Digital Architectures of 'Smart' Cities and the Fourth Amendment: A Response to Andrew Ferguson

Steven I. Friedland[*]

ABSTRACT: The constant flow of advances in digital technology have led almost inexorably to the development of digitally run or "smart" cities. Professor Andrew Ferguson suggests that urban designers should intentionally minimize Fourth Amendment entanglements and violations when planning such smart places. This response amplifies what Professor Ferguson offers, points out a few gaps, and offers some additional ideas.

I. INTRODUCTION 177

II. LEGAL BACKGROUND 179
A. *THE PRE-DIGITAL AGE* 179
1. *Katz v. United States* 179
2. The Third-Party Rule 180
3. The Supreme Court Trilogy 180
4. *Carpenter* 181
5. Where *Jones*, *Riley*, and *Carpenter* Leave Off 181
B. *THE DIGITAL AGE* 182

III. ANALYSIS OF 'SMART SENSORVEILLANCE' 183
A. *AMPLIFYING PROFESSOR FERGUSON* 183
1. Does the Fourth Amendment Really Apply to Smart Cities? 183
2. Sensors Matter 185
3. Digital Urban Design Likely Will Create a Variety of Entanglements with the Fourth Amendment Going Forward 185

* The author is a Senior Scholar and Professor of Law at Elon University School of Law. He is an honors graduate of Harvard Law School and holds LL.M. and J.S.D. degrees from Columbia University, where he was a Dollard Fellow.

B. *MINDING THE GAPS* 186
1. The Human Brain and Bias 187
2. Loose Ends: Legal and Policy Variables 188
i. *The Indeterminacy of* Katz*, the Third-Party Rule, and Fourth Amendment Doctrine* 188
ii. *A Higher Level of Scrutiny?* 188
iii. *New Technologies, Justices, and Interpretations* 189
iv. *The Workability of the Third-Party Rule—When a Wall Starts Crumbling Down* 190
v. *Policy Variables* 191
vi. *The Driver of Expediency* 191
C. *WHERE DOES THIS LEAVE US? SOME SUGGESTIONS* 193
1. Digital Architecture: Firewalls 193
2. Reimagine "Search" Categories 193
3. Pragmatism Over Constitutionalism 194
4. Is Positive Law the Answer? 194
5. Do Not Forget the Forgotten Third Amendment 195

IV. CONCLUSION 196

I. INTRODUCTION

In *Structural Sensor Surveillance*[1] Professor Andrew Ferguson provides an astute—some might say smart—lens for viewing urban planning from a Fourth Amendment digital perspective. This Response to Professor Ferguson's article does three things. First, it amplifies some of his observations and conclusions.[2] Second, this Response fills in some gaps and critiques some of the article's assumptions.[3] Third, it offers a few suggestions of its own.[4]

"Smart"[5] means many things in the current lexicon. Within the realm of Fourth Amendment, it means something that is part of a digital network producing a stream of data. The common use of the word "smart" in this context indicates that there will be valuable—perhaps even monetized —information produced by the networks that multiple entities might want to or in fact access. These networks have sensors linked to each other to

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

2. One agreement lies in his effort to analyze the interface between smart cities and the Fourth Amendment.

3. Gaps and critiques include the incomplete and anachronistic Fourth Amendment doctrine, the unknowable nature of technological advances, the implicit bias within all of us that distorts rational planning, and policy variables that will impact city structure.

4. Suggestions range from bolstering firewalls, to redesigning the Fourth Amendment doctrine, not just projecting it based on existing caselaw, and adding the Third Amendment to the mix.

5. The word "smart" in the Webster's Dictionary means "having or showing a high degree of mental ability." *Smart* Merriam-Webster, https://www.merriam-webster.com/dictionary/smart [https://perma.cc/27HN-SU6W].

effectively create massive surveillance systems. The networks associated with these goods, from connected doorbells to thermostats to digital assistants, create what is commonly referred to as the Internet of Things ("IoT").[6] Unlike with physical surveillance, transaction costs are low. While these surveillance systems often are initiated by consumers who enjoy the conveniences of the IoT or businesses that utilize the information highway for profit or efficiency, the IoT also involves systems deployed or accessed by government entities.

While governmental use of smart sensor structural design in cities can greatly assist cities, it also poses a threat through the mass-surveillance systems it creates. Professor Ferguson has termed this byproduct of smart sensors "sensorveillance,"[7] showing that the surveilling sensors have a potential windfall of information for crime investigators and a diminishment of privacy. He notes:

> 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. They can seek to understand points of environmental vulnerability, victims most at risk, and patterns of crime. They can seek to understand crime data in terms of geography, time, people, and patterns, and visualize it across the days, weeks, or years. Using smart sensor technologies, police will possess a powerful investigative "time machine."[8]

Professor Ferguson's article explains how the structural design of "smart" cities embedded with tens of thousands of sensors on communications networks could minimize violations of the Fourth Amendment:

> 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 . . . .[9]

While the crux of Professor Ferguson's inquiry lies in the government use of sensor-derived information, sensorveillance is not simply a product of intentional malevolent snooping by the government.[10] It is much broader, often initiated by large online companies, such as Google and Amazon, and the consumers that voluntarily offer their information to the companies. The consumers often don't anticipate, however, how their information is used. As one commentator observed: "Though the intended consequence of smart city

6. *See* Ferguson, *supra* note 1, at 53–54, 63, 69.

7. *Id.* at 50.

8. *Id.* at 51 (footnotes omitted).

9. *Id.*

10. *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 628–29 (2017).

technology may be efficiency, the unintended consequence may be surveillance."[11] The fact that snooping occurs without scienter does not make it any less snooping or an invasion of privacy.

Yet, Professor Ferguson argues that no matter how mass data is derived, the intentionality of digital design in cities matters: "Depending on how the sensors are configured, these city environments can either create a Fourth Amendment search problem or avoid one."[12] With this one sentence, he reveals the scope of his intentions—combining complex legal analysis with urban planning. In essence, it is not only avoidance of Fourth Amendment violations that he is advocating, but a much more ambitious policy-based utilitarian model that would result from Fourth Amendment tailoring. He asserts that this would be beneficial for democracy overall by promoting citizen engagement.[13]

This Response largely agrees with Professor Ferguson's embrace of forward planning—instead of just a retrospective about a decided case—and his creation of potential standards for a greater utilitarian process and better city infrastructures. Yet, as city subway riders are warned, he needs to mind the gap(s) in his projections, ranging from ransomware attacks to implicit bias. Further, he might possibly consider some additions, doubling-down on firewalls and adding in the Third Amendment as a potential reinforcing bulwark.

This Response has a compact structure. Part II is a short background section framing the applicable Fourth Amendment law and directly follows this Introduction. Part III explains in greater detail this Response's alignment with Professor Ferguson, the gap(s) to be minded, and some suggestions. The Response then ends with the expected conclusion in Part IV.

II. LEGAL BACKGROUND

A. THE PRE-DIGITAL AGE

1. *Katz v. United States*

The seminal case in Fourth Amendment search analysis is *Katz v. United States*,[14] occurring coincidentally in a telephone booth, a relic of pre-digital times. The case described a search triggering the Fourth Amendment as an invasion of privacy, which Justice Harlan's concurrence defined as a two-prong test—requiring an examination of both the subjective and societal (objective) expectation of privacy to determine if a search has occurred.[15] Even if there was a search, the case directs courts to a second question: whether the search was reasonable—and thus constitutional—under the

11. Jan Whittington, *Remembering the Public in the Race to Become Smart Cities*, 85 UMKC L. REV. 925, 927 (2017).

12. Ferguson, *supra* note 1, at 51.

13. *Id.* at 51–52.

14. Katz v. United States, 389 U.S. 347 (1967).

15. *Id.* at 361 (Harlan, J., concurring).

Fourth Amendment. This test has survived for more than fifty years and, while heavily criticized,[16] persists.

2. The Third-Party Rule

The progeny of *Katz*[17] are numerous and concern a wide array of applications. Perhaps the most significant involve private information being divulged by a person or private entity to third parties. The so-called Third-Party Rule is perhaps the most impactful vestige of the pre-digital era. In cases such as *Smith v. Maryland*[18] and *United States v. Miller*,[19] the Supreme Court held that information voluntarily disclosed to a third party no longer retains any reasonable expectation of privacy. This doctrine had a huge impact on Fourth Amendment analysis when it came to interpreting the scope of the Fourth Amendment.

Many commentators believe the Supreme Court's interpretation of the Fourth Amendment, dating back 50 years into the last century, is outdated.[20] As noted above, *Katz* occurred in the context of a phone booth. Most young Americans have never used a phone booth, and might not know how to use one if given the opportunity.

3. The Supreme Court Trilogy

The trilogy of *United States v. Jones*,[21] *Riley v. California*,[22] and *Carpenter v. United States*[23] essentially comprise the leading cases setting the parameters of Fourth Amendment doctrine in the digital age. As Professor Ferguson recognizes, it is important to try to synthesize the trilogy of digital era cases.[24] In *Jones*, a majority of the justices found that 28 days of continuous GPS surveillance of a car on public streets constituted a search under the Fourth Amendment test of reasonable expectation of privacy.[25] In *Riley*, the Court concluded that a search incident to a lawful arrest did not include a search of a cellphone, which was qualitatively different than searches of other physical containers.[26] *Carpenter* adds a significant piece of the puzzle. *Carpenter* involved both cell phones and cars. Carpenter was tracked by cell phone after

16. *See generally* Timothy Casey, *Electronic Surveillance and the Right to be Secure*, 41 U.C. DAVIS L. REV. 977 (2008) (arguing that the application of *Katz* has led to anomalous results, especially in the electronic surveillance context).

17. *See, e.g.*, California v. Ciraolo, 476 U.S. 207 (1986); Kyllo v. United States, 533 U.S. 27 (2001).

18. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

19. United States v. Miller, 425 U.S. 435, 445–47 (1976).

20. *See generally* Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946 (2016) (arguing that previous cases have not afforded personal property enough protection in certain instances).

21. United States v. Jones, 565 U.S. 400 (2012).

22. Riley v. California, 573 U.S. 373 (2014).

23. Carpenter v. United States, 138 S. Ct. 2206 (2018).

24. *See* Ferguson, *supra* note 1, at 74–75.

25. *Jones*, 565 U.S. at 403–05.

26. *Riley*, 573 U.S. at 393–98, 401.

government agents received seven days of cell-site location data from Carpenter's phone company.[27] The data showed where Carpenter was located when a series of robberies had occurred.[28] The Supreme Court held that the government collection of this information invaded Carpenter's reasonable expectation of privacy and constituted a search.[29]

4. *Carpenter*

Carpenter, in particular, provided some additional answers about what constitutes a search under the Fourth Amendment—and then raised more questions. There were differing understandings of how it augmented the doctrinal analysis. As Professor Ferguson noted, a key advance of *Carpenter* was to allow a motion to suppress evidence under the Fourth Amendment when "the Government employs its own surveillance technology . . . *or leverages the technology* of a [private company]."[30]

If accurate, this reading of *Carpenter* suggests doubts about the continued viability of the Third-Party Rule and indicates that by acquiring the records of a private company the government may well be routinely "searching" the records without a warrant. But it does not put to rest what exactly *Carpenter* means. That remains an open question, as the Court takes one bite of the apple at a time, resisting the opportunity to offer sweeping rules.

5. Where *Jones*, *Riley*, and *Carpenter* Leave Off

Professor Ferguson offers his own five-point continuum about how to generalize the holdings of the Supreme Court cases in the digital era, particularly *Jones*, *Riley*, and *Carpenter*, into a coherent structure for future use. He states that "[a]long 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."[31]

Thus, it is not enough to simply look at whether there is massive systematic surveillance in the information marketplace, but it is important to more carefully sift through the salient features of that surveillance. When it comes to use of surveillance data in criminal cases, Ferguson notes: "At least when data is used against defendants in criminal cases, the more centralized a system of sensor data collection, the more Fourth Amendment issues arise."[32]

---

27. *Carpenter*, 138 S. Ct. at 2212.

28. *Id.* at 2212–13.

29. *Id.* at 2217.

30. *Id.* (emphasis added). Justice Alito stated in his dissent, "the Court effectively allows Carpenter to object to the 'search' of a third party's property, not recognizing the revolutionary nature of this change." *Id.* at 2260 (Alito, J., dissenting).

31. Ferguson, *supra* note 1, at 79.

32. *Id.* (footnote omitted).

B. THE DIGITAL AGE

The digital age really has facilitated surveillance—massive self-surveillance by individuals, by private entities for commercial gain, and by the government. Private entities often have led the charge in creating massive perpetual surveillance systems, often to promote their profit margins. This includes those systems that were created only as a byproduct of new technology directed at other areas.

The Internet of Things, in particular, has created an explosion of sensor-based networks by private as well as public entities. These sensors, numbering in the billions, do not often have many protections from hackers and instead are vulnerable to attack. While the conveniences provided are significant, from smart doorbells, lights, cars, clothing, and just about any other thing that can be imagined, there are significant costs—especially hacking—that are becoming more and more apparent.

Several examples illustrate these claims. The company Intrado, for example, manufactures proprietary commercial software called "Beware." The software assigns "threat scores" to local residents[33] after gathering information from the IoT, social media, and more. The company's website stated that its web-search algorithm "scan[s] massive amounts of commercial data and presents it as actionable intelligence, complete with threat scores in an easy-to-read headline format—all within seconds of an initial query."[34] After sorting billions of data points in seconds,[35] the software assigns a color to an individual—green, yellow, or red, in ascending order of threat.[36] The tool has been used by police departments when responding to calls.[37]

Another example of propensity-based tracking involves the largest U.S. supplier of outdoor billboards, Clear Channel Outdoor.[38] The company created "smart billboards," based on a program named Radar.[39] This program allowed the billboards to track the cell phones possessed by any drivers and their passengers in the vicinity of the billboards. With that information, the company was able to then follow up at a later time to determine whether any of the individuals had accessed the website of the company whose ad the

33. Alicia Marie Tan, *A California Police Department Decides How Dangerous You Are Using This Software*, MASHABLE (Jan. 15, 2016), http://mashable.com/2016/01/15/fresno-police-beware/#VqU4VPo_jZqb [https://perma.cc/Z4RL-SWPD].

34. *Id.*

35. *Id.*

36. *See* Ms. Smith, *Beware: Surveillance Software Police are Using to Score Citizens' Threat Level*, CSO (Jan. 11, 2016, 10:37 AM), https://www.csoonline.com/article/3020669/beware-surveillance-software-police-are-using-to-score-citizens-threat-level.html [https://perma.cc/3TDX-82GL].

37. *Id.*

38. CLEAR CHANNEL OUTDOOR, http://clearchanneloutdoor.com [https://perma.cc/HT99-4YYS].

39. *See, e.g.*, *Clear Channel Outdoor Americas Launches 'RADAR' – New Data Analytics Solution for Marketers to Plan and Buy Out-of-Home Media and Measure Target Audience Segment Outcomes*, BUS. WIRE (Feb. 29, 2016, 7:50 AM), https://www.businesswire.com/news/home/20160229005959/en/Clear-Channel-Outdoor-Americas-Launches-%E2%80%99RADAR%E2%80%99 [https://perma.cc/5NBJ-TW4S].

billboard was advertising.[40] While this is not the same as what was described in the film *Minority Report*[41]—in which a small poster ad specifically targeted the protagonist, John Anderton, to sell him a particular type of beverage—it certainly creates a new type of performance tracking that governments would be glad to possess.

"Smart" athletic apparel provides another illustration of how the IoT and networks with sensors can further shapeshift accepted notions of privacy.[42] Several college sports departments have entered deals with apparel companies for millions of dollars[43] that in part provide players with smart apparel—clothing containing tiny radio sensors that can collect and transmit reams of biometric data related to such things as speed, distance, vertical leap, height, maximum time aloft, shot attempts, length of ball possession, heart rate, and running routes.[44]

Finally, in July of 2021 it was reported that new spyware named Pegasus has been sold by a cyber-surveillance company, NSO Group, to governments around the world.[45] This software has been reportedly used by authoritarian regimes to target journalists, dissidents, and opposition politicians.[46]

III. ANALYSIS OF 'SMART SENSORVEILLANCE'

This Part does several things: (1) amplifies several arguments made by Professor Ferguson; (2) adds a few pieces to the puzzle he presents; (3) and makes some suggestions.

A. AMPLIFYING PROFESSOR FERGUSON

1. Does the Fourth Amendment Really Apply to Smart Cities?

This Section will start amplifying some of Professor Ferguson's major points by first examining his decision to look at the Fourth Amendment

---

40. *Id.*

41. MINORITY REPORT (Twentieth Century Fox 2002).

42. It is not just a new dimension in colleges. Major League Baseball, for example, approved wearable technology even during games in 2016. Mike Vorkunov, *Innovation vs. Invasion of Privacy: MLB Wearable Technology Battle Looms*, USA TODAY (Sept. 22, 2016, 12:48 AM), http://www.usatoday.com/story/sports/mlb/2016/09/21/innovation-vs-invasion-privacy-mlb-wearable-technology-battle-looms/90783188 [https://perma.cc/9CLF-JE28]. Players can wear the Zephyr Bioharness to track their breathing and heart rate, as well as the Motus Sleeve, which has a chip in it that tracks arm angles and the forces placed on the ligaments in the elbow from throwing. *Id.*

43. *See, e.g.*, *U-M Launches Exercise and Sport Science Initiative*, MICHIGAN NEWS (Sept. 29, 2016), http://ns.umich.edu/new/releases/24230-u-m-launches-exercise-and-sport-scienceinitiative [https://perma.cc/C84C-MECQ]; Marc Tracy, *With Wearable Tech Deals, New Player Data Is Up for Grabs*, NY TIMES (Sept. 9, 2016), https://www.nytimes.com/2016/09/11/sports/ncaafootball/wearable-technology-nike-privacy-college-football.html?_r=0 [https://perma.cc/355L-AKDF].

44. *See* Tracy, *supra* note 43.

45. Ronen Bergman & Patrick Kingsley, *Israeli Spyware Maker is in Spotlight Amid Reports of Wide Abuses*, N.Y. TIMES (Sept. 29, 2021), https://www.nytimes.com/2021/07/18/world/middleeast/israel-nso-pegasus-spyware.html [https://perma.cc/9GMC-2QUQ].

46. *Id.*

digitally and systemically in the context of city planning, utilizing the trilogy of major Supreme Court cases on digital search issues—*United States*,[47] *Riley*,[48] and *Carpenter*.[49] His analysis of "smart" surveillance arising from a digital layer of cognizable architectural design offers an appealing and thought-provoking approach to navigating the Fourth Amendment crucible of the future, particularly as that Amendment emerges from phone booths and enters the world of wireless networks. At a minimum it is important to evaluate the use of "smart" things in all contexts—including cities—against a Fourth Amendment backdrop. Professor Ferguson's article explores what these sensors built into city structures[50] mean to the still-modernizing Fourth Amendment. Significantly, the idea of digital construction fits naturally within the context of an urban planning environment. Professor Ferguson's emphasis recognizes the centrality of the transformation from physical to digital structuring in the world generally.

Professor Ferguson provides broad support for concluding that the Fourth Amendment applies to smart cities as well as other entities. He shows how viewing things from a systemic perspective is very helpful in an age of systems. Otherwise, piecemeal development—of the Fourth Amendment doctrine or cities—can lose its purpose, cohesiveness, and operability.

He further notes: "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."[51] Thus, the Fourth Amendment applies not just to individual police officers, but to cities and any other public entities that feed the investigative, crime prevention, and law enforcement arms of government. The choice of digital architectures thus can make a significant difference in whether the Fourth Amendment is violated.[52] Choices will involve how "localized, networked, aggregated and/or centralized" data will be.[53] He is likely correct in believing that "[w]ithout the long-term, aggregated nature of collection and acquisition, maybe much of the smart city falls outside of the Fourth Amendment's reach."[54] The same conclusion applies to

47. United States v. Jones, 565 U.S. 400 (2012).

48. Riley v. California, 573 U.S. 373 (2014).

49. Carpenter v. United States, 138 S. Ct. 2206 (2018).

50. Ferguson writes, "[t]raditional 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. 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." Ferguson, *supra* note 1, at 55 (footnote omitted).

51. *Id.* at 80 n.168.

52. Ferguson notes that cities cannot just run around the Fourth Amendment by lowering privacy expectations: "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." *Id.* at 88.

53. *Id.* at 79. "Simple sensors, if designed to remain simple, localized, and limited, might well remain outside of core Fourth Amendment concerns." *Id.* at 86.

54. *Id.* at 90. "Of course, the streetlights could be linked in a network of other streetlights, and energy data could be aggregated. But a lack of identifying information and tracking capabilities could also remove it from Fourth Amendment scrutiny." *Id.* at 86 (footnote omitted).

any sensors that are intentionally designed to limit data collection and retention.

2. Sensors Matter

Professor Ferguson understands the far-reaching power of these tiny network sensors. The sensors in networks create information pathways that aggregate the information, create value, and eventually naturally erode privacy. With the advances in local networks, the smart home already has become an incredibly revealing source of intimate data to both public and private groups. First, government entities like public utilities might directly and intentionally collect information from a private house. For example, electrical and water use from a smart home meter might be a direct government collection.[55] Second, private companies will offer residents of smart homes a plethora of sensor-connected conveniences, from smart thermostats to coffee makers, beds, and toothbrushes.[56] In addition, electronic assistants, such as Amazon Echo, Google Home, Nest, and Facebook's Portal TV offer new levels of convenience at the sound of a voice or touch of a finger.[57]

The data gathered is usually mediated by a private third-party company or companies, adding layers of disclosure.[58] Importantly, the data may reveal many granular details about a person's life that they would not disclose to others—when they shower, have therapy or sex, or deal with physical or emotional issues.

3. Digital Urban Design Likely Will Create a Variety of Entanglements with the Fourth Amendment Going Forward

Professor Ferguson smartly mines an important intersection—urban design and Fourth Amendment concerns. This kind of broad, institutional analysis does not use caselaw as the centerpiece but rather rests on how government can maximize its objectives without running afoul of the Constitution. This offers a very useful perspective, although it risks diverging into a policy debate that distracts from the article's core: which right takes precedence—the right to freedom of action or the right to security?

Identifying entanglements in doctrine and policy is useful in and of itself. This is like a GPS that identifies potential obstacles ahead. It is very important

---

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

56. *See, e.g.*, *Everything You Need to Know About Smart Home Technology*, OTELCO, https://www.otelco.com/resources/smart-home-guide [https://perma.cc/63Z6-95SR].

57. *See, e.g.*, *New Ways Alexa Makes Life Simpler and More Convenient*, AMAZON (Sept. 25, 2019), https://www.aboutamazon.com/news/devices/new-ways-alexa-makes-life-simpler-and-more-convenient [https://perma.cc/E4SW-NR2R].

58. Kaveh Waddell, *The NSA's Bulk Collection Is Over, but Google and Facebook Are Still in the Data Business*, ATLANTIC (June 3, 2015), https://www.theatlantic.com/politics/archive/2015/06/the-nsas-bulk-collection-is-over-but-google-and-facebook-are-still-in-the-data-business/458496 [https://perma.cc/NRP7-RYKQ] ("Private-sector data collection can reveal as much about a person as government surveillance, privacy advocates say.").

from a planning perspective to try to embed the smart technologies with the city structures for maximum benefit.

In addition, while Professor Ferguson tailored city planning to avoid Fourth Amendment violations, he recognizes that city design will not be isolated or occur in a vacuum but in the real world, with competing drivers. He understands that these drivers likely will include expectations of city residents surrounding security, safety, and community. Yet, he correctly points out that these expectations will not undermine the privacy expectations assessed under the Fourth Amendment through doctrines of implied consent or assumption of the risk:

> 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.[59]

This point is worth illuminating; it serves to limit how cities can manipulate resident expectations for Fourth Amendment purposes. It also indicates, though, that showdowns and conflicts are likely to arise regarding a central underlying tension—the right to freedom of action versus the right to security. Just because citizens want security does not mean cities will be allowed to circumvent the Fourth Amendment; the lesson is that the core value of the Fourth Amendment must be met first.

B. MINDING THE GAPS

A few additional pieces of the puzzle—what I have called gaps—should be considered. First, the articulation of Professor Ferguson's plan to tailor city planning to the Fourth Amendment will have predictive flaws. Perhaps the foremost flaw involves any prediction involving the future of Fourth Amendment jurisprudence. One cannot really depend on the incomplete doctrinal foundation provided by the Supreme Court's cautious entry into the digital age. Indeed, Professor Ferguson takes advantage of the deficiency in the Supreme Court's somewhat antiquated and incomplete quasi-digital approach to the Fourth Amendment by adding his own interpretive construct of what a completed constitutional analysis might entail. Ferguson's article adds another brick in the wall showing the Supreme Court is long overdue with a complete digital remodeling of the Fourth Amendment.

Assumptions about the waves of new technology and shifting political and environmental climates also may have a significant impact on future planning. Further, Professor Ferguson should not overlook the varying interests of the actors who have the power to create such architectures—namely politicians and lobbyists. Other pragmatic challenges likely will play a role in the execution of city planning, such as the impacts of disparate city revenues, cybercriminal attacks, and the positive laws of the different city councils.

---

59. Ferguson, *supra* note 1, at 88.

Further, there is the possible application of the forgotten Third Amendment,[60] which dovetails with Fourth Amendment privacy by arguably creating its own privacy realm in the digital age when government "cybersoldiers" are effectively "quartered" in houses even without a physical trespass, gathering significant and intimate information for the purposes of preventing or investigating terrorist actions.

These additional issues raise significant questions. For example, what will the real drivers of a city's digital architecture be? Even if one of the drivers of city planning is avoiding Fourth Amendment quicksand, how well can cities—and their experts—really adapt to what will develop? Professor Ferguson's tough issues are not necessarily unique to his proposals, but rather left for us all—his efforts to carve out a digital design structure in the shadow of an outdated Third-Party Rule, a cautious Supreme Court, notwithstanding *Carpenter*, waves of opportunistic technology, and a variety of crises (e.g., a pandemic) presents a grand guess as to what might happen in the future, not a way to build on a firm foundation. In essence, there is no easy way to get ahead of the Supreme Court in suggesting a Fourth Amendment jurisprudence when its foot-dragging is coupled with the whipsaw of advancing technology.

1. The Human Brain and Bias

Professor Ferguson assumes that "reasonableness" will serve as a yardstick for urban digital design, but it may be less applicable than he believes. The purpose in gathering information in a smart city is generally reasonable, but advances in neuroscience show that the human brain is a pattern seeking device that often acts based on instinct and not critical cognition. These "fast thinking" actions are often wrong and subject to bias. This can be seen with the number of people who believe rumors, conspiracies and Internet posts without verification or proof.[61] Misuse of technology occurs frequently, from people in their electric "auto assist" cars[62] to IRS employees misusing their power to collect information from others.

When people can gather information in the digital age behavioral economics studies have shown that people value gains and losses differently.[63]

---

60. The Third Amendment states that "[n]o Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." U.S. CONST. amend. III.

61. As Mark Twain (or possibly Jonathan Swift) astutely stated, "a lie can travel halfway around the world while the truth is still putting on its shoes." Niraj Chokshi, *That Wasn't Mark Twain: How a Misquotation Is Born*, N.Y. TIMES (Apr. 26, 2017), https://www.nytimes.com/2017/04/26/books/famous-misquotations.html [https://perma.cc/QR8H-V88Q].

62. For example, the Tesla auto-drive software has been abused by drivers on multiple occasions, some with fatal consequences. *See, e.g.*, Bryan Pietsch, *2 Killed In Driverless Tesla Car Crash, Officials Say*, N.Y. TIMES (Sept. 1, 2021), https://www.nytimes.com/2021/04/18/business/tesla-fatal-crash-texas.html [https://perma.cc/PV3L-ZNRQ] ("Mark Herman, the Harris County Precinct 4 constable, said that physical evidence from the scene and interviews with witnesses led officials 'to believe no one was driving the vehicle at the time of the crash.'").

63. *See* Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk*, 47 Econometrica 263, 279 (1979) (describing how people make decisions based on the potential

Kahneman and Tversky found that people value gains more than losses in their Prospect Theory.[64] Thus, there likely are financial and perhaps other incentives to keep gathering information regardless of potential future Fourth Amendment implications because studies show people are more motivated by expediency in the present than potential benefits in the future.[65] Potential loss of evidence may not be significant enough to deter cities under utilitarian analysis. That is, the exclusionary rule may just not be a strong enough deterrent. Thus, reason can be a smokescreen for bias.[66] This bias extends to Supreme Court decisions as well and is often a product of the unconscious brain.[67]

2. Loose Ends: Legal and Policy Variables

While the article offers a snapshot of some of the legal and technological variables that will confront urban planners, the number and variety of those variables will weigh heavily on any proposed route in the future.

i. The Indeterminacy of Katz*, the Third-Party Rule, and Fourth Amendment Doctrine*

We still don't know what the Fourth Amendment means for future technologies and applications. The trilogy of *Jones*, *Riley*, and *Carpenter* are an unfinished work in progress. What results is a slippery standard that will also be driven by technology, environment, and culture, not just the courts.

Why spend millions of dollars speculating what might be in urban architecture when it might not come to pass? It is especially difficult to declare that the Supreme Court's Fourth Amendment doctrine has a wholeness or internal consistency when it still revolves around a case involving a phone booth, *Katz v. United States*. The Fourth Amendment instead faces numerous interfaces without as many common doctrinal threads.

ii. A Higher Level of Scrutiny?

In a way, the *Riley*, *Jones*, and *Carpenter* trilogy has created a form of stricter scrutiny for the courts, pouring a type of Equal Protection analysis[68] into the

---

value of losses and gains rather than the final outcome). People have biases relating to certainty, loss aversion, and isolated data.

64. *Id.* at 263. Prospect Theory refers to Kahneman and Tversky's proposed alternative to utility theory, in response to their "critique of expected utility theory as a descriptive model of decision making under risk." *Id.*

65. *Id.*

66. *See generally* Sherri Lee Keene, *Stories That Swim Upstream: Uncovering the Influence of Stereotypes and Stock Stories in Fourth Amendment Reasonable Suspicion Analysis*, 76 MD. L. REV. 747 (2017) (discussing in part *Whren v. United States*, where the Supreme Court stated that as long as there was a legitimate reason to stop individuals under the Fourth Amendment, the existence of another and likely pretextual stop would not nullify the legitimacy of the stop).

67. *Id.* at 751–53.

68. The Supreme Court's Equal Protection analysis usually classifies governmental line-drawing into categories, which then are accorded different levels of scrutiny. Three primary levels of scrutiny include strict, intermediate, and rational basis. While rational basis scrutiny generally presumes the government action is valid, the other two tiers do not attach such a presumption

Fourth Amendment. While the Court has resisted using similar terminology or crafting differing levels of analysis for digital matters, it seems that the existence of a search has become more of a continuum of factors creating a closer level of scrutiny as more factors appear and a tipping point (but not a bright line) for a finding of unconstitutionality. For example, 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*.[69] Thus, information about what occurs in the home is still a very important factor in the search analysis and might provide better guidance on what is permitted in the future.

iii. New Technologies, Justices, and Interpretations

Further, new technologies will mean new court cases. For example, the world of face recognition software is gaining in use, by businesses and police departments, and is changing rapidly. The Los Angeles Police Department has admitted using such technology almost 30,000 times in the past decade.[70] Yet, there have been many attacks on the accuracy and reliability of face recognition theory and application, in particular that it is biased in the way it works.[71] The Clearview AI company has compiled more than three billion photos for its database and is offering its services to police departments[72] among other organizations.[73] Courts likely will face many challenges to this technology in the future.

Also, new justices mean new approaches. As the Supreme Court changes, so too will its Fourth Amendment doctrinal path. This is particularly true as aging justices leave the court, replaced by justices from different generations, particularly those who are comfortable with and understand at least some of how the digital world works.

---

and are more difficult to meet. *See* RUSSELL L. WEAVER, STEVEN I. FRIEDLAND & RICHARD D. ROSEN, CONSTITUTIONAL LAW: CASES, MATERIALS AND PROBLEMS 886 (5th ed. 2021).

69. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 525–27 (7th Cir. 2018).

70. *See* Kevin Rector & Richard Winton, *Despite Past Denials, LAPD Has Used Facial Recognition Software 30,000 Times in Last Decade, Records Show*, L.A. TIMES (Sept. 21, 2020, 12:43 PM), https://www.latimes.com/california/story/2020-09-21/lapd-controversial-facial-recognition-software [https://perma.cc/RTY3-Q8S4]. The common usage allegedly helps officers solve crimes more quickly. *Id.*

71. *See, e.g.*, Karen Hao, *A US Government Study Confirms Most Face Recognition Systems Are Racist*, MIT TECH. REV. (Dec. 20, 2019), https://www.technologyreview.com/2019/12/20/79/ai-face-recognition-racist-us-government-nist-study [https://perma.cc/GH8H-95FS] ("For one-to-one matching, most systems had a higher rate of false positive matches for Asian and African-American faces over Caucasian faces, sometimes by a factor of 10 or even 100. In other words, they were more likely to find a match when there wasn't one.").

72. The NY Police Department has used Clearview AI in its crime interdiction efforts. *See* Tate Ryan-Mosley, *The NYPD Used a Controversial Facial Recognition Tool. Here's What You Need to Know*, MIT TECH. REV. (Apr. 9, 2021), https://www.technologyreview.com/2021/04/09/1022240/clearview-ai-nypd-emails [https://perma.cc/33JD-F4M3].

73. "Clearview AI has been heavily criticized for its use of personally identifiable information, its decision to violate people's privacy by scraping photographs from the internet without their permission, and its choice of clientele." *Id.*

And there will always be commentators who try to divine what the Fourth Amendment really means and provide their own structural vision of how to apply the cases, muddying the waters for urban planners with competing experts. The use of different canons of construction can be seen in recent cases, such as *Carpenter*.[74] As one commentator noted:

> Professor Paul Ohm suggests that a three-factor test emerges from the majority opinion. When the government seeks to access large, private databases containing nonpublic information about individuals, judges should ask whether the information (1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection.
>
> [On the other hand,] Professor Orin Kerr identifies three different requirements needed to trigger Fourth Amendment protections for records that contain metadata like location information rather than content: (1) the records exist because of digital age surveillance methods; (2) they are not the product of a user's meaningful voluntary choice because they are necessarily created when a person uses core digital age technologies; and (3) they tend to reveal the privacies of life beyond the legitimate interests of criminal investigations.
>
> [Further,] Professors Susan Freiwald and Stephen Wm. Smith, the latter a former magistrate judge, distinguish five factors as central to the Court's inquiry: whether the surveillance technique was (1) hidden, (2) continuous, (3) indiscriminate, and (4) intrusive, along with (5) the expense and effort required to compile the data.[75]

iv. The Workability of the Third-Party Rule—When a Wall Starts Crumbling Down

As the Third-Party Rule reveals its inability to offer a reasonable analysis in the digital world, it faces even more pressure in future Supreme Court cases.[76] Will the long-standing rule be the approach in the future until it is finally totally discredited or discarded? Or will it soon be abandoned, and a new rule created? These questions are extremely important for any planning infrastructure given the centrality of the Third-Party Rule to current constitutional privacy. If the Court creates new limits and further erodes or trashes the rule, what will that mean for information collection? Also, much

---

74. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

75. LAURA HECHT-FELELLA, BRENNAN CTR. FOR JUST., THE FOURTH AMENDMENT IN THE DIGITAL AGE: HOW *CARPENTER* CAN SHAPE PRIVACY PROTECTIONS FOR NEW TECHNOLOGIES (Mar. 18, 2021), https://www.brennancenter.org/sites/default/files/2021-03/Fourth-Amendment-Digital-Age-Carpenter.pdf [https://perma.cc/LVM6-JGNL] (footnotes omitted).

76. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417, 424 (2012) (Sotomayor, J., concurring) (Alito, J., concurring); *Carpenter*, 138 S. Ct. at 2223, 2235, 2246, 2261 (Kennedy, J., dissenting) (Thomas, J., dissenting) (Alito, J., dissenting) (Gorsuch, J., dissenting).

of the limit depends on the remedy created for the Fourth Amendment—the exclusionary rule—which further depends on motions to suppress evidence in criminal cases. Without formal cases reaching the motion stage, it is unclear what teeth the Fourth Amendment will really have on the information highway of the future.

v. Policy Variables

What is the purpose of a city? This existential question is not simply one for the classroom. As has been said before, "a city is not a computer,"[77] meaning city planners can decide to orient their visions around a hub other than constitutionally sound digital architectures. This is why housing codes and zoning are needed to create minimum standards—otherwise there could be substandard structures and dangers.[78] That would be similar to relying on the administrative agencies to craft most laws in particular areas because the legislature does not have the capacity or will to do so. In essence, it is just not the job of agencies to do so or the legislature to inform Fourth Amendment parameters.

Also, many of the problems with information gathering lie at the doorstep of private companies. Their desire for information will not be deterred by the Fourth Amendment since it does not apply to them as private parties. The acquisition of this private information by cities, however, can and ought to be deterred by the prospect of Fourth Amendment violation if the Third-Party Rule is changed and direct acquisition of the information can be properly limited.

vi. The Driver of Expediency

Governments and the police can be driven by short-term expediency more than the potential for long-term Fourth Amendment violations. We have seen numerous examples of this in recent years in different ways.

Cities may favor expediency over long-term constitutional legitimacy in their urban planning depending on their resources. Especially if cities don't have the money, they are not likely to prioritize compliance with prospective and speculative frameworks to elide Fourth Amendment difficulties. Cities also may prize community care efforts by police that justify the use of data to help residents, not merely interdict crime.

The lack of city planning and the impact of alternative variables is illustrated by the lack of preparedness by the State of Texas' electric grid for

77. Shannon Mattern, *A City is Not a Computer*, PLACES (Feb. 2017), http://www.placesjournal.org/article/a-city-is-not-a-computer/?cn-reloaded= 1#0 [https://perma.cc/AW6U-TXVK].

78. Even having such codes may not be enough if they are deficient in nature or implementation. *See, e.g.*, Christian De La Rosa & Andrea Torres, *Surfside Collapse: College Students in Love Found Dead as Death Toll Reaches 79*, LOCAL10.COM (July 10, 2021, 8:33 AM), https://www.local10.com/news/local/2021/07/10/surfside-building-collapse-university-of-chicago-student-found-dead-on-day-crews-recoved-12-dead [https://perma.cc/2WBS-M2DL].

the deep freeze of the winter of 2021.[79] The State had separated its grid from other states, in essence "going it alone." This approach did not serve it well, and it remains to be seen if a modified digital approach will be adopted in the future.

One primary illustration of how expediency might supersede long-term planning is the recent spate of criminal cyberhacking of things important to the American economy, from gas to meat.[80] The Colonial Pipeline hack on May 6, 2021, shut down the pipeline's delivery of gas and oil—almost half of all fuel consumed on the east coast—for almost a week and caused the company to pay almost four million dollars in bitcoin. This attack through an old Virtual Private Network ("V.P.N.") account of the company showed the vulnerabilities of critical systems to infiltration. With other ransomware attacks occurring after the Colonial attack, it became very clear that cities need protection from ransomware and other digital attacks, perhaps more than preventive planning about potential Fourth Amendment issues. The meat hack in June 2021 involved the largest supplier of meat in the world, the JBS Company.[81] The company paid the hackers 11 million dollars to continue their operations.[82]

Another illustration is the potential use of the Pegasus cyber-security software[83] if it becomes available to city politicians. Like with a tempting dessert, politicians might not be able to just "say no," particularly if they think no one will find out about it in the mix of many other software programs that provide massive amounts of data to the same cities.

In addition, climate change issues such as heat waves and ocean flooding create huge disruptions in how cities function. Cities likely will prioritize gathering information in a heat wave, such as the heat dome[84] and other heat waves that occurred over the western United States in the summer of 2021,[85] over any potential entanglement with the Fourth Amendment. Also,

---

79. *See* Robinson Meyer, *Texas Failed Because It Did Not Plan*, ATLANTIC (Feb. 21, 2021), https://www.theatlantic.com/technology/archive/2021/02/what-went-wrong-texas/618104 [https://perma.cc/6NDR-5G5L].

80. *See, e.g.*, Stephanie Kelly & Jessica Resnick-ault, *One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators*, REUTERS (June 8, 2021, 7:06 PM), https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08 [https://perma.cc/374W-6TQY].

81. Kevin Collier, *Meat Supplier JBS Paid Ransomware Hackers $11 Million*, NBC NEWS (June 9, 2021, 8:42 PM), https://www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html [https://perma.cc/SX4Z-5QZN].

82. *Id.*

83. Bergman & Kingsley, *supra* note 45.

84. *See, e.g.*, Isabella Grullon Paz, *California Braces for Dangerous Weekend of Record-Setting Heat*, N.Y. TIMES (July 16, 2021), https://www.nytimes.com/2021/07/08/us/heat-wave-warning-california.html [https://perma.cc/7RSF-N7Q2].

85. *See, e.g.*, *id.* ("California is bracing for another dangerous heat wave and record-breaking temperatures this weekend, just two weeks after a heat dome descended on the normally temperate Pacific Northwest, killing hundreds of people and capping North America's hottest June on record.").

California cities were not ready for the ferocity of recent wildfires. What else might arise in the future?

C. Where Does This Leave Us? Some Suggestions

If "smart" devices are inevitable, especially those that cross over into Fourth Amendment violation territory such as the new Pegasus software might, the real questions for digital urban planners might involve vulnerabilities and accuracy, not concern for eventual Fourth Amendment exclusion. What we see from Professor Ferguson's argument is that, at the least, we need protections from the sensors and ourselves. These protections can occur in different ways, as this Section will outline.

1. Digital Architecture: Firewalls

While there undoubtedly will be digital architectures in smart cities, it should be assumed that planners will continue to maximize use of sensors and technology if it brings expedient results. Instead of minimizing information flow, planners probably will follow a path identified by Professor Ferguson and learn to build firewalls to minimize access to the information by police, but not the information flow itself. In a way, this probably will be more like a dam-controlled river than a slow-flowing stream that does not produce a lot of water in the first place.

Thus, the emphasis likely should be about how to limit collections that occur and creating better government transparency—not omitting collection altogether. Consequently, governments should create firewalls to limit police access to information in the investigation of crime. While Professor Ferguson advocates "that the relationship between smart data collection and law enforcement monitoring remains separate and distinct,"[86] he does not provide sufficient details about how this will occur, particularly in light of the polarized political society where information is used against other domestic groups, not simply against foreign incursions. Thus, while governments will want to be flexible as to how information is used—e.g., to help citizens with streetlights, traffic congestion, and theft prevention—there must be transparency and clear limits in how police access sensor-produced information. Preventing digital indulgences are just as important as what the information is used to accomplish.

2. Reimagine "Search" Categories

Perhaps it is time to modify search categories, particularly those classifications where information is gathered outside of the criminal interdiction context. One large existing category is administrative searches, but that does not seem to provide adequate limits for the digital explosion or an explanation of how the information can be used in a large, interconnected smart environment such as a city. While cities may use information to promote health and safety, the information now can be saved in perpetuity and used

86. Ferguson, *supra* note 1, at 100.

for crime control and other similar purposes with little if any transaction costs downstream. It is the downstream usage and cross-over of information from a preventive measure—such as information about sidewalk congestion used to interdict crime—that should be one focus of courts in enforcing the Fourth Amendment in the digital age.

3. Pragmatism Over Constitutionalism

Given the speculative doctrinal and technological variables of the future—especially in terms of continuing case law and high-tech advances—cities may contour information-gathering to prioritize pragmatic issues, such as extremes brought about by climate change and cyberattacks like the one in 2021 on the Colonial Pipeline, over potential Fourth Amendment violations. Questions such as what are cities to do about climate issues like droughts in the western United States, fires in California, or increasing water intrusion along coastal areas[87] will likely drown out the call cognizance of Fourth Amendment issues. For example, the question of how Texas should prepare for the next deep freeze with its electric grid likely would not include a Fourth Amendment analysis.

One clearly pressing pragmatic question is what should be done by cities and states to prevent ransomware attacks? These are increasingly problematic, as the attack on the Colonial pipeline showed. That attack on the pipeline supplying 45 percent of oil and gas to the Eastern Seaboard of the United States not only shut down the pipeline but caused panic among consumers in several states.[88] Only after Colonial paid the attackers more than four million dollars was the company able to resume operations.[89] That resumption took several days, raising anxiety levels across the nation.[90] Consequently, a city may prioritize collecting data to minimize disasters or attacks over potential Fourth Amendment violation.

4. Is Positive Law the Answer?

Positive law[91] may indeed help and even be the best possible gap-filler for digital design of cities in the future, but it should not serve as the answer to

87. Consider, for example, New York after its last big storm, Sandy, New Orleans after Katrina, the Dixie California Wildfire of 2021, and the Creek fire of 2020. *See* CAL. DEP'T OF FORESTRY & FIRE PROT., TOP 20 LARGEST CALIFORNIA WILDFIRES (Oct. 26, 2021), https://www.fire.ca.gov/media/4jandlhh/top20_acres.pdf [https://perma.cc/TT5J-TQ6P]

88. Marisa Peñaloza, *Ransomware Attack Shuts Down a Top U.S. Gasoline Pipeline*, NPR (May 9, 2021, 11:07 AM), https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline [https://perma.cc/F7K2-GRRP].

89. Michael D. Shear, Nicole Perlroth & Clifford Krauss, *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES (June 7, 2021), https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html [https://perma.cc/2NT6-TPJ2].

90. *Id.*

91. Positive law is defined as "[a] system of law promulgated and implemented within a particular political community by political superiors, as distinct from moral law or law existing in an ideal community or in some nonpolitical community." *Positive Law*, BLACK'S LAW DICTIONARY (11th ed. 2019).

crafting Fourth Amendment friendly architectures. Instead, the positive law question just confirms that the doctrine needs extensive work. While Professor Ferguson ends with positive law, it is really just a good place to begin the exploration. An antiquated Fourth Amendment doctrine fraught with a variety of perils that do not address technological advances will not be saved by an infusion of positive government laws. There are several reasons for this. While laws will increase transparency and promote better understandings of the impact of the Fourth Amendment, a new tapestry of laws is very costly. For example, why should cities create laws first and have rulings on their constitutionality later, perhaps much later? The laws crafted by legislatures, particularly in the laboratories of the states, do not increase the legitimacy of judicial decision-making—it is not the legislature's job to come up with constitutional guidelines or substitute for judicial decision-making. Judges are constrained by *stare decisis* and canons of interpretation. Politicians can compromise, use broad policy, favor constituent groups, and accept industry input from lobbyists and their political parties, among many other things. Simply put, it should not be the legislature that guides the courts.

5. Do Not Forget the Forgotten Third Amendment

The Third Amendment states: "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[92]

As information gathering becomes ever more invasive, the Third Amendment may also be seen as a limitation on excessive, continuous, and endless gathering of information in homes by police or military forces that effectively deprives residents of the privacy afforded by the walls, doors, and roofs of their dwellings and instead serves as an equivalency of the quartering of soldiers without consent. This Section details how this could become a reality and revitalize an Amendment in desuetude.

Today it is not so far-fetched to believe that government "cybersoldiers" using the latest technology can extract data from private houses—from location of the occupants to friends, products purchased, electricity used, foods favored and so on—that would be the equivalent of "quartering" soldiers there without consent.

With increasing focus on domestic terrorism and the use of military equipment and tactics by the police, lines are blurring between local community policing and larger government security matters, including what might be called "military matters." Consequently, the Third Amendment[93] should be added to the digital architecture calculus for smart cities as well. The Third Amendment also provides a limit on the power of the government. Specifically, it prohibits the government from quartering soldiers in private houses in times of peace. While this may seem far afield

92. U.S. CONST. amend. III.

93. *Id.* ("No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.").

from sensors accumulating data as a part of networks, that is not the case. The Amendment has even greater applicability when the surveillance is built into the city's systems and is not just a transient event.

Conducting military operations—including the prevention and investigation of domestic terrorism—in a person's home violates the boundaries set by the Third Amendment. In today's digital world it would be improper to read the words of the Third Amendment literally, treating it merely as surplusage. Instead, the Amendment's check on government tyranny should be viewed as restricting cybersoldiers from focusing surveillance instrumentalities on and around private residences in an intrusive way—or using proxies to do so, similarly to *Carpenter*—that would serve as the functional equivalent of military quartering in the eighteenth century.

IV. CONCLUSION

Professor Ferguson's article on intentionally designing digital infrastructures of smart cities to minimize potential violations of the Fourth Amendment is a fine illustration of the importance of advance planning. In the digital world, "sensorveillance"[94] will be occurring with greater frequency and broader application. Digital architectures undoubtedly will be used to promote the smooth and effective operation of cities of the future. Yet, the incomplete and antiquated Third-Party Rule, combined with ever-advancing technologies and pragmatic issues such as ransomware attacks, implicit bias, and political decision-making, undermine the predictive value of such an effort to create a digital layer of urban planning that meets the requirements of the Fourth Amendment. Consequently, clearer boundaries of what information can be gathered and what cannot, transparency in how information-gathering occurs, and review of what governments are doing with the information should all become pillars in the future of the government information-gathering activities. Professor Ferguson's article provides a useful foundation for future city planning.

94. Ferguson, *supra* note 1, at 50, 112.