a Fourth Amendment search of digital cell-site records starts and ends).

178. This conclusion again assumes a collection of data that is used in a criminal case. Standing to bring a similar challenge as a civil rights action or facial challenge is a hurdle that would need to be cleared.

179. *Carpenter*, 138 S. Ct. at 2217.

180. *Id.* (emphasis added).

recognizing the revolutionary nature of this change.”¹⁸¹ So the fact that smart cities would rely on third-party data collectors as intermediaries would not extinguish Fourth Amendment claims.

It also does not matter that the data is collected for commercial purposes. As the *Carpenter* Court stated, “[a]lthough such records are generated for *commercial purposes*, that distinction does not negate Carpenter’s anticipation of privacy in his physical location.”¹⁸² Thus, in a smart city, even one “managed” by a private company, the fact that records were held by a commercial party would not extinguish constitutional expectations of privacy. Essentially, the Court erased the distinction between rules governing searches of digital records and physical searches of people, homes, papers, and effects.¹⁸³ Now both types of searches require a reasonable expectation of privacy analysis.¹⁸⁴

If accurate, this reading of *Carpenter* directly impacts the ability of government to access third-party records and raises the real concern that in automatically acquiring these records, the government is routinely “searching” without a warrant. If the magic of a smart city is to constantly and seamlessly collect third-party data from all its citizens through an API, then by design the government is acquiring constitutionally-protected records without a warrant. At least for comprehensive, aggregated, digital records that are the type that would deserve a reasonable expectation of privacy, this collection runs afoul of the Fourth Amendment—unless a warrant or applicable exception applies.

2. Visual Surveillance & Object Recognition

Video cameras equipped with some level of object recognition technology will be a part of a smart city.¹⁸⁵ Object recognition software has already made its way to not-so-smart cities through ALPRs,¹⁸⁶ facial

181. *Id.* at 2260 (Alito, J., dissenting).

182. *Id.* at 2217 (majority opinion) (emphasis added).

183. *Id.* at 2255 (Alito, J., dissenting) (“For the majority, this case is apparently no different from one in which Government agents raided Carpenter’s home and removed records associated with his cell phone.”); *id.* (“[The majority] decides that a ‘search’ of Carpenter occurred within the meaning of the Fourth Amendment, but then it leaps straight to imposing requirements that—until this point—have governed only *actual* searches and seizures.”).

184. *See id.*

185. STANLEY, *supra* note 72, at 3; Scott Dunn, *Harnessing the Power of Video to Create Smart Cities*, SMARTCITIESDIVE (Oct. 9, 2018), <https://www.smartcitiesdive.com/news/harnessing-the-power-of-video-to-create-smart-cities/539209> [<https://perma.cc/SFA3-KF67>]; Rick Rojas, *In Newark, Police Cameras, and the Internet, Watch You*, N.Y. TIMES (June 9, 2018), <https://www.nytimes.com/2018/06/09/nyregion/newark-surveillance-cameras-police.html> [<https://perma.cc/8QDS-PR5U>]; Aviva Shen, *New Orleans Eyes Bars and Restaurants as New Focus of Surveillance*, BLOOMBERG CITYLAB (Feb. 9, 2018, 8:00 AM), <https://www.citylab.com/life/2018/02/new-orleans-eyes-bars-and-restaurants-as-new-focus-of-surveillance/552836> [<https://perma.cc/ULW4-S7CM>].

186. Koops et al., *supra* note 80, at 672–74.

recognition technologies,¹⁸⁷ and literal object recognition technology that can, for example, pick out the color of a hat, or identify a particular sports team logo on a shirt.¹⁸⁸ Coded digitally, the video images can be stored and searched as needed.¹⁸⁹

This collection of searchable video footage raises Fourth Amendment concerns, but any conclusion rests on weighing the principles of aggregation, permanence, and pervasiveness. From a pure tracking analogy, the ability to track cars, people, or objects as they go about a city raises privacy concerns similar to the *Jones* concurrence and the *Carpenter* majority. If a car's location (for 28 days) or a cell phone's aggregated location (for seven days) violates a reasonable expectation of privacy,¹⁹⁰ so would this visual tracking surveillance system that can reveal a car or a person across a city for a month or more.¹⁹¹ A government agent accessing a database of stored video (searchable by identifiable object) is not much different from a government agent accessing a database of stored cell phone locations.

Of course, the level of individualized detail can be modified to protect privacy. For example, a privacy-protective object recognition system could identify the outlines or shadows of people, cars, and bicycles without identifying the particular person associated.¹⁹² This type of technological fix might avoid Fourth Amendment search problems (in theory) because the identification would not be precise or searchable. But if a less privacy-protective model is adopted, the visual surveillance net will run square into Fourth Amendment search principles.

Similarly, the localization of video surveillance might reduce Fourth Amendment concerns. Along the continuum of systemic surveillance, a single camera recording a street scene is qualitatively and quantitatively different than a series of networked cameras that can track a person from street to street over long periods of time.¹⁹³ Minimizing aggregation and permanence concerns and limiting tracking capabilities might be the difference between a constitutional surveillance system and an unconstitutional one. In fact, the more the technology avoids the principles articulated earlier, the more likely the technology will survive Fourth Amendment scrutiny.

187. Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961, 1972–73 (2018).

188. See *supra* notes 61–62 and accompanying text.

189. Fussell, *supra* note 70.

190. See *supra* notes 161–63 and accompanying text.

191. See Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. (forthcoming 2021).

192. See *supra* note 107 and accompanying text.

193. See, e.g., *People v. Tafoya*, No. 17CA1243, 2019 WL 6333762, at *6–8 (Colo. App. Nov. 27, 2019); *United States v. Houston*, 965 F. Supp. 2d 855, 871 (E.D. Tenn. 2013); *State v. Jones*, 903 N.W.2d 101, 113–14 (S.D. 2017); *United States v. Anderson-Bagshaw*, No. 12-3074, 2012 WL 6600331, at *7 (6th Cir. Dec. 19, 2012).

3. Public Utilities

A residential street in a smart city will have houses and apartments so people can live there. These homes will become part of the smart infrastructure of a city. Utilities will connect these dwellings using sensors creating hard questions about which places should remain private and which might lose an expectation of privacy.

The Supreme Court has acknowledged that “[a]t the very core’ of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’”¹⁹⁴ The protection covers the information coming from inside the house that could not otherwise be obtained by physical surveillance.¹⁹⁵ In *Kyllo v. United States*, the Court held that police interception of heat patterns emanating from a home using a thermal imaging device was a Fourth Amendment search.¹⁹⁶ In *Florida v. Jardines*, the Court held that a dog sniff of marijuana scents outside a front door was a Fourth Amendment search.¹⁹⁷ Further, the concurring Justices in *Jardines* argued that invasive visual surveillance into the house (e.g., with binoculars) would also be a search.¹⁹⁸ The sensitive or intimate nature of the information obtained was immaterial; all that mattered was the source of the information—namely the home.¹⁹⁹

In the smart sensor context, a smart home can become an incredibly revealing source of intimate data. First, government entities like public utilities might directly collect information from a private house. For example, electrical and water use from a smart home meter might be a direct

194. *Kyllo v. United States*, 533 U.S. 27, 31 (2001) (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)).

195. *Id.* at 34 (“We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area,’ constitutes a search—at least where (as here) the technology in question is not in general public use.” (citation omitted) (quoting *Silverman*, 365 U.S. at 512)).

196. *Id.* at 40 (“Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.”).

197. *Florida v. Jardines*, 569 U.S. 1, 3–4, 11–12 (2013).

198. *Id.* at 12–13 (Kagan, J., concurring) (stating the Fourth Amendment protects against “police officers . . . standing in an adjacent space and ‘trawl[ing] for evidence with impunity” (alteration in original) (quoting *id.* at 6 (majority opinion))); see also *Collins v. Virginia*, 138 S. Ct. 1663, 1671 (2018) (“In physically intruding on the curtilage of Collins’ home to search the motorcycle, Officer Rhodes not only invaded Collins’ Fourth Amendment interest in the item searched, *i.e.*, the motorcycle, but also invaded Collins’ Fourth Amendment interest in the curtilage of his home.”).

199. *Kyllo*, 533 U.S. at 37 (“In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.”); *id.* at 38 (“[T]here is no necessary connection between the sophistication of the surveillance equipment and the ‘intimacy’ of the details that it observes—which means that one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful.”).

government collection. Second, private companies might offer smart homes filled with conveniences (e.g., smart thermostats, coffee makers, beds, and toothbrushes), along with a host of augmented home information devices (e.g., Amazon Echo, Google Home, Nest, Facebook's Portal TV).²⁰⁰ This data usually finds itself mediated by a private third-party company, but reveals granular details about when people wake up, eat, sleep, have sex, shower, listen to music, and when and what they watch on television.²⁰¹ In a smart city, like a normal city, warrantless collection of this information from a home would be a Fourth Amendment search.

The Seventh Circuit Court of Appeals recently held that the government collection of electricity levels from a home using a "smart meter" constituted a Fourth Amendment search under *Carpenter*.²⁰² The Court held that though "reasonable," the act of a public utility obtaining electricity information from a home through a smart meter was technically a "search."²⁰³ Relying on *Carpenter*, the Seventh Circuit reasoned that whether viewed as a government entity or a private third party, the Fourth Amendment still protected this private information originating from a constitutionally-protected source like the home.²⁰⁴ Other digital trails collected directly from a home's smart devices will likely be similarly analyzed as protected because of their shared source.

Along the continuum of digital search principles, the collection of private information from private homes is pretty significant. Though the tracking principle is not implicated, concerns about aggregation, permanence, permeation, and the fact that it would arbitrarily apply to everyone without individualized suspicion, all raise real concerns. In fact, many of the traditional Fourth Amendment search principles blend with new principles to make a strong claim that the warrantless collection of data from our homes (even as utilities or infrastructure) would be a search.

Of course, if data control mechanisms were designed to avoid some of the Fourth Amendment concerns, the constitutional analysis might be different. First, if the data was not identifiable, the aggregation and privacy problems would abate. Second, if the data was not permanently stored, concerns about retrospective searching could be avoided. Third, if the data were siloed from other forms of data collection, one type of utilities data (i.e., water usage, electricity) might not be seen as invading an expectation of

200. See generally Ferguson, "Smart" Fourth, *supra* note 11 (discussing how data collected from "smart" devices should be protected under the Fourth Amendment).

201. See Joshua McNichols, *A Smart Home Neighborhood: Residents Find It Enjoyably Convenient or a Bit Creepy*, NPR (Nov. 9, 2019, 3:04 PM), <https://www.npr.org/2019/11/09/777747209/a-smart-home-neighborhood-residents-find-it-enjoyably-convenient-or-a-bit-creepy> [https://perma.cc/75Z6-78HP] (discussing the selling of a data-driven and data-collecting home).

202. *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 526–27 (7th Cir. 2018).

203. *Id.*

204. *Id.*

privacy. As will be discussed in Part VI, all of these technical choices to collect, share, aggregate, or deanonymize data are choices that can be made at a city-wide level to protect privacy.

4. Smart Streetlights

On the safest side of the Fourth Amendment continuum are smart sensors that by design are programmed to limit the collection of data. Smart streetlights offer a good example. One version of a smart streetlight might just be a sensor that provides data about electrical efficiency, use, or need of repair.²⁰⁵ Another type could be a sensor that triggers when a person passes by as a signal to light up, but does not capture any other information.²⁰⁶ Of course, the streetlights could be linked in a network of other streetlights, and energy data could be aggregated.²⁰⁷ But a lack of identifying information and tracking capabilities could also remove it from Fourth Amendment scrutiny.

Simple sensors, if designed to remain simple, localized, and limited, might well remain outside of core Fourth Amendment concerns. As many sensors can be designed to be networked or not, and to collect limited information or not, this recognition might suggest a way forward for city design. As will be discussed, these data choices at the sensor level might have much broader constitutional implications for society.²⁰⁸

Of course, smart streetlights need not remain siloed and limited in capability. Early deployments have raised concerns that these simple sensor devices could be repurposed to collect additional data including locational information.²⁰⁹ Sensors can advance in collection capacity and be connected relatively easily to things like video.²¹⁰ As one civil liberties advocate cautioned, “I think rather than call them smart bulbs in smart cities I’d call them surveillance bulbs in surveillance cities.”²¹¹ Though not originally designed to collect anything other than maintenance data about the lights themselves, the

205. *NYPA Installs More than 2,400 LED Streetlights Throughout New York City*, T&D WORLD (Jan. 14, 2020), <https://www.tdworld.com/electric-utility-operations/article/21120518/nypa-installs-more-than-2400-led-streetlights-throughout-new-york-city> [<https://perma.cc/NRJ5-LC5L>].

206. See MAHADEV EAKAMBARAM, INTEL, SMART STREET LIGHTS FOR BRIGHTER SAVINGS AND OPPORTUNITIES 1, 3 (2017), <https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/smart-street-lights-for-brighter-savings-solutionbrief.pdf> [<https://perma.cc/7EXZ-92N3>].

207. Justin Rohrlach & Dave Gershgorin, *The DEA and ICE Are Hiding Surveillance Cameras in Streetlights*, QUARTZ (Nov. 9, 2018), <https://qz.com/1458475/the-dea-and-ice-are-hiding-surveillance-cameras-in-streetlights> [<https://perma.cc/VT4K-GQKF>].

208. See *infra* Part VI.

209. Gomez, *supra* note 48.

210. See Sarah Holder, *In San Diego, ‘Smart’ Streetlights Spark Surveillance Reform*, BLOOMBERG CITYLAB (Aug. 6, 2020, 12:52 PM), <https://www.bloomberg.com/news/articles/2020-08-06/a-surveillance-standoff-over-smart-streetlights> [<https://perma.cc/KHZ5-AYXV>].

211. Holder, *supra* note 84 (quoting Chad Marlow of the ACLU).

growth of thousands of sensor locations has raised questions for how they might be used in the future.²¹²

C. RESPONSES TO THE REASONABLE EXPECTATION OF PRIVACY PUZZLE

Smart sensor advocates might push back that such locational tracking—even on an API, city-wide scale—should not be considered a Fourth Amendment issue. After all, the collections are conducted in public, the tracking is ubiquitous rather than targeted, and citizens are consenting to collection by being present and using city services. In addition, the type of data, the mode of acquisition, and the purpose for collection are different in kind than traditional Fourth Amendment law enforcement-focused searches. Though not without some persuasive force, each one of those arguments was explicitly or implicitly rejected in *Carpenter* in the context of far less invasive cell-site location tracking. This Section briefly responds to these arguments, examining concerns about: (1) public exposure; (2) consent—assumption of risk; (3) the type of data at issue; and (4) the means of acquisition.

1. Public Exposure

As an initial matter, take the argument that because the data collection is all occurring in public, locational data does not deserve an expectation of privacy. Before *Jones* and *Carpenter*, the argument that public exposure undermined a reasonable expectation of privacy would likely be persuasive with the caveat that the *Knotts* Court expressed concern about mass surveillance in public.²¹³ But after *Jones* and *Carpenter*, the long-term, continuous collection of this type of aggregated public information—including public location tracking—is likely a search for Fourth Amendment purposes. Compared to a GPS device on a car or a cell-site record for a phone, the pervasive, multi-prong collection of smart city data vastly overwhelms the type of single-source public surveillance now requiring a

212. See POLICING PROJECT, N.Y.U. L., *PRIVACY AUDIT & ASSESSMENT OF SHOTSPOTTER, INC.’S GUNSHOT DETECTION TECHNOLOGY* 10–15 (2019), <https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d41808gee1e50001b5f9f9/1564573839757/Privacy+Audit+and+Assessment+of+Shotspotter+Flex.pdf> [<https://perma.cc/BF88-YAGL>]; Jesse Marx, *Smart Streetlights Aren’t Delivering the Data Boosters Promised*, VOICE OF SAN DIEGO (Apr. 29, 2020), <https://www.voiceofsandiego.org/topics/government/smart-streetlights-arent-delivering-the-data-boosters-promised> [<https://perma.cc/8KGL-YKYL>].

213. *Carpenter v. United States*, 138 S. Ct. 2206, 2215 (2018) (“This Court in *Knotts*, however, was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance. The Court emphasized the ‘limited use which the government made of the signals from this particular beeper’ during a discrete ‘automotive journey.’ Significantly, the Court reserved the question whether ‘different constitutional principles may be applicable’ if ‘twenty-four hour surveillance of any citizen of this country [were] possible.’” (citation omitted) (quoting *United States v. Knotts*, 460 U.S. 276, 283–85 (1983))); *Knotts*, 460 U.S. at 284 (“[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.”).

warrant. The fact that people or data have been exposed to the public does not end the Fourth Amendment analysis.

A second related argument is that maybe because of the explicit surveillance threats inherent in a smart city, one's ordinary expectation of privacy should be replaced with a specially defined smart city expectation of privacy (which would be significantly less protective than that of a traditional city). The argument would be that if you walk around a city with warning signs symbolically and literally informing you that you have no expectation of privacy, maybe you should not have any expectation of privacy. This argument unearths the long-held criticism of the reasonable expectation of privacy doctrine—that it can be too easily overcome if the government announces that there is no longer an expectation of privacy.²¹⁴

If the Fourth Amendment is going to apply in smart cities, however, it cannot be that governments can simply circumvent constitutional protections by announcing a city-wide change to expectations of privacy.²¹⁵ The whole point of the Fourth Amendment is to figure out the balance between constitutional and unconstitutional searches, not erase the protections by announcing the arrival of the smart surveillance state. Though other exceptions or interpretations might apply, a blanket city-wide exception to the Fourth Amendment by fiat will not hold.²¹⁶

2. Consent—Assumption of Risk

A second response might be that citizens assume the risk of losing their privacy when they choose to live in a smart city—that by living in a smart city one “consents” to digital tracking.²¹⁷ Though not an irrational argument, it runs against the *Carpenter* majority's determination that assumption of risk should not be read into the use of societally necessary communication tools.²¹⁸

²¹⁴. See *Smith v. Maryland*, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (discussing how law enforcement could not constitutionally search all mail just by announcing to the general public that mail no longer had an expectation of privacy).

²¹⁵. William Shepard McAninch, *Unreasonable Expectations: The Supreme Court and the Fourth Amendment*, 20 STETSON L. REV. 435, 444 (1991) (discussing how the government could not eviscerate Fourth Amendment freedoms by fiat).

²¹⁶. See *infra* Section V.A (discussing the special needs exception).

²¹⁷. This argument either falls under the “consent exception” to the Fourth Amendment or the related argument that one assumes the risk of disclosure by entering a smart city. Compare Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (explaining the underlying consent theory of the third-party doctrine), with Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009) (challenging the consent argument).

²¹⁸. *Carpenter*, 138 S. Ct. at 2220 (“Cell phone location information is not truly ‘shared’ as one normally understands the term. In the first place, cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society.” (quoting *Riley v. California*, 134 S. Ct. 2473, 2484 (2014))); see also *id.* (“Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-

We do not assume the risk or consent to cell-site tracking even though we might understand (at some level) about how cell phones work. As the Court states: “Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily ‘assume[] the risk’ of turning over a comprehensive dossier of his physical movements.”²¹⁹

Similarly, traveling in public in a smart city is not a voluntary relinquishment of rights. Just as cell phone users do not voluntarily give up their locational privacy in an ordinary city, citizens in a smart city are not voluntarily giving up information that is being collected automatically and ubiquitously. In a smart city, you cannot go “off the grid” because the city is the grid.²²⁰ Like a cell tower, the collection simply happens and the automatic, involuntary nature of this collection does not limit the Fourth Amendment’s reach and protection.²²¹

This consent–assumption of risk argument was more directly repudiated by Justice Neil Gorsuch in dissent: “Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a search of those papers by the government.”²²² Yes, you might choose to live in a smart city, but you do not consent to unconstitutional tracking by choosing to live there. Justice Gorsuch also dismissed a related “assumption of risk” argument that by giving information to a third party, you assumed the risk of the government obtaining it.²²³ Not only did this argument not make sense to him in the context of cell phone companies, but it did not convince him for other third-party situations.²²⁴ Like the majority, Justice Gorsuch viewed the assumption of risk idea no longer viable in the digital age. Other scholars have agreed that consent may not work with omnipresent surveillance technologies.²²⁵

mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates.”).

219. *Id.* (alteration in original) (quoting *Smith*, 442 U.S. at 745).

220. Thank you to Professor Wayne Logan for this point.

221. See Matthew Tokson, *Inescapable Surveillance*, 105 CORNELL L. REV. (forthcoming 2021).

222. *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

223. *Id.* (“The Court has said that by conveying information to a third party you ‘assum[e] the risk’ it will be revealed to the police and therefore lack a reasonable expectation of privacy in it. . . . That rationale has little play in this context. Suppose I entrust a friend with a letter and he promises to keep it secret until he delivers it to an intended recipient. In what sense have I agreed to bear the risk that he will turn around, break his promise, and spill its contents to someone else? More confusing still, what have I done to ‘manifest my willingness to accept’ the risk that the government will pry the document from my friend and read it *without* his consent?” (alteration in original) (quoting *Smith*, 442 U.S. at 744)).

224. *Id.*

225. Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1484–86 (2019); Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. (forthcoming 2020) (manuscript at 103–05), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557508 [<https://perma.cc/LP4S-NH3Y>].

3. Type of Data

A third response might be that though some types of data that a smart city collects could trigger Fourth Amendment concerns, not all city data should be considered equally. Some data is more private than other data.²²⁶ Without the long-term, aggregated nature of collection and acquisition, maybe much of the smart city falls outside of the Fourth Amendment's reach.

The *Carpenter* Court implicitly makes this distinction about the type of data at issue, suggesting that courts “consider[] ‘the nature of the particular documents sought’ to determine whether ‘there is a legitimate “expectation of privacy” concerning their contents.’”²²⁷ In dissent, Justice Anthony Kennedy critiqued the creation of a “multifactor analysis—considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness.”²²⁸ Though meant as a critique of the majority, this insight might be helpful in thinking through which forms of sensor data warrant Fourth Amendment protection.²²⁹ It may be the case that to determine whether a search has occurred, courts will be required to analyze not just the third-party nature of the records, but also the type of sensor data, the information, comprehensiveness, intimacy, and other factors.

This may provide a loophole for some smart city collection if it is designed in a way to avoid over-collection or to limit collection of more private data. Perhaps some smart data will need to be excluded because of the type of personal information revealed. In fact, as will be discussed in Part VI, a city might design its collection systems to avoid aggregation or long-term collection and thus design itself outside of Fourth Amendment constraints.

4. Acquisition of Data

The *Carpenter* decision leaves many open questions, but one of the biggest is when the “search” occurs.²³⁰ Unlike a search by physical means, *Carpenter* involved a request to obtain digital records held by a third party. Did the search occur when the third-party cell phone company collected the information, when the police asked for it, when they received it, when they examined the digital information or at some other time?²³¹

226. Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 4 (2020).

227. *Carpenter*, 138 S. Ct. at 2219 (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)).

228. *Id.* at 2234 (Kennedy, J., dissenting).

229. *Id.* at 2231 (“For each ‘qualitatively different category’ of information, the Court suggests, the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party.” (quoting *id.* at 2216, 2219–20 (majority opinion))).

230. Kerr, *Initial Reactions*, *supra* note 137, at 17–20; Orin S. Kerr, *Implementing Carpenter*, in *THE DIGITAL FOURTH AMENDMENT* (forthcoming) (manuscript at 15–16), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 [<https://perma.cc/VG8R-F38C>].

231. See Kerr, *Initial Reactions*, *supra* note 137, at 17–20.

The Court uses “acquire” and “acquisition”²³² to hint that the government request and/or subsequent possession of the records was the moment the Fourth Amendment applied. The Supreme Court’s language is ambiguous, leaving the question simply unanswered. This ambiguity around cell-site signals is heightened for sensor data. What would “acquire” or “acquisition” mean in the context of smart sensors that are collecting data both directly for government uses and by third parties all the time? Is the only data of constitutional interest the data acquired by the government? Also, does the government have to actually acquire the information or is the intent to acquire enough? In *Jones*, the search occurred with the placement of the GPS with the intent to gather information. If intent to acquire is enough, might that mean that the placement of the smart city sensors themselves would be enough to trigger constitutional scrutiny? Such a conclusion does not make much analytical sense, but these questions are not answered by *Jones* or *Carpenter*, leaving real uncertainty for smart city design.

D. CONCLUSION: REASONABLY SMART EXPECTATIONS OF PRIVACY IN PUBLIC

The Supreme Court’s piecemeal approach to digital privacy has created the unintended consequence that large-scale, smart city sensor systems likely violate the existing reasonable expectation of privacy test—at least if done in cooperation with law enforcement. Though perhaps an accident of doctrinal development, the result is an impediment to smart city development. Simply put, the expectations of modern privacy may not quite fit the expectations of our future cities. As will be discussed in Part VI, this tension may necessitate a change in expectations, or a change in law, or a change in technology—but it does require some change.

This tension with the expectation of privacy in public is only the first of two doctrinal analyses arising from existing Fourth Amendment law. The next Part looks at the recently resurrected trespass theory of searches as applied to structural surveillance.

IV. THE FOURTH AMENDMENT & SMART SENSORS AS TRESPASS SEARCHES

In addition to considerations of privacy, the Fourth Amendment is concerned with security from government intrusion into private property.²³³ Direct physical interference with personal property (“effects”) or people or homes has been a long-standing consideration in Fourth Amendment

232. *Carpenter*, 138 S. Ct. at 2214, 2220–24.

233. Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 309 (1998) (“The Fourth Amendment was a creature of the eighteenth century’s strong concern for the protection of real and personal property rights against arbitrary and general searches and seizures.”).

cases.²³⁴ As the Court recognized in *Carpenter*, “[f]or much of our history, Fourth Amendment search doctrine was ‘tied to common-law trespass’ and focused on whether the Government ‘obtains information by physically intruding on a constitutionally protected area.’”²³⁵

This theory of search as “trespass” or “physical intrusion” was reclaimed in *Jones v. United States*, with Justice Antonin Scalia’s majority opinion holding that the placement of a GPS device on a car was a search for Fourth Amendment purposes.²³⁶ In *Jones*, the Court held that a search occurs when “[t]he Government physically occupied private property for the purpose of obtaining information”²³⁷—in that case touching the bottom of the car with the purpose of obtaining locational information about the suspect via a GPS tracking device. One type of trespass search, then, occurs when the government physically touches personal property with the intent to gather information without a warrant.²³⁸

The Court expanded this theory to homes in *Florida v. Jardines*, where, in another majority opinion written by Justice Scalia, the Court held that a Fourth Amendment search occurred when police brought a drug-sniffing dog onto the curtilage of a home.

“The Amendment establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections: When ‘the Government obtains information by physically intruding’ on persons, houses, papers, or effects, ‘a “search” within the original meaning of the Fourth Amendment’ has ‘undoubtedly occurred.’”²³⁹

The touchstone of the search turned on the physical intrusion into a constitutionally protected space by government agents seeking information.²⁴⁰

234. *United States v. Jones*, 565 U.S. 400, 404–05 (2012) (“We have no doubt that such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.”).

235. *Carpenter*, 138 S. Ct. at 2213 (quoting *Jones*, 565 U.S. at 405, 406 & n.3); *Jones*, 565 U.S. at 406 (“As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas (‘persons, houses, papers, and effects’) it enumerates.”).

236. *Jones*, 565 U.S. at 404 (“We hold that the Government’s installation of a GPS device on a target’s vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a ‘search.’” (footnote omitted)).

237. *Id.*; see also *id.* at 414 (Sotomayor, J., concurring) (“[T]he trespassory test applied in the majority’s opinion reflects an irreducible constitutional minimum: When the government physically invades personal property to gather information, a search occurs.”).

238. *Id.* at 407 (majority opinion) (“As Justice Brennan explained in his concurrence in *Knotts*, *Katz* did not erode the principle ‘that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.’” (quoting *United States v. Knotts*, 460 U.S. 276, 286 (1983) (Brennan, J., concurring))).

239. *Florida v. Jardines*, 569 U.S. 1, 5 (2013) (quoting *Jones*, 565 U.S. at 406–07 n.3).

240. *Id.*

Finally, in *Grady v. North Carolina*, the Supreme Court applied the trespass theory to “persons.”²⁴¹ In *Grady*, the question before the Court was whether attaching a satellite-enabled monitoring device to a person as a condition of probation constituted a search.²⁴² As a registered sex offender, Grady was required by state law to wear a GPS-like device.²⁴³ He objected on Fourth Amendment grounds and the Court, applying the trespass–touch–physical intrusion theory of *Jones* and *Jardines*, agreed with his argument.²⁴⁴ “In light of [*Jones* and *Jardines*], it follows that a State also conducts a search when it attaches a device to a person’s body, without consent, for the purpose of tracking that individual’s movements.”²⁴⁵ The Court held that it was immaterial that the regulation was civil and not criminal in nature, recognizing “‘that the Fourth Amendment’s protection extends beyond the sphere of criminal investigations,’ and the government’s purpose in collecting information does not control whether the method of collection constitutes a search.”²⁴⁶ Thus, the third type of trespass search is when the government physically touches the person with the intent to gather information without a warrant.²⁴⁷

Applied to smart sensors embedded in our physical world, this Fourth Amendment trespass search rule raises a few hard questions. Though the vast majority of the surveillance apparatus will focus on digital, non-touching sensor searches, smart cities will still create a few anomalous trespass problems. For example, a smart sidewalk that records each footstep will technically meet the definition of a Fourth Amendment trespass search.²⁴⁸ The government will be physically touching people, with the intent to gather information about them. Though we do not usually think of the ground we walk on as touching us, it is in fact doing so. The same would hold for cars driving on smart roads which collect the data about driver’s speed, erratic behavior, etc. Like the trespass definition from *Jones*, the government (here,

²⁴¹. *Grady v. North Carolina*, 135 S. Ct. 1368, 1370–71 (2015) (per curiam).

²⁴². *Id.* at 1369–70.

²⁴³. *Id.* at 1369.

²⁴⁴. *Id.* at 1369–71.

²⁴⁵. *Id.* at 1370.

²⁴⁶. *Id.* at 1371 (citation omitted) (quoting *City of Ontario v. Quon*, 560 U.S. 746, 755 (2010)); see also *Camara v. Mun. Ct. of S.F.*, 387 U.S. 523, 534 (1967) (holding that housing inspections are “administrative searches” constituting “significant intrusions upon the interests protected by the Fourth Amendment”).

²⁴⁷. The Court has explicitly addressed physical intrusion on effects, homes, and people and would likely hold the same for physical papers. After all, the paradigmatic violation necessitating the original Fourth Amendment was government agents physically rifling through the papers of John Wilkes and others. Physical intrusion into papers would likely violate the Fourth Amendment on a trespass theory (in addition to violating an expectation of privacy).

²⁴⁸. While a little too technical, courts have found trespass searches on similarly technical trespasses. See, e.g., *Taylor v. City of Saginaw*, 922 F.3d 328, 332–36 (6th Cir. 2019) (holding that tire chalking to determine a violation of a parking law was a Fourth Amendment search under a *Jones* trespass theory, but was reasonable).

a sensor on the road surface) is touching a Fourth Amendment effect (the car) for the purposes of gaining information. Similarly, this reverse touch might happen when biometrics like fingerprints or palmprints are required to access smart devices or smart apartment buildings or workplaces. Again, the machine would be physically touching a human being to obtain information (biometric identification) from the person. This would be a technical trespass search.

The formalism of this approach should strike most observers as a bit odd. But then most observers of Justice Scalia's *Jones* trespass theory also thought the trespass nature of the harm made little sense. Touching the underside of a Jeep to affix a GPS device did not seem to be the real property, security, or privacy harm incurred, yet that harm is exactly what the majority held was a Fourth Amendment violation.²⁴⁹ Similarly, most homeowners would be hard-pressed to explain the tangible harm of a trespass by a police dog on one's porch, but that was the holding in *Jardines*.²⁵⁰ The formalism of unwanted physical intrusion with personal or real property aligns with the unwanted touching of a smart sidewalk trying to gain information about you.

Smart sensor technologies may also be embedded in effects or clothing such as to raise Fourth Amendment concerns.²⁵¹ Tracking sensors such as RFID chips or other smaller sensors are both cheap and unobtrusive, allowing almost any object to be tagged.²⁵² From sweaters to teddy bears, consumer goods are regularly tracked with readable technology.²⁵³ In trespass terms, the Fourth Amendment is triggered when the government places a sensor on the privately owned effect with the intent to get information. For example, affixing a smart license plate on a car, or a smart sensor on a trash can, or connecting a smart meter to a house, would all be similar trespasses. The search would occur when government officials affirmatively placed sensors on the private property of citizens in a smart city (not before they purchased the item). The ease of being able to trace a particular item may well tempt police because the tracking value is so clear.²⁵⁴

Trespass searches in a smart city may be more accidental than intentional, but because the intent is clearly to gather information the rule

249. *United States v. Jones*, 565 U.S. 400, 404–11 (2012).

250. *Florida v. Jardines*, 569 U.S. 1, 6–7 (2013).

251. Jill Duffy, *Why Smart Clothes Still Need Work*, PC MAG. (Jan. 29, 2016), <https://www.pcmag.com/news/why-smart-clothes-still-need-work> [<https://perma.cc/UKW3-9UJ9>]; *Smart Clothing*, WAREABLE, <https://www.wareable.com/smart-clothing> [<https://perma.cc/6A6T-7BE7>].

252. Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2330–31 (2007) (discussing RFID tagging of pets, students' backpacks, and clothes).

253. *See id.*

254. The fact that these contacts are not done in a law enforcement capacity may not matter as much if you take the language of *Grady* seriously. In *Grady*, the Court recognized that non-criminal governmental intrusions also implicate the Fourth Amendment. *See Grady v. North Carolina*, 135 S. Ct. 1368, 1370–71 (2015) (per curiam).

becomes implicated. While I am not trying to overstate the reach of the *Jones–Jardines* line of physical trespass searches, such lines may well get crossed when building a physical city.

V. FOURTH AMENDMENT IN THE DIGITAL CITY: EXCEPTIONS?

To make the argument that some structural sensor systems are unconstitutional under both existing Fourth Amendment theories means overcoming a few objections. Perhaps, as in other special places, the rules governing the Fourth Amendment should be different. In this argument, a special needs exception—akin to that applied to places like airports, stadiums, subways, schools, and border crossings—should control the analysis.

The second and perhaps more compelling objection is that though some smart sensor surveillance constitutes a technical Fourth Amendment search, the search is nevertheless “reasonable” under the Fourth Amendment. In many Fourth Amendment cases, the Supreme Court has addressed only the threshold search question and not the ultimate reasonableness of the governmental actions. Both of these objections will be addressed in turn.

A. SPECIAL NEEDS EXCEPTION

In evaluating Fourth Amendment protections, the Supreme Court has recognized that place matters.²⁵⁵ The Fourth Amendment protections at the border, at a school, airport, or the Super Bowl are different than other places.²⁵⁶ The “special needs” exception has developed to allow for a different balance between government interests and personal privacy in those areas and for certain government activities.²⁵⁷

The theory behind the “special needs” exception is that certain areas or activities or statuses require a reweighting of the normal balance of power between governmental investigating authority and individual privacy.²⁵⁸ At

²⁵⁵. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (“As the Court’s opinion states, ‘the Fourth Amendment protects people, not places.’ The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a ‘place.’”).

²⁵⁶. *United States v. Martinez-Fuerte*, 428 U.S. 543, 561–62, 566–67 (1976) (border); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653–54, 664–65 (1995) (schools); *MacWade v. Kelly*, 460 F.3d 260, 263 (2d Cir. 2006) (mass transit); *Johnston v. Tampa Sports Auth.*, 530 F.3d 1320, 1322–26 (11th Cir. 2008) (discussing the constitutionality of mass pat-down searches at a professional football game under the special needs and consent exceptions to the Fourth Amendment).

²⁵⁷. Christopher Mebane, Note, *Rediscovering the Foundation of the Special Needs Exception to the Fourth Amendment* in *Ferguson v. City of Charleston*, 40 HOUS. L. REV. 177, 178 (2003).

²⁵⁸. Kenneth Nuge, *The Special Needs Rationale: Creating a Chasm in Fourth Amendment Analysis*, 32 SANTA CLARA L. REV. 89, 97–98 (1992) (“Since noncriminal penalties are assessed against citizens detected in administrative searches, and since these searches are primarily intended to advance government policy rather than to criminally punish, the Supreme Court has had little difficulty embracing the constitutionality of administrative searches premised on decreasing levels of suspicion.”).

these times, the government interest gets priority because the government is not acting in its usual investigatory policing capacity.²⁵⁹ For example, at the international border, the strong governmental interest of national sovereignty overcomes the weaker privacy interest of individual entering the country.²⁶⁰ Some warrantless searches are allowed at the border because the government is acting to guard its sovereignty, not necessarily investigate crimes.²⁶¹ At a public school, the obligation of school officials to provide a safe learning environment outweighs unfettered student privacy rights.²⁶² School officials are given greater latitude to search students because they are not solely acting as criminal investigators.²⁶³ Similar rebalancing happens at airports and on subways and other transit systems where the interests of public safety outweigh the limits of more traditional investigation roles.²⁶⁴ Similar exceptions apply to government activities, either because the person's status is treated differently in some way,²⁶⁵ or because the activity puts the government in a non-policing role.²⁶⁶ All special needs exceptions share this same reality—there is something special about the place or activity that shifts the focus from the normal concern about investigative police power.

The question becomes: Should smart cities be considered a special place necessitating the use of the “special needs” exception? Are smart cities “Fourth Amendment-free” zones? The answer is likely no for two related reasons. First, the city-as-place is too large and undifferentiated a space to fit

259. For example, in the government employee context the fact that the government is the employer creates a special circumstance that warrants a different application of the Fourth Amendment. See Timothy C. MacDonnell, *The Rhetoric of the Fourth Amendment: Toward a More Persuasive Fourth Amendment*, 73 WASH. & LEE L. REV. 1869, 1923 (2016) (“The ‘special needs’ render the normal probable cause and warrant requirements impracticable when the government is engaged in ‘legitimate work-related, non-investigatory intrusions as well as investigations of work-related misconduct.’” (quoting *O'Connor v. Ortega*, 480 U.S. 709, 725 (1987))).

260. Robert S. Logan, Note, *The Reverse Equal Protection Analysis: A New Methodology for “Special Needs” Cases*, 68 GEO. WASH. L. REV. 447, 484 (2000) (“Border control is another type of important governmental interest that, in some circumstances, should give rise to a quasi-special needs classification.”).

261. See *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) (“[T]he Fourth Amendment’s balance of reasonableness is qualitatively different at the international border than in the interior.”).

262. *New Jersey v. T.L.O.*, 469 U.S. 325, 339–40 (1985) (recognizing different levels of Fourth Amendment rights in a public school setting).

263. *Id.* at 341–42.

264. Alexander A. Reinert, *Revisiting “Special Needs” Theory via Airport Searches*, 106 NW. U. L. REV. 1513, 1522–26 (2012) (discussing the legal history of airport searches).

265. *Griffin v. Wisconsin*, 483 U.S. 868, 873–74 (1987) (probationer); *O'Connor v. Ortega*, 480 U.S. 709, 725 (1987) (government employee).

266. For example, drug testing has been deemed a special needs exception. See, e.g., *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 658 (1995); *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 663–66 (1989); see also *Ferguson v. City of Charleston*, 532 U.S. 67, 75 (2001) (considering drug testing of pregnant mothers).

neatly within the exception. Second, the police role and activities in a smart city are not different enough to justify the exception.

In a world without any sensor-enhanced cities, one might make the argument that the first smart city should be a special place with different Fourth Amendment rules. Compared to every other city in America, the area would seem special enough. But that argument misconceives the justification for the special needs exception. The special places are not simply different places than the rest of the world around them, but are places involved in particular activities that warrant less privacy protection because of other non-law-enforcement interests at play.²⁶⁷ A smart city may have those places (schools, stadiums, subways), but also has every other place that a normal city does. Excepting out the entire city as special would make little sense. Instead, a smart city may replicate “special” places with more data collection in some places than others.²⁶⁸

Further, the special needs rationale does not comport with the relationship between police and citizens in a smart city. Police and citizens in such a city are not in any different relationship necessitating a special needs exception. When police are investigating crime in a smart city, they are investigating crime. Their role does not change just because it is happening with digital means. Whereas the special needs exception was created for government agents playing non-investigative roles (which will also happen in a smart city), as a general matter police will be playing the same role in both types of cities. It is not that special needs do not exist in the smart city, but they do not exist in any different way than a traditional city. Areas, activities, and statuses will give rise to special considerations, but not because they arise in a smart city. Smart cities might be special, but they do not create a generalized city-wide special needs exception.

B. REASONABLENESS

The Supreme Court has written that the “touchstone of the Fourth Amendment is ‘reasonableness,’” putting great emphasis on the “unreasonable” language in the Fourth Amendment.²⁶⁹ Though much of the debate in this Article (and the case law) draws the threshold line of when a government action becomes a Fourth Amendment “search,” the

267. Joseph S. Dowdy, *Well Isn't That Special? The Supreme Court's Immediate Purpose of Restricting the Doctrine of Special Needs in Ferguson v. City of Charleston*, 80 N.C. L. REV. 1050, 1055–56 (2002) (“Special needs exist where the privacy interests implicated by the search are minimal, and where the requirement of individualized suspicion places some important governmental interest in jeopardy.” (footnotes omitted)).

268. The puzzle of special needs areas in a smart city may warrant its own separate article.

269. *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)); *see id.* (“Our cases have determined that ‘[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant.’” (alterations in original) (quoting *Vernonia Sch. Dist.*, 515 U.S. at 653)).

reasonableness analysis asks whether searches without a warrant might still be constitutional under certain circumstances. For example, in the *Jones* GPS case, the Court's entire discussion focused on whether the attachment of a GPS device was a Fourth Amendment "search," and not whether this search was reasonable (and thus still constitutional).²⁷⁰

The debate over the relationship between the warrant requirement and reasonableness has long engaged Supreme Court Justices.²⁷¹ If interpreted broadly, reasonableness provides a work-around to the limitations imposed by the warrant requirement, as all evidence would be admitted if deemed reasonable (even if obtained without a probable cause warrant). Thus, the argument has offered those conservative Justices critical of the current threshold "search" tests a way around the doctrine.²⁷²

Here, the question is whether the collection of smart sensor data is nevertheless "reasonable" because the information is being collected for non-law-enforcement purposes. The Seventh Circuit decided its *Naperville* case on smart electricity readers in homes along those lines.²⁷³ There, the court held that collection of the municipal smart meter data from the home was a Fourth Amendment "search" after *Carpenter*, but that the collection was reasonable under the Fourth Amendment.²⁷⁴ The Seventh Circuit determined that because the smart meters were installed solely for electrical grid improvement and not for criminal investigation, the collection of electrical data was reasonable.²⁷⁵ The Seventh Circuit applied the Supreme Court's reasonableness test, assessing reasonableness "by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of

270. The Supreme Court explicitly acknowledged that they were not deciding the reasonableness issue because it had not been raised by the government. *United States v. Jones*, 565 U.S. 400, 413 (2012).

271. See, e.g., *California v. Acevedo*, 500 U.S. 565, 582 (1991) (Scalia, J., concurring in judgment) ("Although the Fourth Amendment does not explicitly impose the requirement of a warrant, it is of course textually possible to consider that implicit within the requirement of reasonableness. For some years after the (still continuing) explosion in Fourth Amendment litigation that followed our announcement of the exclusionary rule in *Weeks v. United States*, our jurisprudence lurched back and forth between imposing a categorical warrant requirement and looking to reasonableness alone." (citation omitted)).

272. Kathleen M. Sullivan, *Foreword: The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 98–99 (1992) ("[W]hen liberals win using rules, conservatives want balancing—as in the shift in Fourth Amendment law from the fixed requirements of a warrant or particularized cause to the ever-expanding substitution of multi-factored 'reasonableness' tests for searches and seizures instead."). Generally speaking, however, the current understanding is that when government officials are acting in an investigatory capacity, a judicial probable cause warrant is necessary, but when officials are acting in a non-investigative capacity courts apply a balancing of interests.

273. *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 528 (7th Cir. 2018).

274. *Id.* at 527–29.

275. *Id.* at 529 ("Smart meters allow utilities to reduce costs, provide cheaper power to consumers, encourage energy efficiency, and increase grid stability. We hold that these interests render the city's search reasonable, where the search is unrelated to law enforcement, is minimally invasive, and presents little risk of corollary criminal consequences.").

legitimate governmental interests.”²⁷⁶ In the electricity monitoring situation, the intrusion of collecting home energy levels was minimal, and the need for a smarter electrical grid was strong. On balance, the court determined that the equities favored the government.

Applied broadly to the smart city context, the questions would be: (1) whether the wholesale collection of smart data could be deemed reasonable because the information was not generated primarily for law enforcement reasons; and (2) whether on balance the intrusion of large-scale data collection favors legitimate government interests.

First, as a baseline, the Fourth Amendment protections have never been solely about protection from law enforcement as opposed to general government intrusion.²⁷⁷ Numerous cases refuse to draw neat lines between government investigation and police investigation.²⁷⁸ After all, the Fourth Amendment is a check on general governmental power, not just specific police power.

That said, when the government acts with a non-law-enforcement focus the Supreme Court has on occasion changed the analysis. The issue becomes whether there is a non-law-enforcement justification for the search which requires a different reasonableness balancing. The answer for a smart city is “maybe.” One could design a smart city to avoid sharing data with law enforcement. One could create mechanisms to blind officers from being able to access the collected data. A smart city government that consciously cut off data access to law enforcement (absent a warrant) might be much more likely to survive constitutional challenge. Similarly, intentional decisions to collect data only for non-law-enforcement purposes might strengthen the government’s defense about the purpose of collection. Though purpose alone cannot control the reasonableness analysis and a non-law-enforcement goal does not avoid all Fourth Amendment problems, these types of intentional choices about how to protect or minimize data might be critical for a city to claim the smart collection was reasonable.

276. *Id.* at 528 (quoting *Delaware v. Prouse*, 440 U.S. 648, 654 (1979)).

277. As the Supreme Court recognized in *Weeks*, the Fourth Amendment applies to all government actors, not just police or law enforcement actors. *Weeks v. United States*, 232 U.S. 383, 391–92 (1914), *overruled by* *Mapp v. Ohio*, 367 U.S. 643 (1961) (“The effect of the Fourth Amendment is to put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority, and to forever secure the people, their persons, houses, papers and effects against all unreasonable searches and seizures under the guise of law. This protection reaches all alike, whether accused of crime or not, and the duty of giving to it force and effect is obligatory upon all entrusted under our Federal system with the enforcement of the laws.”).

278. See *Grady v. North Carolina*, 135 S. Ct. 1368, 1371 (2015) (“‘It is well settled,’ however, ‘that the Fourth Amendment’s protection extends beyond the sphere of criminal investigations.’” (quoting *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755 (2010))); *Camara v. Mun. Ct. of S.F.*, 387 U.S. 523, 533 (1967).

The key is establishing that the relationship between smart data collection and law enforcement monitoring remains separate and distinct.²⁷⁹ Without specific memorandums of understanding or laws that forbid law enforcement access to city data, the default will likely be that police can obtain it like any other city information. In fact, because many cities will be designed to enhance public safety and because of the attraction of big data surveillance technologies, it would be odd for police not to have direct access to many of the data feeds. As will be discussed in Part VI, the data-sharing arrangement need not be set up this way, but without clear legal limits on police acquisition of smart data, it seems likely that police will have access.

The second big question is how a court would balance the government interests of data collection against individual privacy interests. As discussed in Part II, the potential privacy invasion in smart cities is at a scale never seen before, and the capacity to obtain granular data about individuals is unprecedented. Further, the government interest in obtaining the information is not terribly urgent. The need is ongoing and continuous, but usually not any sort of exigency. Though the whole point of a smart city is massive data collection, this does not necessarily translate into an automatic prioritizing of governmental access to all of that data over privacy interests. Any deference to government interests for particular governmental needs must confront the reality that the balancing rationale may not make sense at scale (with multiple overlapping sensor systems at issue). It is one thing to balance a particular surveillance tactic, or a special type of administrative inspection, or even a type of municipal efficiency; it is another thing to balance a collection of such tactics, inspection, and services that span an entire city and are all possibly aggregated. With city-wide mass surveillance, any individualized reasonableness balancing determination becomes quite difficult.

Both parts of the reasonableness analysis—purpose and balancing—can be made easier to analyze if smart city designers are intentional about the legal rules that govern the city. As will be discussed in the next Part, the choices made to draft legal protections into the blueprints of smart city design might be critically important not only to protecting privacy and security, and furthering innovation, but also to surviving a Fourth Amendment challenge that a smart city is unconstitutional.

VI. A DIGITAL PRIVACY-FOCUSED POSITIVE LAW

Some structural sensor surveillance likely violates the Fourth Amendment, which may reflect more on the limits of the Fourth Amendment than the new technologies. This Part describes how a smart city might design itself out of the confusion that is the Fourth Amendment search doctrine. This Part takes the insight that design choices can alter Fourth Amendment

279. See *supra* note 278 and accompanying text.

protections and expand them, proactively addressing privacy design and thus constitutional design.

Two considerations play a central role in this reimagining of Fourth Amendment protections. First, digital rights can be built into the municipal code of a smart city, regulating data collection, use, and sharing. Second, Privacy by Design²⁸⁰ principles that inform the technical engineering of smart devices, networks, and cities provide a framework for establishing normative expectations of privacy. Neither of these theories is new, but as applied to smart sensors, they offer concrete solutions to the data privacy puzzle. Because smart city infrastructure would be designed from scratch, unlike traditional *ex post* analyses of reasonable expectations of privacy, one can *ex ante* design these Fourth Amendment expectations and data rules from the outset and across the entire city. By designing a “legal layer”²⁸¹ into the architecture of a smart city, planners can shape citizens’ Fourth Amendment expectations.

To be clear, the ultimate Fourth Amendment determination will be made by judges with an obligation to interpret the U.S. Constitution.²⁸² Statutory or other law cannot replace the constitutional floor, but it can inform it and raise privacy protections above that floor so the Fourth Amendment question becomes less significant.²⁸³ A digital positive law would offer guideposts for courts attempting traditional analysis of the constitutionality of a particular law enforcement action.

This insight that positive law might clarify the Fourth Amendment search doctrine finds support in Justice Gorsuch’s *Carpenter* dissent, which discusses a positive law approach to the Fourth Amendment.²⁸⁴ The argument—itsself inspired by William Baude and James Stern’s article *The Positive Law Model of*

280. See generally ANN CAVOUKIAN, INFO. & PRIV. COMM’R OF ONT., *PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES* (Jan. 2011) [hereinafter CAVOUKIAN, *FOUNDATIONAL PRINCIPLES*], https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf [<https://perma.cc/7VR5-WYGP>] (describing seven information management principles that enhance information privacy).

281. See *infra* Section VI.E.

282. U.S. CONST. art. VI, cl. 2 (“This Constitution . . . shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.”).

283. Marc L. Miller & Ronald F. Wright, *Leaky Floors: State Law Below Federal Constitutional Limits*, 50 ARIZ. L. REV. 227, 228 (2008) (“One of the most widely accepted notions in American constitutional law is that the federal Constitution and interpretations of that Constitution by the Supreme Court of the United States set a ‘floor’ for personal liberties. State courts and state legislatures cannot properly go below the federal floor.”). Professors Miller and Wright critique this claim as being overbroad and inexact, but the claim still holds as a general assertion.

284. *Carpenter v. United States*, 138 S. Ct. 2206, 2270 (2018) (Gorsuch, J., dissenting) (“[P]ositive law may help provide detailed guidance on evolving technologies without resort to judicial intuition. State (or sometimes federal) law often creates rights in both tangible and intangible things.”).

the Fourth Amendment²⁸⁵—becomes even more useful when one can create a digital positive law from scratch. I argue that smart cities can establish a digital positive law floor that will set forth the Fourth Amendment parameters of privacy and security for both private actors and the government in a way that is more protective than the current standard. My argument is not that data rights should be converted into property rights, because without a privacy or human rights framework, property rights do not adequately protect data. Instead, I argue that positive law—which can grant data control and digital rights—in addition to technological choices might offer more protection.

This Part proceeds in five Sections. The first Section looks at the contours of Justice Gorsuch's Fourth Amendment theory of positive law as a source of constitutional framing. The second Section looks at data property and control laws that can be repurposed to create enforceable data rights, the interference with which would constitute a Fourth Amendment search. The third Section examines various positive law approaches separate from a pure property-focused framework. The fourth Section examines how the Fourth Amendment expectation of privacy threshold can be established through digital design principles. These principles, which create enforceable expectations of privacy, can be written into law at the outset. Finally, the fifth Section proposes the construction of a "legal layer" mapped on top of the digital layer that connects city sensors. This legal layer will govern, node by node, what happens to the collected sensor data in a smart city network. The result will be a smart city with Fourth Amendment protections enforced through municipal and computer code.

A. THE POSITIVE LAW MODEL

Justice Gorsuch's *Carpenter* dissent critiqued the existing theories of the Fourth Amendment, hinting that he was looking for another framework to address the doctrine in a digital age.²⁸⁶ Though not adopting a positive law approach, he suggested one might offer a promising option worth exploring in a future case.

As an initial matter, Justice Gorsuch noted that positive law has always influenced the Fourth Amendment: "From the founding until the 1960s, the right to assert a Fourth Amendment claim didn't depend on your ability to appeal to a judge's personal sensibilities about the 'reasonableness' of your expectations or privacy. It was tied to the law."²⁸⁷ Legal rules promulgated by

285. William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1825–26 (2016).

286. *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting) (looking for "another way" to answer the Fourth Amendment issues brought on by new technology).

287. *Id.*; see also *United States v. Jones*, 565 U.S. 400, 407–08 (2012) ("We have embodied that preservation of past rights in our very definition of 'reasonable expectation of privacy' which we have said to be an expectation 'that has a source outside of the Fourth Amendment, either by

duly constituted legislatures offered, he suggested, a form of clarity, thus allowing judges an easier time interpreting Fourth Amendment violations without resorting to more subjective sensibilities as to assumed societal expectations.²⁸⁸ Judges are, after all, more practiced at interpreting written law and less adept at judging societal norms. The appeal to an established written law was also, he claimed, more democratic,²⁸⁹ and thus (theoretically) more responsive to public will.²⁹⁰ Finally, the positive law could adapt—both to technology and changed circumstances—allowing greater flexibility. For example, one could draft laws about data ownership and data control, or mandate certain privacy protections, or create fiduciary or bailee relationships through legislative rules.²⁹¹ These rules need not even be statutory if there were a clear customary norm of a particular legal rule. To Justice Gorsuch, the appeal of positive law rested on this mixture of history, utility, legitimacy, and pragmatism.²⁹²

In his *Carpenter* dissent, Justice Gorsuch did not commit to a *general* positive law approach for the Fourth Amendment, but he did provide some useful clues to creating a *digital* positive law for personal data. For example, Justice Gorsuch noted that federal and state law “defin[es] ‘[p]roperty’ to include ‘property held in any digital or electronic medium.’”²⁹³ Digital information could be considered property if explicitly written into the law. In addition, Justice Gorsuch read the telecommunications law governing cell-site

reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.” (quoting *Minnesota v. Carter*, 525 U.S. 83, 88 (1998))).

288. *But see* Wayne A. Logan, *Fourth Amendment Localism*, 93 IND. L.J. 369, 372 (2018) (asking whether Fourth Amendment norms should be localized).

289. *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting) (“Beyond its provenance in the text and original understanding of the Amendment, this traditional approach comes with other advantages. Judges are supposed to decide cases based on ‘democratically legitimate sources of law’—like positive law or analogies to items protected by the enacted Constitution—rather than ‘their own biases or personal policy preferences.’” (quoting Todd E. Pettys, *Judicial Discretion in Constitutional Cases*, 26 J.L. & POL. 123, 127 (2011))).

290. *Id.* (“A Fourth Amendment model based on positive legal rights ‘carves out significant room for legislative participation in the Fourth Amendment context,’ too, by asking judges to consult what the people’s representatives have to say about their rights.” (quoting Baude & Stern, *supra* note 285, at 1852)).

291. *See* DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 103 (2004); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 614–16 (2015); Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 356 (“If there is a bailment relationship, this implies that data holders have a duty to secure data in a manner analogous to how bailees protect tangible property.”).

292. *See supra* notes 286–88 and accompanying text.

293. *Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J., dissenting) (quoting TEX. PROP. CODE ANN. § 111.004(12) (West 2017)) (“A similar inquiry may be appropriate for the Fourth Amendment. Both the States and federal government are actively legislating in the area of third party data storage and the rights users enjoy.” (citing Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2018))).

data as potentially creating a property right in the data akin to digital papers or effects: “It seems to me entirely possible a person’s cell-site data could qualify as *his* papers or effects under existing law.”²⁹⁴

Both examples show how statutory law could create enforceable property rights if drafted correctly. If the positive law explicitly granted property rights and control over the data, interference with the digital property could be considered a Fourth Amendment search.²⁹⁵ Despite the theoretical opening, Justice Gorsuch left any conclusion about these particular arguments for a future day because the record was insufficiently developed for further analysis.²⁹⁶ At least for the cell-site locational data at issue in *Carpenter*, Justice Gorsuch was not willing to follow a positive law approach.

Unlike a Supreme Court Justice who must look backwards to divine whether a statutory law explicitly created a positive law expectation in a specific case, urban planners in a smart city could design these “data as property” protections from the outset. And, once established in the law, any interference with this property interest without a warrant could be subject to Fourth Amendment limitations. Note also that Justice Gorsuch’s connection of property rights and positive law is just one possible option for positive law rules. Positive law can also create rules about control, deletion, rights, autonomy, and other non-property-based protections.

The next three Sections briefly explore how a smart city might think about creating a digital positive law for municipal data.

B. DIGITAL PROPERTY: FOURTH AMENDMENT PROTECTIONS THROUGH PROPERTY RIGHTS

In many legal contexts, data is property.²⁹⁷ Entire industries now exist to collect and sell personal data. In the smart city context, the city designers know that certain types of data will be collected as a matter of course.²⁹⁸ So, for example, the locational systems that track people through a city API via their smart devices could be (and likely will be) monetized to sell advertising

294. *Id.* at 2272.

295. See Baude & Stern, *supra* note 285, at 1873–74; Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 MISS. L.J. 1229, 1244–46 (2012); Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, 3.

296. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) (“The problem is that we do not know anything more. Before the district court and court of appeals, Mr. Carpenter pursued only a *Katz* ‘reasonable expectations’ argument. . . . Even in his merits brief before this Court, Mr. Carpenter’s discussion of his positive law rights in cell-site data was cursory. . . . In these circumstances, I cannot help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument.”).

297. See generally JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM (2017) (discussing the law around intellectual property of data).

298. Ava Kofman, *Google’s Sidewalk Labs Plans to Package and Sell Location Data on Millions of Cellphones*, INTERCEPT (Jan. 28, 2019, 7:05 AM), <https://theintercept.com/2019/01/28/google-alphabet-sidewalk-labs-replica-cellphone-data> [https://perma.cc/4QGN-JZUY].

or other goods.²⁹⁹ The data is valuable, but can also be protected. Data can be turned into a property right via law and protected from commercial acquisition without specific legal authorization.

Municipalities, having a role in city data collection, may be able to write laws that are protective of this information. So, for example, whereas the ordinary consumer and company contractual agreement over data might not protect the consumer at all, a municipal smart city government could rewrite that protection to explicitly grant a property right (or the right to control the data). In smart cities, the data rules can be precise and regulated *ex ante*. Through municipal code, a city could establish who owns data at every smart city collection point.

The reason why such a digital positive law might matter in the Fourth Amendment context is that by putting the data property rules in municipal law, a smart city can establish a threshold privacy–property line for a search.³⁰⁰ Just like a law that says entering the curtilage of a home is burglary or taking personal property is an interference with chattel, so laws can be written to protect data from acquisition. If digital positive law grants a property right in smart city data and if the data is acquired without a duly authorized warrant, it would make it a Fourth Amendment search (absent an exception).³⁰¹ Such a positive law approach might be unwieldy in an already established urban environment with existing property laws and norms that vary by jurisdiction. But when you are designing the smart city from scratch, you can write the rules at the creation.

In practical effect, this means that a smart city’s municipal body would need to think through the data ownership rules at the front end and write the ownership agreements into law. This would be a shift from the current company–consumer agreements that dominate data ownership in the United States. As but one example, the current data relationship with the free LinkNYC Wi-Fi kiosks in New York City offers a fairly standard trade off: In return for free Wi-Fi, city residents provide personal data to use the “free” service.³⁰² A smart city could rewrite the data relationship at the front end. A city could pass a law that residents own the data going into the Wi-Fi kiosk and

299. Valentino-DeVries et al., *supra* note 77; Summers, *supra* note 50.

300. But courts would still determine final Fourth Amendment interpretation. *See supra* note 282 and accompanying text.

301. The statutory rule might also obviate the need for many Fourth Amendment battles because the matter could be resolved as a statutory, non-constitutional matter.

302. Arman Tabatabai, *The Economics and Trade-Offs of Ad-Funded Smart City Tech*, TECHCRUNCH (Dec. 1, 2018, 11:00 AM), <https://techcrunch.com/2018/12/01/the-economics-and-tradeoffs-of-ad-funded-smart-city-tech> [https://perma.cc/NNgD-4EWW]; Kaveh Waddell, *Will New York City’s Free Wi-Fi Help Police Watch You?*, ATLANTIC (Apr. 11, 2016), <https://www.theatlantic.com/technology/archive/2016/04/linknyc-new-york-wifi-privacy-security/477696> [https://perma.cc/ZM4G-BEC6].

retain a property interest in the information.³⁰³ If a police detective should seek to gain access to this digital property without a duly authorized warrant, it would be considered a search for Fourth Amendment purposes because the law granted a clear property interest in the data with which the police officer has now interfered.³⁰⁴ The digital positive law establishing ownership would be explicit in the statute, and the police detective's access of the information would be a search under this positive law theory. Similar data ownership laws could be written for electrical use, trash, smart cars, smart phones, etc. The point is that because engineers design and build the system from the front end, they can establish the rules of when a search occurs.

Property-based rights protections, of course, have serious limitations because digital property is easily bargained away, and the power dynamics of the interaction remain starkly imbalanced. The surveillance capitalism economy that has monetized data demonstrates that individual choices over data do not result in much protection at all.³⁰⁵ A pure property-based positive law around data will likely mirror similar economic and social imbalances and create significant and unfair power imbalances. In fact, personal data might become the extractive raw materials for a data-driven economy, but one that does not equally share the value. As long as economically powerful technology companies control access, individual property rights will not be properly valued or balanced. This imbalance will be especially true when the data being negotiated involves necessary public goods like municipal services.

C. POSITIVE LAW: FOURTH AMENDMENT PROTECTIONS THROUGH LAW

Positive law need not be property-based. Positive law involves rules directed against private parties.³⁰⁶ One could, consistent with current positive law theories, shape data expectations through formal legal rules. As a recent example, the California Consumer Privacy Act reshaped data rights for individuals living in California³⁰⁷ as did the General Data Protection

303. As one example, Sidewalk Labs had proposed the creation of a civic data trust to avoid the problems of monetizing public data. A civic trust would control the public data and regulate its dissemination so as not to simply allow private companies to monetize it. *See* SIDEWALK LABS, *supra* note 105, at 11–16.

304. In many ways this is what Justice Gorsuch was exploring with his discussion of the property rights in the Stored Communications Act. *See* *Carpenter v. United States*, 138 S. Ct. 2206, 2270 (2018) (Gorsuch, J., dissenting).

305. *See generally* SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* (2019) (exploring the impacts of surveillance capitalism).

306. Baude & Stern, *supra* note 285, at 1825 (“Instead of making Fourth Amendment protection hinge on whether it is ‘reasonable’ to expect privacy in a given situation, a court should ask whether government officials have engaged in an investigative act that would be unlawful for a similarly situated private actor to perform. That is, stripped of official authority, has the government actor done something that would be tortious, criminal, or otherwise a violation of some legal duty?”).

307. CAL. CIV. CODE §§ 1798.100–1798.192 (West 2019).

Regulation's approach to data control in Europe.³⁰⁸ Though workings of both laws are beyond the scope of this Article, they offer examples of how such data protective laws can reshape expectations of data privacy through positive law.³⁰⁹

To be clear, positive law need not be the adoption of the Baude and Stern "positive law theory," which looks to violations of private law to interpret whether government action violates the Fourth Amendment.³¹⁰ In fact, a better framework might be based on Professor Richard Re's insightful critique of the Baude and Stern article and his proposal to establish a "positive law floor."³¹¹ As Professor Re suggests:

Whereas the positive law model would treat laws directed toward private parties as a hard ceiling on the meaning of the word "search," my suggestion is that courts might treat privacy laws directed toward private parties as a presumptive floor on the Fourth Amendment's prohibition against "unreasonable searches." On this view, when lawmakers guard against privacy intrusions *by private parties*, then similar intrusions *by the government* would be presumptively unreasonable.³¹²

In other words, the legislative choice to restrict private data collection in smart cities would provide powerful evidence that those limitations also restrict governmental collection of that data. Legislative action would inform what would be considered a reasonable government action by regulating private data collection. And again, because this positive law would be created at the outset to govern both private and government data collection, the legal expectations could be made more transparent.

Of course, there are real limitations of what Professor Wayne Logan calls "Fourth Amendment localism."³¹³ Any positive law will necessarily be localized to a place which can add significant complications to the analysis beyond that particular city.³¹⁴ One smart city might design legal protections different from another, and the influence of corporate power on such decisions could be quite substantial, if not dangerous. Writing municipal laws to govern privacy—especially with assistance of technology companies and engineers—may not

308. See generally Council Regulation 2016/679, 2016 O.J. (L 119) (EU) (establishing individuals' rights in regard to their data).

309. See, e.g., Nicholas F. Palmieri III, *Who Should Regulate Data?: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws*, 11 HASTINGS SCI. & TECH. L.J. 37, 59 (2020); Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1583–86 (2019).

310. Michael J. Zydney Mannheimer, *Decentralizing Fourth Amendment Search Doctrine*, 107 KY. L.J. 169, 211 (2018–2019).

311. Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 332–37 (2016).

312. *Id.* at 332.

313. Logan, *supra* note 288, at 372–76 (challenging the Fourth Amendment localism model).

314. *Id.*

necessarily reflect the interests of all community members. Fraught issues must be addressed: who holds political power, concerns about the marginalization of disadvantaged communities, structural economic incentives, and a whole host of socio-economic realities involving capacity, democratic engagement, and knowledge.

Yet this type of rethinking about how to design legal protections around surveillance technologies has already begun. Professors David Gray and Danielle Citron have suggested a “technology-centered approach” to determine which types of surveillance count as a Fourth Amendment search.³¹⁵ The proposed test—which arguably influenced the majority in *Carpenter*—would mark any surveillance technology a search if it “has the capacity to facilitate broad programs of indiscriminate surveillance that raise the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of government.”³¹⁶ For smart sensors, the technology-centered approach would classify much of the surveillance architecture as a Fourth Amendment problem.

But answering this threshold question does not resolve how smart cities should address the choices in new technologies. In his book, *The Fourth Amendment in an Age of Surveillance*, Professor Gray undertakes to build out some of this Fourth Amendment scaffolding.³¹⁷ He suggests designing legal constraints around the eight operational stages of big data collection: (1) deployment; (2) data gathering; (3) data aggregation; (4) data storage; (5) data access; (6) data analytics; (7) accessing the results of data analytics; and (8) uses of data analytics.³¹⁸ In his book, Gray applies each stage to a series of technologies, including many which will make an appearance in a smart city. The point is that this type of structured legal and technological analysis at each moment of data collection can be accomplished. In the same way computer science engineers must make decisions about possible outcomes based on possible inputs, challenges, and changes, so must the lawyers. Step by step, collection point by collection point, the moments of data collection can be regulated at the outset.

*D. DIGITAL PRIVACY RIGHTS: FOURTH AMENDMENT EXPECTATIONS
THROUGH COMPUTER CODE*

In addition to legal code, one can also create expectations of privacy through computer code. Privacy experts and scholars have expended considerable thought to creating privacy frameworks under the concept of

315. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 101–03 (2013).

316. *Id.* at 101. See generally Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (providing, arguably, the intellectual framework for the majority’s test in *Carpenter*).

317. DAVID GRAY, *THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE* 267–74 (2017).

318. *Id.*

“Privacy by Design” and other related frameworks.³¹⁹ The idea, in brief, is that privacy principles can be embedded in technology to restrict the flow of personal information.³²⁰ Intentionally designing the technology to default toward privacy, anonymize data, and restrict access can strengthen overall privacy.³²¹

As an example of how Privacy by Design might work with smart sensors, take the innovation of smart meters which collect energy readings from homes. As discussed earlier in the Seventh Circuit case involving energy meters as proof of criminal activity,³²² these types of data collection systems can reveal incriminating evidence from the home. In a “Privacy by Design”-influenced city, however, a smart energy grid can be engineered to not collect any personally-identifying information. In fact, in a white paper entitled *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study*, Dr. Cavoukian and her team demonstrate how the different data sources can be siloed and anonymized so as not to reveal personal information.³²³ Essentially, the researchers offer a technical privacy fix to a complex but common city problem.

More specifically, in Ontario, the key was to organize information flows in separate “domains” with personal privacy protection around each domain. In this context, a domain is a separate data circuit that is not connected to others. In the Ontario smart grid example, designers suggest a domain around the home so individual customers can control the information shared about smart appliances and other energy use.³²⁴ The goal is to remove all

319. See generally CAVOUKIAN, FOUNDATIONAL PRINCIPLES, *supra* note 280 (explaining seven principles of information management); ANN CAVOUKIAN, INFO. & PRIV. COMM’R OF ONT., OPERATIONALIZING *PRIVACY BY DESIGN*: A GUIDE TO IMPLEMENTING STRONG PRIVACY PRACTICES (Dec. 2012) [hereinafter CAVOUKIAN, IMPLEMENTATION GUIDE], <https://collections.ola.org/mon/26012/320221.pdf> [<https://perma.cc/F7AR-7MNJ>] (discussing how to implement information management principles).

320. See sources cited *supra* note 319.

321. This theory was the stated governing policy in Quayside in part because Dr. Ann Cavoukian both created the theory and was asked to be an initial advisor to Quayside. After her initial support, Dr. Cavoukian resigned from the Quayside project over concerns that the government and private entities involved were not committed to Privacy by Design principles. ‘Not Good Enough’: *Toronto Privacy Expert Resigns from Sidewalk Labs over Data Concerns*, CBC NEWS (Oct. 21, 2018, 4:49 PM), <https://www.cbc.ca/news/canada/toronto/ann-cavoukian-sidewalk-data-privacy-1.4872223> [<https://perma.cc/ES7J-X2Q4>].

322. *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 523 (7th Cir. 2018).

323. See generally INFO. & PRIV. COMM’R OF ONT., OPERATIONALIZING *PRIVACY BY DESIGN*: THE ONTARIO SMART GRID CASE STUDY (Feb. 2011) [hereinafter INFO. & PRIV. COMM’R OF ONT., CASE STUDY], <http://www.ontla.on.ca/library/repository/mon/25002/307374.pdf> [<https://perma.cc/465W-MEZV>] (describing the privacy plans to keep electricity data protected in Ontario by limiting access through siloed circuits); CAVOUKIAN & POLONETSKY, THIRD PARTY ACCESS, *supra* note 47 (discussing third-party aggregation of customer energy information and related privacy issues); INFO. & PRIV. COMM’R OF ONT., GOLD STANDARD, *supra* note 47 (discussing the development of Ontario’s Smart Grid and related privacy issues).

324. INFO. & PRIV. COMM’R OF ONT., CASE STUDY, *supra* note 323, at 7.

personally-identifying information on the home devices, separating out this first domain from any services that the electrical company might offer.³²⁵ They suggest a second, separate domain for services which would include customer data for billing purposes, in which particularized information about a home would be kept, but also aggregated with other home data retaining a measure of customer anonymity.³²⁶ Finally, engineers suggest a third domain for the larger grid to monitor the large-scale use of electricity across a jurisdiction.³²⁷ This grid domain will not have any connection with the other two. The three domains are separate and the consumer data in one cannot be linked to the others, offering some measure of privacy about individual home electricity use.³²⁸ This type of purposeful privacy protective action can be embedded in all sorts of smart city technology—so long as data privacy is emphasized at the beginning.³²⁹

Professor Woodrow Hartzog has gone one step further to sketch out the blueprints for smart technologies designed for privacy. In his book *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Hartzog offers suggestions on how to design technologies conscious of the legal and regulatory frameworks in which they exist.³³⁰ His argument is that by consciously focusing on design—how we interact and connect with new technologies—we can change conceptions of privacy, trust, and develop legal rules to protect that privacy or obscurity that we need for a functioning democracy.³³¹ Professor Hartzog's argument is that design choices (interfaces, buttons, prompts) can directly control use and thus expectations of privacy.³³² If we imagine smart sensors in a smart city as merely a collection of such technologies, then how we design the human interface will have a direct consequence on privacy. Professor Hartzog demonstrates how every infringement by technology is really a design problem, and that the key to shaping privacy is to think through those design issues at the front end of creation.³³³

For Fourth Amendment purposes, this type of intentional design focus is not only protective of data privacy, but helps establish reasonable expectations of privacy. If the question is whether an individual has a reasonable

325. *Id.* at 8.

326. *Id.* at 7–9.

327. *Id.* at 7, 10.

328. *Id.* at 11.

329. See Hiller & Blanke, *supra* note 9, at 336–37.

330. WOODROW HARTZOG, *PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 7, 157–93 (2018).

331. *Id.*

332. *Id.*

333. *Id.* Though beyond the scope of this Article, Professor Hartzog tackles some of the smart technologies that will make their way into a smart city and offers suggestions for redesign with an eye toward privacy. *Id.*

expectation of privacy in their smart home connected to a smart grid, the design principles embedded in the code or the grid may suggest the answer. Thus, even if the police somehow circumvent the privacy controls (via the home or electrical company), the law—as established by the computer coded norms—would govern the expectation of privacy analysis. A judge does not have to guess about reasonable societal expectations because the default computer code sets the rule. Acquisition of smart grid data that runs into a Privacy by Design default or automatic deletion of data rule or intentional silo would be a Fourth Amendment issue. In other words, the existing privacy protections programmed into the technology will influence the legal analysis. Whether we are talking about electricity, trash, cars, or other smart devices, design can change constitutional protections—so long as it is built with privacy in mind.

E. DESIGNING THE “LEGAL LAYER”

A truly smart city will require a “legal layer” to be built on top of the digital layer already built into the physical infrastructure. This legal layer can be envisioned as a legal blueprint that maps directly onto the digital layer, node for node, sensor by sensor. Every sensor node of digital collection will have a legal judgment about the use, access, retention, expectations, and security of data to go along with it. This legal layer will address Fourth Amendment privacy and security protections, but also embrace other statutory or regulatory protections (including those that encapsulate rules regarding use of health data, personal data, financial data, etc.). This legal layer will be reflected in the technological design and protected by code. And just as a team of engineers will design the smart city for optimal performance, a team of lawyers will design smart laws within Fourth Amendment constraints. Building off the theoretical and practical insights of scholars, civil rights advocates, and engineers, this legal layer will embed a proactive approach to digital management of personal information.³³⁴

The imagination that has spurred smart cities’ design can extend to alter the legal landscape. If technology innovators—with the vision to reimagine a city’s built environment—are also invested in developing legal, ethical, and technological rules to protect privacy at the outset, many of the Fourth Amendment problems could be minimized. New visions of how to rethink privacy and security protections through a legal layer are possible and could help re-engineer the future of the Fourth Amendment. The goal, however, must be to design the city structure and legal structures wisely in parallel with the digital layer. The challenge for the future is to bring together legal

334. Building a smart city without a legal layer is a design flaw that not only will raise Fourth Amendment concerns (if the arguments in this paper are convincing), but will raise a whole host of avoidable problems. A legal layer will be the only way to proactively respond to criticisms that a smart city is really just a city of surveillance or data capitalism or both.

scholars, technologists, ethicists, companies, and impacted communities to start designing the legal layer before the municipal blueprints are finalized.

VII. CONCLUSION

This Article attempts to initiate a conversation about the Fourth Amendment's future, using smart sensor infrastructure as a heuristic for the very real technological change coming. The Article offers a warning and a path forward, but the real work—as with any good innovation—will be in the design process. Law, code, and design principles must be created with a vision of the type of privacy, security, and autonomy citizens will want in a smart city. These decisions will not only shape the physical architecture of where we walk, work, and play, but will shape the architecture of privacy for all those who live in and interact with a smart city. Such decisions will also shape the constitutional law in that city, as judges will use these early technological choices to shape a digital positive law responsive to Fourth Amendment principles and values.