Washington Law Review

Volume 93 | Issue 4

12-1-2018

Privacy Localism

Ira S. Rubinstein

PRIVACY LOCALISM

Ira S. Rubinstein*

Abstract: Privacy law scholarship often focuses on domain-specific federal privacy laws and state efforts to broaden them. This Article provides the first comprehensive analysis of privacy regulation at the local level (which it dubs "privacy localism"), using recently enacted privacy laws in Seattle and New York City as principal examples. Further, this Article attributes the rise of privacy localism to a combination of federal and state legislative failures and three emerging urban trends: the role of local police in federal counterterrorism efforts; smart city and open data initiatives; and demands for local police reform in the wake of widely reported abusive police practices.

Both Seattle and New York City have enacted or proposed (1) a local surveillance ordinance regulating the purchase and use of surveillance equipment and technology by city departments, including the police, and (2) a law regulating city departments' collection, use, disclosure, and retention of personal data. In adopting these local laws, both cities have sought to fill two significant gaps in federal and state privacy laws: the public surveillance gap, which refers to the weak constitutional and statutory protections against government surveillance in public places, and the fair information practices gap, which refers to the inapplicability of the federal and state privacy laws to government records held by local government agencies.

Filling these gaps is a significant accomplishment and one that exhibits all of the values typically associated with federalism such as diversity, participation, experimentation, responsiveness, and accountability. This Article distinguishes federalism and localism and shows why privacy localism should prevail against the threat of federal and—more importantly—state preemption. This Article concludes by suggesting that privacy localism has the potential to help shape emerging privacy norms for an increasingly urban future, inspire more robust regulation at the federal and state levels, and inject more democratic control into city deployments of privacy-invasive technologies.

---

* Senior Fellow, Information Law Institute, New York University School of Law; Senior Fellow, Future of Privacy Forum. The author wishes to thank everyone who generously commented on this work during presentations at NYU Law's Privacy Research Group, the Privacy Law Scholars Conference, and NYU Law's Conference on Privacy Localism: A New Research Agenda. Particular thanks go to Kevin Bankston, Kiel Brennan-Marquez, Catherine Crump, Nestor Davidson, Daniel Francis, Barry Friedman, Amanda Levendowski, Bilyana Petkova, Joel Reidenberg, Jason Schultz, Stefaan Verhulst, and Jan Whittington for reading and commenting on earlier drafts of the paper. I also wish to thank a number of government and company officials and privacy advocates who answered my questions about local privacy laws: Ginger Armbruster, Courtney Bowman, Larry Byrne, Rebecca Lipman, Shankar Narayanan, Laura Negron, Mary Perry, Michael Price, Andrew Schaffer, Amy Tsai, and Jessie Woo. I owe a debt of gratitude to Allexia Bowman Arnold, Nicholas Cody, Sarah Smith and my other editors at *Washington Law Review* for their superb editing and unflagging enthusiasm. I also thank my research assistants, Erin Bansal, Christian Abouchaker, Alexia Ramirez, Cecilia Coelho Romero, and especially Nathaniel Tisa, for excellent help with this project.

INTRODUCTION

Over the past decade, the U.S. Congress has largely abdicated its role in regulating online consumer privacy or modernizing electronic surveillance laws to strengthen privacy protections in the context of emerging technologies. Congress enacted many important privacy laws from the 1970s through the 1990s, and updated several of them in the 2000s, but since then its privacy accomplishments have dwindled.[1] Both Democrats and Republicans have introduced comprehensive online consumer privacy bills but have not passed any of them.[2] Despite five years of debate, Congress has also failed to update the Electronic Communications Privacy Act (ECPA), the thirty-two-year-old law governing electronic surveillance.[3] Congress has fared somewhat better in reforming foreign intelligence surveillance following the revelations of former National Security Agency (NSA) contractor Edward Snowden. For example, it ended bulk collection of telephone metadata under the NSA foreign surveillance law.[4] But the era of reform did not last. During the first year of the Trump presidency, the Republican Congress voted to rescind Obama-era broadband privacy rules,[5] and at the beginning of its second year rejected a bipartisan push to add new privacy protections to a provision of the foreign surveillance law that was about to expire.[6]

During this period, state legislatures have been very active and successful in addressing consumer security and privacy. As of 2017, almost all fifty states have enacted breach notification statutes requiring

---

1. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 36–39 (6th ed. 2018) [hereinafter SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW].

2. *See* discussion *infra* section I.A.1.

3. The most recent attempt at modernization, brought forward in July 2017 by Senators Mike Lee and Patrick Leahy, has languished in the Senate Judiciary Committee since its introduction despite unanimous passage of related legislation by the House. *See* ECPA Modernization Act of 2017, S. 1657, 115th Cong. (2017); Allison Grande, *Sens. Push ECPA Reform Bill to Up Email, Location Privacy*, LAW360 (July 27, 2017, 9:38 PM), https://www.law360.com/articles/948832/sens-push-ecpa-reform-bill-to-up-email-location-privacy (last visited Oct. 20, 2018).

4. Sabrina Siddiqui, *Congress Passes NSA Surveillance Reform in Vindication for Snowden*, GUARDIAN (June 3, 2015, 2:28 AM), https://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden [https://perma.cc/L4Q2-EDA5].

5. S.J. Res. 34, 115th Cong. (2017) (enacted); *see* Kimberly Kindy, *How Congress Dismantled Federal Internet Privacy Rules*, WASH. POST (May 30, 2017), https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html?utm_term=.72a16f43a646 [https://perma.cc/SGU8-E3T8].

6. *See* Louise Matsakis, *Congress Renews Warrantless Surveillance—and Makes It Even Worse*, WIRED (Jan. 11, 2018, 4:19 PM), https://www.wired.com/story/fisa-section-702-renewal-congress/ [https://perma.cc/2Q4L-VVKL].

firms to disclose security breaches involving personal information and a few have set substantive requirements for data security.[7] But states have done more than fill the gaps in federal privacy laws.[8] They have expanded online privacy protections,[9] regulated private- and public-sector use of emerging technologies,[10] and enacted social media privacy laws.[11]

Now there is a new kid on the block: *local* privacy law and regulation. Local governments (primarily cities but also counties) have joined federal and state governments in enacting important new privacy laws.[12] This development has yet to receive attention even in the newest editions of privacy law casebooks and treatises. And the reason is obvious: until recently, cities played only a minor role in information privacy law. But this is beginning to change for several reasons.

American cities, especially large urban centers, are data-rich environments. Cities have large populations and city dwellers generate a vast amount of data through daily interaction with devices and sensors as they crisscross public spaces and utilize city services. A growing number of local police departments rely on special purpose technologies such as video security cameras, facial recognition technology, automatic license plate readers (ALPRs), police dashboard and body-worn cameras, and gunfire location services to assist them in maintaining public order, enforcing criminal laws, and safeguarding citizens against terrorist attacks. In New York City, for example, these surveillance efforts take place on a very broad scale that, when combined with analytic tools for

---

7. *See Security Breach Notification Laws,* NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/LJ9X-LLVQ].

8. *Id.* at 948 (noting that the federal government has yet to enact a general federal data breach notification statute or to establish broad standards requiring private firms outside the financial services or health care sectors to reasonably protect consumer data).

9. *See, e.g.*, Gregory S. McNeal, *California AG Releases Guide to Online Privacy Laws*, FORBES (May 21, 2014, 7:19 PM), https://www.forbes.com/sites/gregorymcneal/2014/05/21/california-ag-releases-guide-to-californias-online-privacy-laws/#2b5ac0b3798c [https://perma.cc/DW4D-YYNP] (describing amendments to California's "landmark" Online Privacy Protection Act of 2003).

10. *See infra* section III.D.1.

11. Beginning in 2012, many states have limited what entities may do with or require of individuals' personal social media accounts. Twenty-six have done so for employers; sixteen for educational institutions; and one for landlords. *See State Social Media Privacy Laws*, NAT'L CONF. ST. LEGISLATURES (Jan. 2, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx [https://perma.cc/5F4P-4MG5].

12. *See infra* sections II.A, II.B.

discovering unanticipated patterns,[13] provide the basis for what Professor Andrew Ferguson and others refer to as "big data policing."[14]

Cities also offer a diverse range of municipal services that touch almost every aspect of each resident's life. City agencies use a variety of means, including city web sites and Internet of Things (IoT) devices, to collect data related to infrastructure, traffic, utilities, tourism, education, child welfare, housing, and healthcare. So-called "smart cities" analyze these massive datasets to enable more efficient and effective monitoring and coordination of maintenance, mobility, environmental management, visitor movements, social services, and neighborhood sentiment.[15] They are also starting to deploy mobile apps to make such services more readily accessible to city residents.[16] And many cities now make these datasets freely available to the wider public through open data programs that publish all sorts of government data that anyone can use, analyze, or redistribute as they wish for a range of beneficial purposes.[17]

The arrival of big data in the urban environment brings with it an array of privacy challenges centered on two very different types of data: police data and civic data.[18] Police data encompasses criminal and arrest records collected by local police departments, other crime data, and related metadata captured by surveillance technologies.[19] Civic data includes both registration data (i.e., birth, death, marriage, and voting records

---

13. *See* Thomas H. Davenport, *How Big Data Is Helping the NYPD Solve Crimes Faster*, FORTUNE (July 17, 2016), http://fortune.com/2016/07/17/big-data-nypd-situational-awareness/ [https://perma.cc/8CQD-QF4A].

14. *See generally* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014).

15. On the value and uses of civic data, see generally STEPHEN GOLDSMITH & SUSAN CRAWFORD, THE RESPONSIVE CITY: ENGAGING COMMUNITIES THROUGH DATA-SMART GOVERNANCE (2014).

16. *See* Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1584 (2015).

17. *See generally* Frederik J. Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 BERKELEY TECH. L.J. 2073 (2015).

18. *See* Liesbet van Zoonen, *Privacy Concerns in Smart Cities*, 33 GOV'T INFO. Q. 472, 474–75 (2016). Zoonen analyzes city privacy concerns by identifying a two-by-two scheme in which there are two types of data (personal or impersonal) and two purposes for collection and use (service or surveillance). Applying this scheme, she argues that police data (personal data combined with surveillance purposes) raises greater privacy concerns than civic data (personal data combined with service purposes).

19. Police data may also include (1) external data collected by other government agencies and (2) privately collected data that a local police department purchases from external sources such as commercial data brokers or police analytic platforms. *See* Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOC. REV. 977, 994 (2017). Police department acquisition of data from other government agencies or from external sources is beyond the scope of this paper.

maintained at the local level) and the vast range of data generated and used by municipal services.

Cities large, medium, and small have responded to the privacy issues associated with urban big data by enacting local surveillance ordinances governing police data and adopting broad privacy principles addressing civic data. More than fifteen cities now have surveillance ordinances requiring local police forces to prepare and publish protocols disclosing the intended use and deployment of surveillance equipment and technologies, including information on data collection, use, access, retention, and sharing with other governmental entities.[20] These and other cities have also developed privacy guidelines governing smart city/IoT data practices, with Seattle and New York City emerging as leaders in these efforts. Both cities have enacted local laws covering *all* municipal data collection and use and have appointed Chief Privacy Officers.[21]

While this legislative activity is partly a response to regulatory gaps left by federal and state privacy laws, privacy localism also results from several broader and overlapping societal trends. These include the war on terror, which heightened the role of local police in federal counter-terrorism activities; "smart city" initiatives, which rely on potentially invasive technologies to help cities achieve important municipal goals such as improving their delivery of services; and the intense public scrutiny of abusive policing practices, including the use of certain surveillance technologies.[22]

This Article provides the first comprehensive analysis of privacy localism by examining its origins, motivations, and outcomes in response to these trends.[23] Using detailed case studies of Seattle and New York City, it considers how these two very different cities have regulated the collection, use, and disclosure of personal information by both police and civilian agencies. This requires exploring a variety of policy issues including how police balance security against privacy safeguards as they

---

20. See *Community Control over Police Surveillance*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance [https://perma.cc/XE7G-TU2J] (identifying cities that have enacted or are considering local laws regulating police acquisition and use of surveillance technologies). Some of these laws also require city council approval prior to acquisition and use. *See infra* sections II.A.1, II.B.1.

21. *See infra* sections II.A.2, II.B.2.

22. *See infra* section I.A.2.

23. For two complementary studies of local privacy regulation that also rely on case studies of major cities, see generally Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016) (discussing Seattle, Oakland, San Diego), and Jan Whittington et al., *Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government*, 30 BERKELEY TECH. L.J. 1899 (2015) (discussing Seattle).

adopt networked surveillance technology and how civilian agencies balance data exchanges and data analysis to achieve public goods against the need to maintain the confidentiality of the underlying data and the trust of local citizens.

What, then, is privacy localism? In normative terms, localism refers to a preference for local control of government function, while the law of localism describes the relations between states and their local governments.[24] This Article mainly addresses cities, but the term "local" covers every political subdivision smaller than a state. Thus, "privacy localism" refers to local control over the collection, use, and disclosure of the personal data of city residents. It encompasses the ordinances, local laws, executive orders, resolutions, regulations, policies, and practices of local governments insofar as they control (1) the surveillance activities of city police departments and other city agencies, and (2) the data collection and use practices of city agencies in the course of providing municipal services. The term also emphasizes a set of values including decentralization and local autonomy, which are traditionally associated with both federalism and localism.[25]

Of course, skeptics will ask whether privacy localism is viable. They will quite properly express doubts as to whether cities—occupying the lowest slot in the federal-state-city hierarchy—have enough power to engage in privacy localism without falling prey to federal, and especially state, interventions. Obviously, local privacy regulations are always at risk of federal and state preemption. Furthermore, federal and state agencies have far more resources at their disposal compared to cities, most of which probably lack the regulatory expertise and personnel needed to enter the already crowded field of privacy regulation or make any significant contributions.[26] Thus, there are structural as well as practical constraints on privacy localism.

And yet, cities can contribute a great deal to privacy law. This Article argues that cities have ample power to regulate both local police surveillance activities and local data governance practices, and that preemption is much less of an obstacle to privacy localism than one might suspect.[27] It offers three arguments in favor of privacy localism. The first is that privacy issues are highly salient to cities for the reasons already

---

24. *See* David J. Barron, *A Localist Critique of the New Federalism*, 51 DUKE L.J. 377, 381 (2001).

25. *See infra* section III.A.

26. *See* Edward Glaeser & Cass R. Sunstein, *Regulatory Review for the States*, NAT'L AFF., Summer 2014, at 37, 48.

27. Note, too, that even when federal or state law threatens to preempt local privacy regulation, it mainly establishes privacy "floors" that cities can and do exceed. *See infra* section III.B.

identified: that is where the people are, and hence where their data is, in great abundance. The second is that both Fourth Amendment doctrine and federal and state electronic surveillance laws are mostly silent on government surveillance in public places (the public surveillance gap),[28] and generally fail to address the data practices of government agencies (the fair information practices gap).[29] Privacy localism fills both of these gaps. The third is that cities are ideally suited to regulate police use of surveillance technology and local data practices because of their willingness to innovate, experiment, and devise novel approaches to privacy protection.

To set the stage for this discussion, Part I briefly considers the perilous state of privacy in the twenty-first century and how cities have responded to federal and state legislative failures and the broader societal trends identified above. It also analyzes in detail the public surveillance gap and the fair information practices gap. Part II then presents detailed case studies of local privacy regulation in Seattle and New York City, examining both local surveillance laws and local privacy principles governing city agencies. It concludes with a preliminary assessment of these regulations in terms of their overall contribution to democratic governance of local police forces and how well they close the two privacy gaps. Part III begins by attempting to sort out the relationship between federalism and localism. Next, it responds to the highly realistic threat that federal and (more importantly) state laws may limit or preempt a city's power to regulate local police surveillance and municipal data service, explaining why this threat is manageable. The Article then concludes with a forward-looking inquiry into the future of privacy localism on a national basis.

I. WHY PRIVACY LOCALISM?

A. Privacy at Risk

1. The Death of Privacy?

In an aptly named article in a 2000 Stanford Law Review symposium on "Cyberspace and Privacy: A New Legal Paradigm?," Professor A. Michael Froomkin analyzed the public and private sector's routine collection of personal data and the growing use of privacy-destroying

28. *See infra* section II.C.2.

29. *See infra* section II.C.3.

technologies.[30] While denying that current privacy law in the United States has kept up with the rapid advance of these technologies and practices, Froomkin rejected the idea that privacy was dead.[31] Rather, he pinned his hopes on fair information practices and surveillance laws restricting data collection, use, and retention.[32]

Almost twenty years later, is it still premature to mourn the death of privacy? Froomkin warned of the dangers of pervasive information collection online and in physical space before the 9/11 terrorist attacks and Congress's expansion of federal surveillance laws and practices; before the rise of pervasive and invasive surveillance technologies—such as networked video surveillance systems, facial recognition software, cheap Global Position System (GPS) tracking devices, the massive data collection resulting from ubiquitous IoT devices and new modes of profiling, and location tracking via social media platforms and third-party apps; and before big data began to systematically undermine the main premises of privacy law.[33] If privacy is not yet dead, it is no doubt stunned.[34] In any case, Froomkin has since ceased to believe that a legal response will emerge anytime soon or that the future bodes well for privacy.[35] And his pessimism certainly seems justified based on Congress's poor record of enacting federal privacy laws that keep pace with a new generation of invasive technologies and the advent of big data.

Despite its poor record, Congress has not been passive. Rather, it has introduced laws and held hearings on numerous subjects—spyware, cybersecurity, online behavioral tracking, cell phone tracking, mobile apps, biometrics, and access to social media passwords—none of which have advanced very far. Between 1970 and the mid-2000s, Congress passed over two dozen mostly sector-specific federal privacy laws.[36] Congress has also taken up omnibus privacy legislation seven times between 1999 and 2011, but few bills were even reported out of committee.[37] In 2016, the Obama Administration tried to jumpstart the

30. A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1468–1500 (2000).

31. *Id.* at 1542.

32. *Id.*

33. *See generally* Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, INT'L DATA PRIVACY L., May 2013, at 74, 76–78.

34. *See* Monty Python, *The Dead Parrot Sketch*, DAVID P. BROWN https://www.davidpbrown.co.uk/jokes/monty-python-parrot.html [https://perma.cc/FQ6R-DU8M].

35. *See* A. Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95 (2017).

36. *See supra* text accompanying notes 1–6.

37. *See, e.g.*, Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); Best Practices Act, H.R. 5777, 111th Cong. (2010); Online Personal Privacy Act, S. 2201, 107th Cong.

legislative process by issuing a draft discussion bill, but it failed to find any sponsors in Congress.[38]

There are ample grounds to predict that the 115th Congress will not surpass its predecessors. To begin with, there is much controversy concerning the accomplishments of the Republican Congress under President Donald Trump.[39] On the privacy front, the verdict is clear: the new Congress has not passed a single privacy bill of note. Instead, it withdrew the Obama Administration's broadband privacy rules, leaving the path open for state legislatures and city governments to take up the slack.[40] It has yet to agree on a data security breach notification bill, even though the existing patchwork of state breach notification laws—all fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted such laws—cries out for federal consolidation.[41] It reauthorized a foreign surveillance provision allowing warrantless surveillance in certain cases without adding new privacy protections.[42] But even a unanimously passed reform bill in the House and a new bipartisan bill in the Senate was not enough to make 2017 the year that Congress achieved ECPA reform.[43]

There are some indications that Congress is stepping up its efforts to enact consumer privacy legislation.[44] In the meantime, the states continue

---

(2002); Consumer Privacy Protection Act of 2002, H.R. 4678, 107th Cong. (2002); Consumer Online Privacy and Disclosure Act, H.R. 347, 107th Cong. (2001); Electronic Privacy Bill of Rights Act of 1999, H.R. 3321, 106th Cong. (1999); Online Privacy Protection Act of 1999, S. 809, 106th Cong. (1999). S. 2201 was reported out of committee but did not advance.

38. *See* Natasha Singer, *Why a Push for Online Privacy Is Bogged Down in Washington*, N.Y. TIMES (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html (last visited Oct. 20, 2018).

39. Kelsey Snell, *What Congress Accomplished and Didn't Accomplish in 2017*, NPR: ALL THINGS CONSIDERED (Dec. 29, 2017, 4:49 PM), https://www.npr.org/2017/12/29/574693600/what-congress-accomplished-and-didnt-accomplish-in-2017 [https://perma.cc/QBS4-7CE3].

40. *See* Eyragon Eidam & Jessica Mulholland, *10 States Take Internet Privacy Matters into Their Own Hands*, GOV'T TECH. (Apr. 10, 2017), http://www.govtech.com/policy/10-States-Take-Internet-Privacy-Matters-Into-Their-Own-Hands.html [https://perma.cc/DKS6-EX8M]; Kindy, *supra* note 5.

41. *See* NAT'L CONF. ST. LEGISLATURES, *supra* note 7.

42. Matsakis, *supra* note 6; *see also* Robyn Greene, *Americans Wanted More Privacy Protections. Congress Gave Them Fewer*, SLATE (Jan. 26, 2018, 7:45 AM), https://slate.com/technology/2018/01/congress-reauthorization-of-section-702-of-the-fisa-is-an-expansion-not-a-reform.html [https://perma.cc/BNT2-Y3NL].

43. *See* Grande, *supra* note 3. This is not the first time ECPA reform has stalled in the Senate after easy passage through the House. *See* Sean D. Carberry, *House Passes Email Privacy Act, Again*, FCW (Feb. 7, 2017), https://fcw.com/articles/2017/02/07/ecpa-passes-house-again.aspx [https://perma.cc/TEC2-VMJF].

44. *See* Daniel R. Stoller, *Bipartisan Senate Quartet in Talks on Data Privacy Bill*, BLOOMBERG L.: PRIVACY & DATA SEC. (Aug. 29, 2018), https://www.bna.com/bipartisan-senate-quartet-n73014482126/ [https://perma.cc/HLJ2-8RZM].

to play the role of "especially important laboratories for innovations in information privacy law."[45] States have always filled gaps in federal privacy law and developed new laws addressing emerging technologies and social practices.[46] In May 2018, the California Legislature passed a bold and sweeping consumer privacy law that may have ripple effects throughout the United States.[47] But for reasons discussed below, the states have neither tackled surveillance laws addressing a new class of pervasive and invasive technologies on a comprehensive basis nor enacted (or extended) state privacy laws to protect records held by local governments. Hence the need for privacy localism.

2. Local Trends

One of the societal trends prompting local privacy regulations is the war on terror, which has forced federal intelligence agencies to enlist state and especially local police departments to serve as their "eyes and ears."[48] With control over billions of dollars in federal funding and generally superior knowledge of foreign threats, the intelligence community seeks to preserve centralized control over local counter-terrorism efforts, even though much of the surveillance conducted within city limits is undertaken by local police.[49] Federal counter-terrorism officials interact with local law enforcement in two main ways. First, the Department of Justice (DOJ) and the Department of Homeland Security (DHS) provide grant-in-aid programs to fund the acquisition of equipment used in

---

45. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 916 (2009) (arguing that preemptive, omnibus federal privacy law would undermine experimentation in federal and state sectoral privacy laws). *Compare id.*, *with* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868 (2009) (arguing that state experimentation tends to follow federal leadership).

46. *See supra* text accompanying notes 7–11.

47. *See* Eric Goldman, *A Privacy Bomb Is About to Be Dropped on the California Economy and the Global Internet*, TECH. & MKTG. L. BLOG (June 27, 2018), https://blog.ericgoldman.org/archives/2018/06/a-privacy-bomb-is-about-to-be-dropped-on-the-california-economy-and-the-global-internet.htm [https://perma.cc/GWQ2-V34M]. The new California law may even prompt Congress to enact long awaited privacy legislation, which industry hopes would include language preempting the new California law. *See* Jedidiah Bracy, *Notes from the IAPP Publications Editor, July 27, 2018*, IAPP: U.S. PRIVACY DIG. (July 27, 2018), https://iapp.org/news/a/notes-from-the-iapp-publications-editor-july-27-2018/ [https://perma.cc/FV4Y-WQXG].

48. Samuel J. Rascoff, *The Law of Homegrown (Counter) Terrorism*, 88 TEX. L. REV. 1715, 1721 (2010). *See generally* Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289 (2012).

49. *See* Waxman, *National Security Federalism in the Age of Terror*, *supra* note 48, at 302–05; Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counter-Terrorism After 9/11*, 3 J. NAT'L SEC. L. & POLICY 377, 388 (2009).

counterterrorism and law enforcement activity, subject to various federal conditions and requirements.[50] Second, many cities participate in Joint Terrorism Task Forces designed to coordinate counter-terrorism activity across multiple levels of government[51]; they also help staff "fusion centers" designed to generate and share local intelligence using sophisticated monitoring and information gathering techniques.[52]

Not surprisingly, New York City took the lead in deploying a broad range of surveillance technologies and otherwise securing the city in the wake of the 9/11 attacks. For example, in 2008, the New York Police Department (NYPD) launched a networked surveillance system in Lower Manhattan "to bring extra protection to the Financial District, one of the most tempting terror targets on earth."[53] It then worked with Microsoft to co-design a citywide network of sensors, databases, devices, software, and related infrastructure known as the "Domain Awareness System" (DAS).[54] Initially, the DAS included video security cameras, automatic license plate readers (ALPRs), and radiation sensors.[55] Later on, the NYPD added geocoded criminal records and integrated the network surveillance capabilities of the DAS with analytic methods designed to inform both tactical decisions (like sending automatic alerts when gunshots were detected) and strategic decisions (like using predictive policing algorithms to help allocate police resources).[56] Recognizing the

---

50. Waxman, *National Security Federalism in the Age of Terror*, *supra* note 48, at 308. Of course, in the aftermath of 9/11, the U.S. government also invested heavily in new surveillance technology for its own use; set up bulk surveillance programs to gain systematic access to huge volumes of telephone and internet metadata, foreign communication, and travel and financial data; and engaged in aggressive data mining and analysis projects like the Total Information Awareness (TIA) program. *See generally* Ira S. Rubinstein et al., *Systematic Access to Private-Sector Data: A Comparative Analysis*, *in* BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 5–48 (Fred H. Cate & James. X. Dempsey eds., 2017) (describing a range of NSA surveillance programs); Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261 (2008) (discussing the TIA program).

51. *See generally* Susan N. Herman, *Collapsing Spheres: Joint Terrorism Task Forces, Federalism, and the War on Terror*, 41 WILLAMETTE L. REV. 941 (2005).

52. *See generally* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2010).

53. RAY KELLY, VIGILANCE: MY LIFE SERVING AMERICA AND PROTECTING ITS EMPIRE CITY 204 (2015).

54. *See* Neal Ungerleider, *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" with Real-Time CCTV, License Plate Monitoring*, FAST CO. (Aug. 8, 2012), https://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito [https://perma.cc/73G3-7267].

55. *See* E. S. Levine et al., *The New York City Police Department's Domain Awareness System*, INTERFACES, Jan.-Feb. 2017, at 70, 75–76.

56. *Id.* at 73.

utility of the DAS for general policing, the NYPD eventually deployed the DAS to every precinct in the city and later developed a mobile version optimized for smartphones and tablets for use by all of its police officers.[57] More recent reports indicate that the NYPD has adopted sophisticated facial recognition technology to search images from social media and surveillance cameras for potential offenders.[58] This amounts to police surveillance of public spaces at an unprecedented scale that, when combined with large-scale analytics, results in big data policing.[59] To its credit, the NYPD understood from the outset that the sheer size and scope of the DAS would raise serious privacy concerns and, in the absence of federal surveillance laws addressing the DAS, adopted privacy guidelines covering its use of this new surveillance system; in 2017, the city council introduced a local surveillance law as well.[60]

Another trend is the rash of smart city initiatives and their tendency to neglect privacy issues.[61] There are many definitions of "smart cities." From the technical perspective of IBM engineer Colin Harrison, the term denotes an instrumented, interconnected, and intelligent city.[62] Privacy researchers Kelsey Finch and Omer Tene start from a similar definition of smart cities as growing networks of connected technologies generating actionable data about the city and its residents ranging from more efficient permit and licensing systems to new transportation services to improved infrastructure, but worry that the "scale on which smart cities collect, analyze, and exploit data about their citizens could set them apart from any other surveillance mechanism in history."[63] At the same time, smart cities also have to contend with a host of new issues resulting from (1) the embrace of "open data," which requires new risk management tools to

57. *Id.*

58. *See* Faiza Patel & Michael Price, *Keeping Eyes on NYPD Surveillance*, BRENNAN CTR. FOR JUSTICE (June 13, 2017), https://www.brennancenter.org/blog/ny-city-council-needs-increase-scrutiny-nypd%E2%80%99s-surveillance-arsenal [https://perma.cc/3N7C-3P5U].

59. Levine et al., *supra* note 55, at 73 (commenting that as of April 2016, the DAS contained the following records: "two billion readings from license plates (with photos), 100 million summonses, 54 million 911 calls, 15 million complaints, 12 million detective reports, 11 million arrests, two million warrants, and 30 days of video from 9,000 cameras"). *See generally* FERGUSON, *supra* note 14.

60. *See infra* section II.B.1.

61. *See* Finch & Tene, *supra* note 16.

62. Colin Harrison et al., *Foundations for Smarter Cities*, IBM J. RES. & DEV., July-Aug. 2012, at 1, 2 (noting that smart cities enable the "capture and integration of live real-world data through the use of sensors, kiosks, meters, personal devices, appliances, cameras, smart phones, implanted medical devices, the web, and other similar data-acquisition systems, including social networks as networks of human sensors").

63. Finch & Tene, *supra* note 16, at 1606.

balance the gains from civic innovation against the risks of re-identification and associated privacy harms;[64] and (2) cities becoming "platforms" and therefore having to mediate how citizens as users interact with smart city technologies and publicly and privately developed apps for accessing city services and datasets ranging from budget projections to building permits to parking violations to student disciplinary reports.[65] As Finch and Tene point out, this new role provides cities with a golden opportunity to act as data stewards by setting new norms and standards around privacy for emerging technologies.[66]

Finally, the growing emphasis on big data policing and smart city enhancements to urban quality of life coincide with a third trend: intense public scrutiny of abusive policing practices such as stop and frisk, racial profiling, excessive use of force, police perjury, police militarization, and—most tragically—multiple police shootings of unarmed civilians.[67] The common factor in these practices is their malignant effect on racial minorities, immigrants, the poor, and the most vulnerable in our communities. The need for police reform provides the broader context and sense of urgency around cities adopting both local surveillance ordinances and citywide data privacy principles.

B. Two Gaps in Privacy Law

Privacy localism helps address two significant gaps in federal and state privacy regulation. The first is the absence of Fourth Amendment or statutory protection for personal information collected in public settings. The second is the absence of federal or state privacy laws applicable to city agencies that collect, store, use, or share records about individuals that contain personal information.

1. The Public Surveillance Gap

Professor Christopher Slobogin recently coined the phrase "panvasive surveillance" to capture the idea that mass surveillance techniques are

64. *Id.* at 1611–13. When cities publish thousands of data sets on all kinds of civic functions, they increase the risk of exposing the sensitive information of local residents. They therefore need tools for evaluating whether, and how, a sensitive dataset may be released to the public while minimizing the risk of privacy violations.

65. *Id.* at 1593–95.

66. *Id.* at 1607.

67. *See generally* JAMES FORMAN JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA (2017); BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 6–14 (2017); FRANKLIN E. ZIMRING, WHEN POLICE KILL (2017).

now "pervasive and invasive," and affect "huge numbers of people, most of whom are innocent of any wrongdoing."[68] For reasons that all of these scholars have readily identified, "the Fourth Amendment is not implicated by most types of panvasive surveillance."[69] Nor do related federal electronic surveillance laws (ECPA) offer protection against police use of panvasive surveillance in public spaces. This results in a gap in the law, the "public surveillance gap."

Privacy theory has long recognized the tension between the surveillance of pedestrians on public streets and the anonymity enjoyed in public places. In his early and influential analysis of the function of privacy in a democratic society, Professor Alan Westin identified anonymity as a "state of privacy" that "occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance."[70] More recently, Slobogin offered a sophisticated treatment of "a right to public anonymity," which he defines as an assurance that when in public, one is "presumptively nameless . . . as far as the government is concerned."[71] His primary concern was to establish a Fourth Amendment basis for "privacy in public."[72] More specifically, he made the case for applying the reasonable expectation of privacy test to closed-circuit television (CCTV) operated by the government in public spaces, notwithstanding the U.S. Supreme Court's contrary holdings in a series of cases described below.[73]

U.S. Supreme Court precedent establishes that citizens do not generally enjoy a reasonable expectation of privacy in public. In *Katz v. United States*,[74] which is best known for Justice Harlan's concurring opinion establishing the reasonable expectation of privacy test, Justice Stewart

---

68. Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1723 (2014) [hereinafter Slobogin, *Panvasive Surveillance*]. Other Fourth Amendment scholars have recognized the same phenomenon, although they call it by different names. *See, e.g.*, Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 286 (2016); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1051–53 (2016).

69. Slobogin, *Panvasive Surveillance*, *supra* note 68, at 1723.

70. ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1970).

71. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 91 (2007) [hereinafter SLOGOBIN, PRIVACY AT RISK].

72. *Id.* at 79–117; *see also* HELEN NISSENBAUM, PRIVACY IN CONTEXT 91 (2010); Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643 (2013) (applying Nissenbaum's theory of contextual integrity to Fourth Amendment analysis); Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141 (2014).

73. SLOBOGIN, PRIVACY AT RISK, *supra* note 71, at 106–17.

74. 389 U.S. 347 (1967).

asserted in the majority opinion that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[75] Over the next few years, the Court consistently held that there is no reasonable expectation of privacy in anything seen or heard from a public vantage point.[76] The Court extended this doctrine to open fields, even if they are secluded and the owner takes steps to shield them from public view,[77] and to naked-eye aerial observation of a person's backyard[78] or a greenhouse with partially open sides and roof.[79] In the "beeper" cases, which involved police use of radio transmitters to follow vehicles and their contents on a public road, the Court held that the Fourth Amendment did not apply because a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[80]

Thus, police use of video cameras, ALPRs, shot detectors, drones, and facial recognition software—in other words, all the components of the NYPD's DAS—would not constitute a search under the plain view or open fields doctrines or the beeper cases.[81] Public surveillance receives somewhat more protective treatment under *United States v. Jones*,[82] a 2012 case in which the police, acting without a valid warrant, attached a GPS tracking device to the underside of a drug suspect's car and tracked his movement over a period of twenty-eight days. In a majority opinion authored by Justice Scalia, the Court revived the traditional trespass theory of the Fourth Amendment to find that the government's physical installation of the device constituted a "search" under the Fourth Amendment.[83] But in two separate concurrences, five justices rejected the

---

75. *Id.* at 351.

76. *See, e.g.*, Harris v. United States, 390 U.S. 234, 236 (1968).

77. Oliver v. United States, 466 U.S. 170 (1984).

78. California v. Ciraolo, 476 U.S. 207 (1986).

79. Florida v. Riley, 488 U.S. 445 (1989). Later cases added the "general public use" exception under which "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public" might require a warrant. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986). But many commentators have disparaged this exception as unworkable given the rapid pace of technological development and the ready availability of even the most sophisticated technology. *See* SLOBOGIN, PRIVACY AT RISK, *supra* note 71, at 54–62.

80. United States v. Knotts, 460 U.S. 276, 281 (1983) (police tracked a container in a car holding chemicals used in drug manufacturing). One exception is when use of the device reveals a "critical fact about the interior of the premises," which would constitute a search and therefore requires a warrant. *See* United States v. Karo, 468 U.S. 705, 715 (1984) (police tracked container to inside of homes).

81. *See* SLOBOGIN, PRIVACY AT RISK, *supra* note 71, at 106–08.

82. 565 U.S. 400 (2012).

83. *Id.* at 404, 409 (as Justice Scalia noted in defending his approach, "[t]he *Katz* reasonable-

trespass approach as artificial and irrelevant; they instead directly confronted the issue of whether long-term GPS monitoring of the defendant's vehicle violated his reasonable expectation of privacy under the *Katz* test and concluded that it had.[84]

Justice Alito's concurrence made this point rather bluntly, stating that the majority's reasoning "largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking)."[85] Justice Sotomayor's concurrence went even further, noting that "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," which the government can then store and efficiently "mine . . . for information years into the future."[86]

Jones signals a greater willingness on the part of the Court to confront new surveillance technologies head-on rather than allow the Fourth Amendment to atrophy in the contemporary setting. Two more recent opinions by Chief Justice Roberts continue this trend. In *Riley v. California*,[87] a unanimous Court held that police require a warrant to search the information on a cell phone seized incident to an arrest because cell phones are quantitatively and qualitatively different from other items found on an arrestee's person, in part due to the "immense storage capacity" of modern cell phones.[88] And this past term, in *Carpenter v. United States*,[89] a divided Court held that the government conducts a search when it accesses historical cell site location information to determine the location of a suspect over a four-month period.[90] As in *Jones* (and drawing on *Riley*), the *Carpenter* court concluded that such monitoring is a "new phenomenon" warranting a higher level of protection than ordinary record requests.[91] Thus, the 5-4 majority opinion adopted a different approach from past cases that both breaks the shackles

---

expectation-of-privacy test has been *added* to, but *not substituted for*, the common-law trespassory test . . .").

84. *Id.* at 413–18 (Sotomayor, J., concurring); *id.* at 418–31 (Alito, J., concurring).

85. *Id.* at 424 (Alito, J., concurring).

86. *Id.* at 415 (Sotomayor, J., concurring).

87. 573 U.S. __, 134 S. Ct. 2473 (2014).

88. *Id.* at 2478.

89. 585 U.S. __, 138 S. Ct. 2206 (2018).

90. *Id.* at 2220.

91. *Id.* at 2216 (characterizing both GPS tracking of a vehicle and cell site location information as "detailed, encyclopedic, and effortlessly compiled").

of trespass theory and begins chipping away at the third-party doctrine.[92] While the Court did not overrule *United States v. Miller*[93] or *Smith v. Maryland*,[94] it refused to apply the third-party doctrine automatically and declined to extend it to the collection of cell site location information.[95] Instead, the Court announced a "digital-*Katz* test for surveillance technologies."[96] This test amounts to a multifactor analysis of data quantity and quality in a specific technology. The majority found that use of this particular surveillance technology violated a reasonable expectation of privacy based on its sensitivity, exhaustiveness, retrieval cost, capability of reconstructing past movement, and voluntariness of third-party sharing. But the Court emphasized that its decision was narrow, while refusing to express a view on other technologies, such as real-time collection of cell site location information or "tower dumps" (a technique for collecting all the devices connected to a specific particular cell site during a particular interval).[97]

Together, *Jones*, *Riley*, and *Carpenter* suggest that a (sometimes thin) majority of the Court firmly believes that when surveillance is all-encompassing, it may violate society's reasonable expectations of privacy, even in cases where the surveillance occurs in public places. And yet, it is not at all clear that this line of cases will alter the Court's treatment of video cameras and the related public surveillance technologies associated with the DAS.[98] Unlike the GPS tracking at issue in *Jones*, which consisted of long-term monitoring of a single known

92. Under this doctrine, no search occurs when a person voluntarily turns over data to a third party such as bank records to a bank or dialed phone numbers to a telecommunications company, because she assumes the risk these records will be shared outside the company, even with the government. *See* Smith v. Maryland, 442 U.S. 735, 742–43 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

93. 425 U.S. 435 (1976).

94. 442 U.S. 735 (1979).

95. *Carpenter*, 138 S. Ct. at 2219–20.

96. Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV.: BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/ [https://perma.cc/97SL-WQNY].

97. *Carpenter*, 138 S. Ct. at 2220. *Carpenter* generated four dissenting opinions, none of which were happy with the Court's new balancing test. Justice Kennedy defended the third-party doctrine, arguing that it controlled cell site location information; Justice Thomas wanted the Court to reconsider (and perhaps repeal) the *Katz* test; Justice Alito worried that the holding would justify challenges to other court orders (including various kinds of subpoenas); Justice Gorsuch objected to *Katz* and the third-party doctrine and hinted at a new property-based test (not confined to trespass) under which a person might have a sufficient interest in his cell site location information as a form of "papers" to justify protection under the Fourth Amendment. *Id.* at 2223–72.

98. *See* Slobogin, *Panvasive Surveillance*, *supra* note 68, at 1747 (concluding that panvasive surveillance remains "immune from constitutional review" notwithstanding the decision in *Jones*).

target, the DAS components engage in universal monitoring of every person or vehicle who passes within range of a video camera, license plate reader, gunshot detector, or drone. These devices passively record and store images and sounds, which are fed into a prescriptive analytics program designed to detect suspicious behavior, including abandoned packages or movement in prohibited areas. If the program triggers an alarm, a trained police officer reviews and evaluates it, taking into account other sensor feeds and geocoded records in the vicinity of the alarming sensor. This prevents the police from deploying resources if the alarm is a false-positive; however, if the officer judges the alarm to be legitimate, a police response follows.[99] Thus, the DAS bears little resemblance to GPS tracking because the monitoring capabilities of the DAS are wide, but not very deep.[100]

Of course, one can devise a hypothetical in which the NYPD uses the wide area monitoring of the DAS to track an individual over an extended period of time. But this is not the intended purpose of the DAS and it seems more likely that if police sought to track specific individuals over an extended period, they would rely on GPS tracking devices (as in *Jones*) or cell site location information (as in *Carpenter*). Nonetheless, some scholars argue that any time the police use a system like the DAS to track and identify an individual, the courts should treat this as a "search" requiring a warrant.[101] But important differences remain between: (1) the ordinary use of individual component technologies of the DAS; (2) the use of the network surveillance capabilities of the DAS when integrated with predictive analytics to track and identify a suspect over time (which might happen in the future); and (3) the twenty-eight day GPS monitoring at issue in *Jones* or the 127 days of cell phone monitoring at issue in *Carpenter*. In short, the ordinary use of the DAS simply does not generate the comprehensive record of a person's public movements that animated the Court's new line of reasoning in *Jones* and *Carpenter*. The absence of long-term monitoring by the DAS seems like enough of a distinguishing factor for the Court to adhere to its earlier reasoning in *Katz* and the pre-

99. Levine, *supra* note 55, at 74.

100. Professor Kiel Brennan-Marquez helped me formulate this distinction.

101. *See, e.g.*, CONSTITUTION PROJECT, GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE: A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES 28 (2007), http://constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf [https://perma.cc/27EF-DW7Z] (arguing that law enforcement must obtain a warrant prior to using a public video surveillance system to track or identify an individual); *see also* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 602–05 (2017).

digital cases rather than treat the DAS or its component parts as another novel technology warranting a different approach.[102]

So far, this section has focused on the Fourth Amendment gap in addressing surveillance of public spaces. There is a parallel gap in federal surveillance laws, which generally do not cover law enforcement use of video surveillance in public spaces. Congress deliberately omitted video surveillance from the scope of the Wiretap Act, which otherwise covers governmental interception of "wire" and "oral" communications.[103] And this omission was not reversed when Congress enacted ECPA, which extended the Wiretap Act to "electronic communications."[104] Furthermore, the operative provision of the Wiretap Act prohibits the "interception" of wire, oral, or electronic communications, and video surveillance does not require "interception" as that term is defined in the statute.[105] Thus, public video surveillance and most other components of the DAS are beyond the scope of ECPA except to the extent that they record conversations.[106] The norm for CCTV cameras and ALPRs is silent recording that captures images but not sounds. Nor are gunshot detectors designed to capture human voices (although occasionally they do, in which case the Wiretap Act might apply).[107]

2. The Fair Information Practices Gap

The Fair Information Practices (FIPs) are the basis for modern privacy regulation, both in the United States and abroad.[108] There are different

---

102. *See Carpenter*, 138 S. Ct. at 2220 (stating that the Court's decision does not "call into question conventional surveillance techniques and tools, such as security cameras").

103. *See* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 6.2.1.A.2 (Kristen J. Mathews ed., 2d ed. 2016) (citing S. REP. NO. 99-541, at 16–17, reprinted in U.S.C.C.A.N. 3555, 3570–71); United States v. Koyomejian, 970 F.2d 536, 539–40 (9th Cir. 1992) (discussing omission).

104. *See* SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 1, at 378.

105. 18 U.S.C. § 2510(4) (2012).

106. If video surveillance includes sound, it would fall within the definition of "oral communications" under the Wiretap Act. *See* SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 1, at 378.

107. *See* Alexandra S. Gecas, *Gunfire Game Changer or Big Brother's Hidden Ears?: Fourth Amendment and Admissibility Quandaries Relating to Shotspotter Technology*, 2016 U. ILL. L. REV. 1073, 1096–97 (2016).

108. *See* SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 1, at 663–65. The FIPs are a set of internationally recognized privacy principles that date back to the 1970s. They have helped shape not only the main U.S. privacy statutes but also European data protection law. *See generally* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICE IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-

formulations of the FIPs and they vary as to both the number of principles and their substantive content. But all versions have in common the allocation of "rights and responsibilities that are associated with the transfer and use of personal information."[109]

In 1974, Congress enacted the Privacy Act, which regulates the way federal agencies collect, maintain, use or disseminate the personal information of individuals.[110] The Privacy Act is the first federal law to embody the FIPs. But it applies only to federal agencies; it does not apply to the private sector or to state or local agencies.[111] Relatively few states have statutes comparable to the Privacy Act and the ten or so that do vary widely. For example, New York's Personal Privacy Protection Act requires that each state agency "that maintains a system of records" must comply with the FIPs.[112] But the law does not apply to local governments. Although Washington is one of the few states to have created an Office of Privacy and Data Protection, whose remit includes updating state agency privacy policies, consumer education and outreach, monitoring citizen complaints, and promoting best practices,[113] Washington does not have a state law imposing the FIPs on government agencies.

It follows that there is a gap—a fair information practices gap—that applies to the collection, use, and disclosure of personal information by most state and city governments. This gap is significant. It means that most local governments are not required by law to adhere to the FIPs. It also means that they neglect an equally important aspect of the Privacy Act, and the more recent E-Government Act, requiring federal agencies

---

electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf [https://perma.cc/8Y2K-6LD8].

109. SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 1, at 664.

110. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)) (limiting disclosure, data collection and retention of such information, requiring various notices, granting a right of access and correction, imposing data security requirements, and providing enforcement rights).

111. *See* SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 1, at 666. There is one exception—the Act's rules for social security numbers apply beyond federal agencies. *Id.*

112. N.Y. PUB. OFF. LAW § 94 (McKinney 2018). A few other states have similar laws, for example, California, Massachusetts, and Minnesota. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS: 2017, 125–26 (2017) [hereinafter SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS]; Uniform Information Practices Act, HAW. REV. STAT. § 92F-1 (2018) (Hawaii); Fair Information Practices Act, IND. CODE § 4-1-6 (2018) (Indiana); Government Records Access and Management Act, UTAH CODE ANN. § 63G-2-101 (West 2018) (Utah). States with much narrower government records laws include Alaska, Connecticut, and Wisconsin.

113. *See* Wash. Exec. Order 16-01 (Jan. 5, 2016), https://www.governor.wa.gov/sites/default/files/exe_order/eo_16-01.pdf [https://perma.cc/2BGY-L5GB]; Office of Privacy and Data Protection Creation Act, H.R. 2875, 64th Leg., Reg. Sess. (Wash. 2016) (codifying E.O. 16-01).

to prepare both System of Records Notices (SORNs)[114] and Privacy Impact Assessments (PIAs).[115]

In sum, the vast majority of states and cities are not bound by the FIPs when state and local agencies collect, store, use, and disseminate personal information. Nor do they benefit from related methodologies and practices like SORNs and PIAs, which require government officials administering data-rich programs to think about privacy protections and hold them accountable if they neglect this responsibility.

II. CASE STUDIES: SEATTLE AND NEW YORK CITY

The case for privacy localism rests on the idea that local autonomy helps promote laboratories for democracy as well as participatory opportunities for citizens. There is little question that states have played this role when acting as first movers in identifying and regulating emerging privacy concerns and enabling simultaneous experimentation with multiple policy solutions. As noted above, California has a long history of enacting innovative privacy laws that have shaped privacy and security standards on a national basis,[116] and recently passed a new consumer privacy law with national implications.[117] This Part argues that the time is ripe to expand this characterization of the benefits of local

114. Federal agencies must publish SORNs in the Federal Register when they maintain personal information in system of records and the information is retrieved by a personal identifier. *See* 5 U.S.C. § 552a(e)(4) (2012). SORNs serve two salutary purposes: they provide (1) notice to the public about their rights under the Privacy Act and (2) useful information for privacy advocates, alerting them to new government databases and thereby enabling them to analyze whether these databases comply with federal law. *See* Jeramie D. Scott, *DoD Claim that NSA in Compliance with Privacy Act Ring Hollow*, EPIC: PRIVACY RTS. BLOG (Feb. 12, 2015, 5:31 PM), http://epic.org/blog/2015/02/dod-claim-nsa-in-compliance-with-the-privacy-act-when-it-clearly-is-n.html [https://perma.cc/G3J8-TLA6]. Second, they force agencies to continually examine and rationalize their own policies and practices (as a prelude to issuing new SORNs).

115. Section 208 of the E-Government Act of 2002 requires agencies to conduct a PIA before developing or procuring IT systems or initiating projects that collect, maintain, or disseminate personal information from or about members or the public. *See* Pub. L. No. 107-347, § 208-b, 116 Stat. 2899, 2921–22 (codified as amended at 44 U.S.C. § 3501 (2012)). The purpose of a PIA is to demonstrate that program managers and system owners have consciously incorporated privacy protections throughout the development of a system or program. Agencies are required to make PIAs publicly available through publication in the Federal Register or through a posting on the agency websites, subject to certain exceptions. *See generally* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-03-22, OMB GUIDANCE FOR IMPLEMENTING THE PRIVACY PROVISIONS OF THE E-GOVERNMENT ACT OF 2002 (2003), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22 [https://perma.cc/LJH5-VN4V].

116. *See* Hogan Lovells, *California Continues to Shape Privacy and Data Security Standards*, IAPP: PRIVACY TRACKER (Oct. 1, 2013), https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/ [https://perma.cc/39RS-AMXV].

117. Goldman, *supra* note 47.

policymaking from states to cities. It explores in detail the experiments with privacy localism in Seattle and New York City. Both cities have enacted or introduced local surveillance ordinances. Both are subject to ongoing judicial oversight related to police practices and abuses. Both have imposed citywide privacy laws while embracing open data programs. Accordingly, they are similar enough for comparison, yet their experiments in privacy also reflect profound differences in their political and cultural make-up, not least of which is New York's direct experience with the devastating 9/11 terrorist attacks.

There are two additional arguments in favor of privacy localism. The first is the new emphasis on governance rules and agency design as solutions to Fourth Amendment doctrinal deficiencies and the lack of transparency and accountability in modern policing. Legal scholars such as Christopher Slobogin,[118] Barry Friedman and Maria Ponomarenko,[119] and Daphna Renan[120] have all turned to administrative law as a new source of insight into these longstanding problems. And privacy localism perfectly exemplifies this administrative turn by relying on locally elected officials to establish policy and exercise discretion in applying local rules in a reasonable manner. The second is that privacy localism in Seattle and New York City seem remarkably successful in addressing the public surveillance gap and the fair information practices gaps.

A. Seattle

Seattle is Washington State's largest and fastest-growing city, with an estimated 2017 population of about 725,000.[121] It has a vibrant local

118. *See* Slobogin, *Panvasive Surveillance*, *supra* note 68.

119. *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827 (2015).

120. *See* Renan, *supra* note 68.

121. U.S. Census Bureau estimates rank Seattle as the eighteenth largest city in the United States. It has a metropolitan area population of over 4,500,000, the thirteenth largest in the country. U.S. CENSUS BUREAU, ANNUAL ESTIMATES OF THE RESIDENT POPULATION: APRIL 1, 2010 TO JULY 1, 2017 [hereinafter U.S. CENSUS BUREAU, ANNUAL ESTIMATES], https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml (last visited Nov. 21, 2018).

economy[122] and a lower crime rate than most medium-size U.S. cities.[123] The City has not experienced a large-scale terrorist act involving major loss of life or serious property damage, although several smaller terrorist incidents have occurred.[124] Thus, for most residents, life in Seattle is not colored by a fear of crime or terrorist attacks nor has the Seattle Police Department (SPD) implemented heightened security measures designed to prevent or respond to such attacks.

Although Seattle's elected offices are officially non-partisan, the city is staunchly liberal with a heavy Democratic tilt.[125] Washington State has a roughly even divide between Democrats and Republicans, but Democrats control the governor's office, the State House of Representatives, and the State Senate.[126] In a recent study calculating the level of conservatism of all U.S. cities with a population above 20,000, Seattle ranked as the third most liberal city.[127]

In Seattle, the mayor appoints the chief of police, who serves at the mayor's pleasure.[128] The SPD is relatively small, with approximately 1,400 sworn officers (about twenty officers per 10,000 residents) and a 2016 budget of about $320 million out of a total citywide budget of $5.1 billion.[129] It has a mixed history with privacy protection/regulation.

---

122. The city/region is home to major high-tech and aerospace firms such as Amazon, Microsoft, Starbucks, and Boeing, the fifth largest U.S. container port, and a globally recognized public university, the University of Washington. *See* Gregory Lewis McNamee, *Seattle, Washington, United States*, ENCYCLOPEDIA BRITANNICA (last updated Oct. 4, 2018), https://www.britannica.com/place/Seattle-Washington [https://perma.cc/X2D5-HHET].

123. *See Violent Crime Statistics for Every City in America*, CBS CHI. (Oct. 22, 2015, 5:00 PM), https://chicago.cbslocal.com/2015/10/22/violent-crime-statistics-for-every-city-in-america/ [https://perma.cc/Y7YJ-W6CN].

124. OFFICE OF EMERGENCY MGMT., CITY OF SEATTLE, SHIVA – THE SEATTLE HAZARD IDENTIFICATION AND VULNERABILITY ANALYSIS (2014), https://www.seattle.gov/Documents/Departments/Emergency/PlansOEM/SHIVA/SHIVAv6.3Final.pdf [https://perma.cc/f5zx-jv7g].

125. *Here's How Seattle Voters' Support for Trump Compared to other Cities'*, SEATTLE TIMES (Nov. 17, 2016, 6:45 AM), https://www.seattletimes.com/seattle-news/politics/heres-how-seattle-voters-support-for-trump-stacks-up-to-other-u-s-cities/ (last visited Oct. 21, 2018) (eighty-seven percent of Seattle voters supported Clinton over Trump in the 2016 election).

126. *See* Jennifer Bendery, *Democrats in Washington State Win Full Control of the Government*, HUFFPOST (Nov. 7, 2017, 11:33 PM), https://www.huffingtonpost.com/entry/washington-state-senate-special-election_us_5a00a45be4b0baea2633bfae [https://perma.cc/SPR4-CYCL].

127. *See* Chris Tausanovitch & Christopher Warshaw, *Representation in Municipal Government*, 108 AM. POL. SCI. REV. 605, 609 (2014) (basing rankings on recent large-scale population surveys regarding public policy).

128. SEATTLE POLICE DEP'T, CITY OF SEATTLE, 2017–2018 PROPOSED BUDGET 369, https://www.seattle.gov/financedepartment/17proposedbudget/documents/SPD.pdf [https://perma.cc/32H8-Y2XX] (overview of the Seattle Police Department).

129. CITY OF SEATTLE, 2016 PROPOSED BUDGET 15,

On the one hand, the SPD is more transparent than most American police forces. For example, the SPD police manual is publicly available on the internet and it covers departmental standards, values, policies, and practices across a range of operational and personnel issues.[130] On the other hand, the SPD has some history of misconduct involving surveillance and use of force. Notable incidents include spying on political protests in the 1960s and 1970s[131]; inadequately preparing for the 1999 World Trade Organization meeting in Seattle, where 100,000 protestors disrupted the conference and engaged in minor rioting[132]; using a stun gun on a seven-months-pregnant African-American woman after she was stopped for going twelve miles over the speed limit and refused to get out of her car or sign her speeding ticket[133]; and two racially-charged use-of-force incidents in 2010, one involving a fatal shooting of a Native American experiencing a mental health crisis,[134] the other involving the kicking, beating, and berating of two handcuffed Latino suspects.[135]

In 2011, the DOJ announced an investigation of the SPD based in part on these widely publicized incidents.[136] The investigation found that the SPD routinely used excessive force and followed policing practices that

---

http://www.seattle.gov/financedepartment/16proposedbudget/documents/16proposedbudgetexecsummary.pdf [https://perma.cc/WKL4-HM5S].

130. SEATTLE POLICE DEP'T, CITY OF SEATTLE, SEATTLE POLICE DEPARTMENT MANUAL (2018) [hereinafter SEATTLE POLICE DEPARTMENT MANUAL], https://www.seattle.gov/police-manual [https://perma.cc/YA7Z-78T2]; *see* Friedman & Ponomarenko, *supra* note 119, at 1848 (identifying Chicago and Seattle as among the few cities with publicly available police manuals).

131. Michael Sweeney, *Seattle Law Limits Police in Intelligence Gathering*, WASH. POST (July 3, 1979), https://www.washingtonpost.com/archive/politics/1979/07/03/seattle-law-limits-police-in-intelligence-gathering/916c9159-31da-4a1f-ab55-9804ba5efa19/?utm_term=.d842564b88e8 [https://perma.cc/7T8F-6ZSN].

132. *See* Sam Howe Verhovek, *Seattle Police Chief Resigns in Aftermath of Protests*, N.Y. TIMES (Dec. 8, 1999), http://www.nytimes.com/1999/12/08/us/seattle-police-chief-resigns-in-aftermath-of-protests.html (last visited Oct. 21, 2018).

133. Adam Liptak, *A Ticket, 3 Taser Jolts and, Perhaps, a Trip to the Supreme Court*, N.Y. TIMES (May 14, 2012), http://www.nytimes.com/2012/05/15/us/police-taser-use-on-pregnant-woman-goes-before-supreme-court.html (last visited Oct. 21, 2018).

134. *See* Lynda V. Mapes, *Carver's Death a Violent End to a Tormented Life*, SEATTLE TIMES (Oct. 15, 2010, 10:00 PM), https://www.seattletimes.com/seattle-news/carvers-death-a-violent-end-to-a-tormented-life/ (last visited Oct. 21, 2018).

135. *See* Steve Miletich & Sara Jean Green, *Video of SPD Officer Kicking Prone Man Sparks Internal Investigation*, SEATTLE TIMES (May 8, 2010, 11:25 PM), https://www.seattletimes.com/seattle-news/video-of-spd-officer-kicking-prone-man-sparks-internal-investigation/ (last visited Oct. 21, 2018).

136. *See* Mike Carter, *Justice Department to Investigate Seattle Police Civil-Rights Practices*, SEATTLE TIMES (Mar. 31, 2011, 9:22 PM), https://www.seattletimes.com/seattle-news/justice-department-to-investigate-seattle-police-civil-rights-practices/ (last visited Oct. 21, 2018).

could lead to discriminatory or biased policing.[137] Although the City of Seattle initially objected to these findings, in 2012 it entered into a consent decree requiring the city to adopt new policies and provide training designed to address excessive force.[138] Five years later, the federal monitor overseeing court-ordered police reforms praised the SPD for achieving a dramatic turnaround but then refused to find the police department in compliance with its federally mandated obligations, due in part to a June 2017 incident in which two white officers fatally shot Charleena Lyles, a thirty-year-old African-American mother of four.[139] The city objected, and six months later, James Robart, a federal district court judge in Seattle, found the SPD in "full and effective compliance" with the court-ordered police reforms.[140]

1. Seattle's Surveillance Ordinances and Body Camera Policy

The 2013 Ordinance—In 2013, the Seattle City Council approved a bill and ordinance requiring city departments to obtain council approval prior to acquiring and using certain surveillance equipment.[141] One explicit goal of the ordinance—which was the first of its kind in the country—was "to avoid creating a constant and pervasive surveillance

---

137. CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE SEATTLE POLICE DEPARTMENT 2 (2011), https://www.justice.gov/sites/default/files/crt/legacy/2011/12/16/spd_findletter_12-16-11.pdf [https://perma.cc/TK6L-S7TS].

138. The Consent Decree

> calls for the restoration of constitutional policing through substantial and far-reaching reform of the SPD's use of force policies and practices, training, full and complete implementation of new policy, adoption of policies and training to eliminate discriminatory policing, and the development of improved relations, trust, and support among and from all of Seattle's many and varied communities.

Seattle Consent Decree: How It Came About, What It Is, and What the Monitor Does, SEATTLE POLICE MONITOR (2017), http://www.seattlemonitor.com/overview/ [https://perma.cc/9S5R-7HVD].

139. Steve Miletich, *Despite Progress, Seattle Police Not Yet in Compliance with Reforms, Federal Monitor Says*, SEATTLE TIMES (Sept. 8, 2017, 4:24 PM), http://www.seattletimes.com/seattle-news/crime/despite-progress-seattle-police-not-yet-in-compliance-with-reforms-federal-monitor-says/ (last visited Oct. 21, 2018). *But see* Steve Miletich, *Seattle Police Dispute Monitor's Report, Say They've Met Federal Reform Standards*, SEATTLE TIMES (Sept. 12, 2017, 3:37 PM), http://www.seattletimes.com/seattle-news/crime/seattle-police-dispute-monitors-report-say-theyve-met-federal-reform-standards/ (last visited Oct. 21, 2018).

140. Steve Miletich, *Seattle Asks Federal Judge to Find It in Compliance with Court-Ordered Police Reforms*, SEATTLE TIMES (Sept. 29, 2017, 12:40 PM), https://www.seattletimes.com/seattle-news/in-watershed-moment-seattle-asks-federal-judge-to-find-it-in-compliance-with-court-ordered-reforms/ (last visited Oct. 21, 2018).

141. *See* SEATTLE, WASH., ORDINANCE 124142 (Mar. 18, 2013) (codified at SEATTLE, WASH. MUN. CODE § 14.18) [hereinafter SEATTLE SURVEILLANCE ORDINANCE], http://clerk.seattle.gov/~scripts/nph-brs.exe?d=ORDF&s1=117730.cbn.&Sect6=HITOFF&l=20&p=1&u=/~public/cbor1.htm&r=1&f=G [https://perma.cc/QHM2-U2HW].

presence in public life."[142] Relying on a consensus approach, the coalition of privacy advocates who initially sought the ordinance collaborated with representatives of the mayor, police chief and county prosecutor, all of whom were represented on the drafting committee that eventually wrote the law.[143]

The city council adopted the surveillance equipment ordinance following negative media reports and a public outcry in response to two incidents: the city's secretive acquisition of two small drones and its installation of surveillance cameras (along with a "mesh network") at Seattle's waterfront.[144] Both were funded by a $5 million federal grant.[145] The SPD behaved secretively in both cases by failing to consult with or notify the city council or the public prior to acquiring or installing the equipment.[146]

The ordinance required SPD and other city agencies to obtain council approval before deploying "surveillance equipment."[147] More specifically, it obligated the SPD to develop operational and data management protocols for all such equipment.[148] The operational protocols addressed the proper deployment, acquisition, and use of the equipment including information on its purpose, type, specific location, and use; its effect on privacy and anonymity rights and how any potential abuses of these rights would be mitigated; a description of data collection practices (including the extent of any real-time monitoring and how data would be used, accessed, retained and shared with other city departments); and a public outreach plan for affected communities.[149] The data management protocols required the SPD to submit written protocols addressing, at a more granular level, how data collected by the surveillance equipment would be retained, stored, indexed, and accessed.[150]

---

142. *Id.*

143. Sweeney, *supra* note 131.

144. Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES (Feb. 7, 2013, 9:33 PM), http://seattletimes.com/html/localnews/2020312864_spddronesxml.html (last visited Oct. 21, 2018); Christine Clarridge, *Waterfront Surveillance Cameras Stir Privacy Fears*, SEATTLE TIMES (Jan. 31, 2013, 8:45 PM), http://seattletimes.com/html/latestnews/2020260670_waterfrontcamerasxml.html (last visited Oct. 21, 2018).

145. Clarridge, *Waterfront Surveillance Cameras Stir Privacy Fears*, *supra* note 144.

146. Crump, *supra* note 23.

147. SEATTLE SURVEILLANCE ORDINANCE, *supra* note 141.

148. *Id.*

149. *Id.*

150. *Id.*

The 2013 surveillance ordinance represented a big step by the SPD toward transparency and accountability in public surveillance. But it had shortcomings, too. First, it defined "surveillance equipment" very narrowly, covering "drones or unmanned aircraft and any attached equipment used to collect data" but excluding many other types of equipment such as body-worn cameras, traffic cameras, and security cameras.[151] Second, the city council adopted a last-minute proposal by the SPD to significantly widen an exemption for using surveillance equipment for purposes of criminal investigations under exigent circumstances.[152] This change expanded the exemption to cover investigations supported by reasonable suspicion.[153] Third, and most importantly, the 2013 ordinance lacked any enforcement mechanism that would impose specific penalties on the SPD if it failed to seek approval or submit the required protocols in a timely fashion.[154] And that is exactly what happened.

The 2017 Ordinance—In the spring of 2017, a combination of media exposure and revived public backlash led the city council to reconsider the effectiveness of the 2013 ordinance and begin work on replacing it. The SPD had purchased and begun using a social media tracking tool called Geofeedia, without seeking approval by the city council or submitting the required protocols.[155] This controversial decision illustrated the lack of clarity over the scope of the 2013 ordinance and

---

151. *Id.* The Seattle Police Department Manual addressed a few of these scenarios but mainly from an operational standpoint. *See* SEATTLE POLICE DEPARTMENT MANUAL, *supra* note 130, at ch. 16.090 (in car video system); *id.* ch. 16.091 (body-worn video pilot program); *id.* ch. 16.170 (automatic license plate readers).

152. Phil Mocek, *Updates to Seattle Surveillance Equipment Bill*, MOCEK.ORG (Mar. 15, 2013), https://mocek.org/blog/2013/03/15/updates-to-seattle-surveillance-equipment-bill/ [https://perma.cc/9HQY-N3S2]; Phil Mocek, *Seattle City Council Pass Ordinance Restricting Surveillance Equipment After Councilmember Harrell Slips in a Gift for Police*, MOCEK.ORG (Mar. 19, 2013), https://mocek.org/blog/2013/03/19/seattle-passes-ordinance-restricting-surveillance-after-harrell-slips-in-gift-for-police/ [https://perma.cc/VS7H-4BE6].

153. SEATTLE SURVEILLANCE ORDINANCE, *supra* note 141. For a detailed account of how this came to pass, see Phil Mocek, *Updates to Seattle Surveillance Equipment Bill*, *supra* note 152; Phil Mocek, *Seattle City Council Pass Ordinance Restricting Surveillance Equipment After Councilmember Harrell Slips in a Gift for Police*, *supra* note 152.

154. *See* Press Release, ACLU Wash., ACLU Urges City Council to Put Teeth into Surveillance Law, Delay Vote to Add Auditing Process (Mar. 18, 2013), https://www.aclu-wa.org/news/aclu-urges-city-council-put-teeth-surveillance-law-delay-vote-add-auditing-process [https://perma.cc/ZU9Y-GD3U].

155. Ansel Herz, *How the Seattle Police Secretly—and Illegally—Purchased a Tool for Tracking Your Social Media Posts*, STRANGER (Sept. 28, 2016), https://www.thestranger.com/news/2016/09/28/24585899/how-the-seattle-police-secretlyand-illegallypurchased-a-tool-for-tracking-your-social-media-posts [https://perma.cc/F2QX-PHUZ].

whether it applied only to hardware or to software as well. An SPD spokesperson told a local newspaper that the Geofeedia purchase "'should have been cleared . . . in accordance with the Seattle Municipal Code'"[156] (i.e., the surveillance equipment ordinance), while a local TV station reported that according to sources inside the police department, "the [surveillance equipment ordinance] applies only to hardware like cameras, not software like Geofeedia."[157] A few weeks later, the ACLU of Northern California blogged that it had obtained records showing that Twitter, Facebook, and Instagram provided user data access to Geofeedia, and that Facebook and Instagram had already cut off Geofeedia's access to company data.[158] In any case, the SPD clearly did not seek approval from the city council or develop any of the required protocols in this case or—quite possibly—in any other case involving covered surveillance equipment between 2013 and 2017.

In developing a new ordinance, the City Council convened a stakeholder working group consisting of council staff, key staff from the mayor's office, the city IT and law departments, and the SPD, along with advocacy groups led by the ACLU-WA. The group met over the course of several months to discuss and revise a draft ordinance developed by the ACLU-WA.[159] The revised ordinance, which the mayor signed into law on August 2, 2017,[160] repealed and replaced the 2013 ordinance, changing it in a number of ways, several of which are worth highlighting.

To begin with, the new ordinance jettisons "surveillance equipment" in favor of two newly defined terms: "surveillance technology," broadly defined as "any electronic device, software program, or hosted software

---

156. *Id.*

157. *See* Essex Porter, *OPA Investigates Reported SPD Acquisition of Tool that Tracks Social Media Posts*, KIRO 7 (Sept. 29, 2016, 8:18 PM), http://www.kiro7.com/news/local/opa-investigates-reported-spd-acquisition-of-tool-that-tracks-social-media-posts/451898379 [https://perma.cc/F4EG-DBYL].

158. *See* Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU OF N. CAL. (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target (last visited Nov. 11, 2018). Twitter soon followed. *See* Ally Marotti & Tribune News Servs., *Twitter Cuts off Chicago Startup Geofeedia After ACLU Reports Police Surveillance*, CHI. TRIBUNE (Oct. 11, 2016, 12:05 PM), http://www.chicagotribune.com/bluesky/originals/ct-twitter-suspends-geofeedia-access-bsi-20161011-story.html [https://perma.cc/NC5K-LPHE].

159. Email from Mary F. Perry, Dir. of Transparency & Privacy, Seattle Police Dep't to Ira Rubinstein, Senior Fellow, Info. Law Inst., NYU (Sept. 11, 2017, 9:21 AM) (on file with author); Memorandum from Amy Tsai to Gender Equity, Safe Cmtys. & New Ams. Comm. (June 28, 2017), http://seattle.legistar.com/View.ashx?M=F&ID=5285300&GUID=80E7C8BB-BAA2-4975-BED5-BE523C258367 [https://perma.cc/NE4N-TJD3].

160. SEATTLE, WASH. MUN. CODE § 14.18 (amended 2017).

solution that is designed or primarily intended to be used for the purpose of surveillance," subject to various exceptions and exemptions that resemble those in place under the 2013 ordinance[161]; and "surveillance data," defined as "any electronic data collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology acquired by the City or operated at the direction of the City."[162] This revision significantly broadens the scope of the ordinance. Indeed, the definition of "surveillance data" was among the most hotly debated issues in the city council hearings. The SPD objected that an overly broad definition would render the ordinance unworkable.[163] The ACLU-WA worried that a narrow definition would undermine transparency and accountability.[164] In the end, the city council split the difference by linking "surveillance data" to technology "acquired by the City or operated at the direction of the City."[165]

The 2017 ordinance also imposes a new obligation on departments filing surveillance impact reports to conduct community outreach prior to council approval.[166] And it narrows the exigent circumstances exception, which previously allowed temporary use of surveillance equipment in advance of council approval based on a criminal investigation supported by reasonable suspicion, but now requires a showing of imminent risk of death or serious injury.[167] This is a much higher standard. Finally, the ordinance adds several new oversight and enforcement provisions including a private right of action against the city for injunctive or declaratory relief for any material violation of the new bill, after a ninety-day opportunity for the city department to address the concern.[168] As a practical matter, however, a requirement that all city departments create an inventory of existing surveillance technologies and process them for

161. *Id.* § 14.18.010.

162. *Id.*

163. *See infra* text following note 355 for further discussion.

164. *See Seattle Adopts Nation's Strongest Regulations for Surveillance Technology*, ACLU WASH. (Aug. 8, 2017), https://www.aclu-wa.org/news/seattle-adopts-nation%E2%80%99s-strongest-regulations-surveillance-technology [https://perma.cc/JLN3-T3CK]. Presumably, this excludes data acquired by the city from independent sources such as DHS or state and local agencies sharing surveillance data with a regional fusion center. Although the ACLU praised the final bill, it also called upon the council to enact a future ordinance ensuring that Seattle's acquisition and sharing of surveillance data is fully regulated, citing the vulnerability of immigrants and refugees to federal enforcement if there are inadequate controls on data sharing. *Id.*

165. SEATTLE, WASH., MUN. CODE § 14.18.010.

166. *Id.* § 14.18.020(C).

167. *Id.* § 14.18.030(C)(1).

168. *Id.* §§ 14.18.060–.070.

council approval at a rate of at least one per month[169] may prove even more burdensome than potential lawsuits depending on the number of such technologies, which may be very high in light of the broader definitions discussed above.

The ACLU-WA praised the replacement ordinance as "the strongest measure adopted by an American city to regulate the acquisition of surveillance technology."[170] In fact, the new Seattle ordinance compares very favorably with strong measures recently adopted in Santa Clara County, California[171] and in Oakland.[172] There is little reason to analyze these ordinances at length because Seattle borrowed from them extensively.

The Body Camera Policy—Seattle has also moved ahead with plans to improve public safety and enhance police accountability by requiring patrol officers to wear body cameras.[173] Both policymakers and advocacy groups believe that body cameras, if properly deployed, can help protect the public against police misconduct and the police against false accusations of abuse.[174] Police use of body cameras raises several difficult policy issues. These include where to set the limits on police discretion over when to record; the privacy interests of victims, suspects, third-parties, and the police; whether to use body cameras inside the home and other private spaces; and how to apply the FIPs to the retention, disclosure, and secondary uses of body camera video footage.[175] In comparison with the locally-negotiated surveillance ordinance, the city did not have as free a hand in resolving these issues locally. Rather, state

169. *Id.* § 14.18.070(3).

170. *Seattle Adopts Nation's Strongest Regulations for Surveillance Technology*, ACLU WASH., *supra* note 165.

171. SANTA CLARA CTY., CAL., OR. NS-300.897 (2016) (codified at SANTA CLARA CTY. ORD. CODE § A40); *see* Kevin Forestieri, *Santa Clara County Cracks Down on Police Surveillance Technology: New Law Aims to Increase Transparency and Public Control over Police Tech*, PALO ALTO ONLINE (June 20, 2016, 7:34 AM), https://www.paloaltoonline.com/news/2016/06/18/county-cracks-down-on-police-surveillance-technology [https://perma.cc/LZY8-BBAG].

172. Cyrus Farivar, *Oakland Passes "Strongest" Surveillance Oversight Law in US*, ARS TECHNICA (May 3, 2018, 1:00 AM), https://arstechnica.com/tech-policy/2018/05/oakland-passes-strongest-surveillance-oversight-law-in-us/ [https://perma.cc/YEU9-UGS8].

173. Jennifer Sullivan, *SPD to Test Body Cameras on a Dozen Officers*, SEATTLE TIMES (Sept. 24, 2014, 9:37 PM), https://www.seattletimes.com/seattle-news/spd-to-test-body-cameras-on-a-dozen-officers/ (last visited Oct. 25, 2018).

174. *See generally* Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All*, ACLU (Oct. 2013), https://www.aclu.org/files/assets/police_body-mounted_cameras.pdf [https://perma.cc/D573-N6C9].

175. *Id.*

legislation and the federal courts both greatly influenced the body camera policies Seattle eventually adopted.

The SPD began experimenting with body cameras in 2014 with a small pilot program involving a dozen officers.[176] Immediately it had to contend with two thorny issues under state law: whether the use of body cameras violated Washington State's all-party consent rule and whether body camera footage would be accessible to the public under Washington's very expansive public disclosure law.

The Washington Privacy Act requires that all parties to a private conversation must consent to an audio recording, although it also states that the consent obligation may be satisfied if any of the parties announces that they will be recording the conversation in a reasonable manner so long as the recording contains that announcement.[177] The SPD circumvented this problem by initially recording only video and not audio.[178] An advisory opinion from the Washington State Office of the Attorney General later clarified that the "Washington Privacy Act does not require officer consent because the Washington [State] Supreme Court has recognized that a conversation between a police officer and a member of the public that occurs in the performance of the officer's duties is not private."[179]

Washington's Public Records Act (PRA) creates a presumption of "full access to information concerning the conduct of every level of government" and generally trumps other laws that conflict with its open-access mandate.[180] The PRA recognizes the right to privacy as a possible exemption from disclosure but defines the right very narrowly[181] and imposes a policy of construing all exemptions narrowly.[182] Thus, the Washington State Supreme Court held in *Fisher Broadcasting Seattle TV*

176. Sullivan, *supra* note 173.

177. WASH. REV. CODE § 9.73.03(3) (2018).

178. Sullivan, *supra* note 173.

179. Wash. Att'y Gen. Op. No. 8, Video and Audio Recording of Communications Between Citizens and Law Enforcement Officers Using Body Cameras Attached to Police Uniforms (Nov. 24, 2014), http://www.atg.wa.gov/ago-opinions/video-and-audio-recording-communications-between-citizens-and-law-enforcement-officers [https://perma.cc/Q8Q3-YFQ6]. The clear majority of states follow a "one-party consent" rule so this is not an issue in these jurisdictions. *See, e.g.*, N.Y. PENAL LAW §§ 25.00–.05 (McKinney 2017).

180. *See* Nissen v. Pierce County, 183 Wash. App. 581, 589–90, 333 P.3d 577, 581–82 (2014) (citing Neighborhood All. of Spokane Cty. v. Spokane Cty., 172 Wash. 2d 702, 714–15, 261 P.3d 119, 125–26 (2011)).

181. WASH. REV. CODE § 42.56.050.

182. *Id.* § 42.56.030; *see, e.g.*, Bldg. Indus. Ass'n of Wash. v. Wash. Dep't of Labor & Indus., 123 Wash. App. 656, 662, 98 P.3d 537, 541 (2004).

LLC v. City of Seattle[183] that police body camera footage in Washington is generally subject to disclosure under the PRA.[184] And this remains the rule even when gross privacy violations may result from the release of unredacted footage.[185] Indeed, Washington's PRA allows requests for police video that are "both anonymous and massively broad."[186] This policy almost halted the SPD pilot program before it even began.

In September 2014, a local programmer named Tim Cleamans filed an anonymous request for "every single video" the SPD ever recorded.[187] SPD's legal advisor on PRA issues, Mary Perry—who had argued and lost *Fisher Broadcasting*—concluded that the under this ruling the police could withhold video footage only in cases under pending litigation.[188] If acted on, Cleamans's request would have been a financial and logistical nightmare. After all, the PRA still required the SPD to review and redact video footage under any applicable privacy exemptions before releasing it and at that time the process was "manual, a painstaking, frame-by-frame ordeal."[189] Eventually, the SPD approached Cleamans and the two sides reached an informal détente in which Cleamans agreed to withdraw his request if the SPD would automatically redact body camera footage and make it available online.[190] With Cleamans's help, the SPD then sponsored a "hackathon" to refine the automated redaction system and launched a YouTube channel featuring footage from the pilot program, with the images automatically blurred and the audio muted.[191] The SPD hired Cleamans as a consultant for six months but after a dispute he resigned and immediately wrote a program for automating requests for the footage, enabling him to file over 2,000 requests over the next year.[192]

---

183. 180 Wash. 2d 515, 326 P.3d 688 (2014).

184. *Id.* at 535, 326 P.3d at 698 (requiring agencies to justify non-disclosure of video on a case-by-case basis).

185. *See* McKenzie Funk, *Should We See Everything a Cop Sees?*, N.Y. TIMES (Oct. 18, 2016), https://www.nytimes.com/2016/10/23/magazine/police-body-cameras.html?_r=0 (last visited Oct. 27, 2018) (describing one such example involving video footage of a woman apparently overdosing on meth, claiming she is pregnant, and being restrained and administered medical aid).

186. Mark Harris, *The Body Cam Hacker Who Schooled the Police*, WIRED (May 22, 2015), https://www.wired.com/2015/05/the-body-cam-hacker-who-schooled-the-police/ [https://perma.cc/5JGZ-KHUA].

187. *See* Funk, *supra* note 185.

188. *Id.*

189. *Id.* (noting that the SPD "was then sitting on more than 1.5 million individual dashcam and surveillance videos, or about 300,000 hours and 350 terabytes total").

190. *Id.*

191. *Id.*; *see also S.P.D. BodyWornVideo*, YOUTUBE, https://www.youtube.com/channel/UCcdSPRNt1HmzkTL9aSDfKuA [https://perma.cc/94PA-9D62].

192. Funk, *supra* note 185. Cleamans also persisted in uploading unredacted video footage to

Meanwhile, in 2015, the federal monitor appointed by Judge Robart to oversee Seattle police reforms endorsed the use of body cameras by officers, calling them a key tool for accountability and transparency.[193] Thereafter, the SPD conducted a six-month pilot program to evaluate body camera technology and equipment during field use.[194] In consultation with officers who had participated in the pilot and community stakeholders, it developed a policy regulating both in-car and body-worn video. In 2015 and again in 2016, the Seattle City Council imposed a proviso to the city budget that would not be lifted until the Council was satisfied that the SPD had engaged in an extensive community outreach process regarding this policy. In January 2017, the Council removed the proviso following the SPD's completion of agreed-upon outreach efforts.[195] The SPD then submitted a draft body camera policy to the Council addressing some of the stakeholder concerns discussed during the outreach events.[196]

On May 3, 2017, Judge Robart approved this policy over the objections of the ACLU-WA and others.[197] The ACLU noted a "confusion of purpose" in the SPD policy: was the goal police accountability or evidence-gathering for criminal prosecution? Clearly the two differ and may diverge. In addition, they argued that the police retained too much discretion to turn cameras on and off. Finally, they pointed to the risk that that body cameras might become a generalized surveillance tool rather than an accountability measure, with predictable results.[198]

By this point in the SPD rollout, the Washington State Legislature had provided some temporary relief to Seattle and other cities facing massive public record requests by (1) amending the PRA to exempt body camera video recordings from disclosure if nondisclosure was essential for the

---

YouTube, including some highly invasive and embarrassing scenes of the police interviewing a sex worker who reveals her name, address, email address, and telephone number in the video.

193. Steve Miletich, *Time for SPD Officers to Wear Body Cameras 'Is Now,' Federal Monitor Says*, SEATTLE TIMES (June 16, 2015, 4:07 PM), https://www.seattletimes.com/seattle-news/time-for-spd-officers-to-wear-body-cameras-is-now-federal-monitor-says/ (last visited Oct. 27, 2018).

194. *See* Memorandum from Amy Tsai, Council Staff, to Gender Equity, Safe Cmtys. & New Ams. Comm. (Feb. 22, 2017) (on file with author).

195. *Id.*

196. The draft policy is reprinted in the Tsai Memorandum, while the final policy is now available in the SPD Manual. *Id.*; *see* SEATTLE POLICE DEPARTMENT MANUAL, *supra* note 130, at § 16.090.

197. Steve Miletich, *Federal Judge Approves Body-Camera Plan for Seattle Police*, SEATTLE TIMES (May 4, 2017, 5:29 PM), https://www.seattletimes.com/seattle-news/crime/federal-judge-approves-body-camera-plan-for-seattle-police/ (last visited Oct. 27, 2018).

198. *See* Shankar Narayan, *Police Body-Worn Cameras: Not a Panacea*, 71 NW. LAW. 32, 34 (2017).

protection of a person's privacy, and (2) creating a presumption that disclosure of certain recordings is offensive to a reasonable person in various sensitive settings or situations (home interiors, medical facilities, an "intimate" image, a minor, and so on).[199] The amendments also made it much harder to request video footage in bulk.[200]

This temporary fix (most of these provisions will expire in 2019) also requires that any law enforcement agency deploying body cameras adopt a policy addressing, at a minimum: (1) activation/deactivation requirements, and officer discretion in this regard; (2) how to respond to a person's unwillingness to communicate with an officer who is recording the communication; (3) requirements for documenting when and why a camera was deactivated prior to the conclusion of an interaction with a member of the public; (4) requirements for notifying a member of the public that he or she is being recorded, including instances where the person finds spoken English challenging; (5) training requirements on body camera usage; and (6) security rules to protect data collected and stored from body cameras.[201] However, the legislation neither settled the disputes over these contested issues nor established any specific substantive requirements. Rather, it created a "Task Force on Body Worn Cameras" to further examine police use of body cameras and submit its findings and recommendations to the governor and state legislature by December 1, 2017.[202] The Task Force's report included recommendations on some issues (such as clarifying the definition of "special exemptions" in the PRA, modifying the definitions of "intimate image" and "minors," and clarifying the retention requirement) but left other issues unresolved (such as whether to strike or retain the provision barring a PRA requestor who prevails in litigation over body camera video from recovering fees and statutory penalties unless the agency acted with bad faith or gross negligence).[203]

This left Seattle with one final issue to tackle: negotiating a new contract with the two SPD unions that had voiced concerns about the effects of a body camera program on patrol officers' working conditions,

---

199. *See* H.B. 2362, 64th Leg., Reg. Sess., 2016 Wash. Sess. Laws 780 (2016).

200. *See generally* WASH REV. CODE § 42.56.240(14) (2018).

201. Wash. H.B. 2362 § 5.

202. JOINT LEGISLATIVE TASK FORCE ON THE USE OF BODY WORN CAMERAS, COMMITTEE REPORT AND RECOMMENDATIONS (2017), http://leg.wa.gov/JointCommittees/Archive/UBWC/Documents/UBWC-FinalRpt.pdf [https://perma.cc/M5S2-ABE4].

203. *Compare id.* at 1–23, *with* Letter from Shankar Narayan, Tech. and Liberty Project Dir., ACLU Wash., to Joint Legislative Task Force (Dec. 15, 2017) (printed in COMMITTEE REPORT, *supra* note 202, at 31).

discipline, and privacy.[204] But rather than delaying full deployment of the body cameras pending completion of union negotiations, in July 2017, then Seattle Mayor Ed Murray issued an executive order calling for deployment of body cameras to all patrol officers in downtown Seattle by September 30, 2017, and a citywide roll-out thereafter.[205] Although the executive order stated that collective bargaining with the police unions would continue prior to and after implementation of the court-approved program, this riled the Seattle police officers' union, leading it to file an unfair labor practice complaint that is still pending as of this writing.[206]

2. Seattle's Privacy Program

The Privacy Initiative—In 2014, Seattle launched a Privacy Initiative aimed at providing greater transparency into the city's data collection and use practices.[207] Moving beyond the narrow focus of the surveillance ordinance, this new initiative sought to ensure that the city took "appropriate steps to facilitate the collection, use, and disposal of data in a manner that balances the needs of the City to conduct its business with individual privacy, in a manner that builds public trust."[208] As part of the Privacy Initiative, Mayor Murray convened a group of stakeholders from across city departments (including the SPD) to establish a set of governing principles, devise an approach to educating city departments on privacy

---

204. Steve Miletich, *Rebuffing Union, Mayor Murray Orders Seattle Police to Begin Wearing Body Cameras*, SEATTLE TIMES (July 18, 2017, 1:46 PM), https://www.seattletimes.com/seattle-news/crime/rebuffing-union-mayor-murray-orders-seattle-police-to-begin-wearing-body-cameras/ (last visited Oct. 27, 2018).

205. Seattle Mayor Exec. Order 2017-03 (July 17, 2017), http://murray.seattle.gov/wp-content/uploads/2017/07/EO-2017-03-body-worn-cameras.pdf [https://perma.cc/Q8LR-66GK]; *see also* Press Release, Office of the Mayor, Mayor Murray Signs Executive Order Requiring Body Cameras on Patrol Officers (July 17, 2017), http://murray.seattle.gov/mayor-murray-signs-executive-order-requiring-body-cameras-patrol-officers/ [https://perma.cc/43CT-FVGK].

206. Steve Miletich, *State Labor Board to Hear Seattle Police Complaint over Use of Body Cameras*, SEATTLE TIMES (Aug. 24, 2017, 8:52 PM), https://www.seattletimes.com/seattle-news/crime/state-labor-board-to-hear-seattle-police-complaint-over-use-of-body-cameras/ (last visited Dec. 2, 2018).

207. Press Release, Office of the Mayor, City of Seattle Launches Digital Privacy Initiative (Nov. 3, 2014), http://murray.seattle.gov/city-of-seattle-launches-digital-privacy-initiative/ [https://perma.cc/3LU9-S3TN]; *see also* Seattle City Council Res. 31570 (Feb. 23, 2015), http://clerk.seattle.gov/~archives/Resolutions/Resn_31570.pdf [https://perma.cc/TG7E-CZTT] (adopting citywide privacy principles).

208. Press Release, Office of the Mayor, City of Seattle Launches Digital Privacy Initiative, *supra* note 207; *see also* Angelique Carson, *Seattle Launches Sweeping, Ethics-Based Privacy Overhaul*, PRIVACY ADVISOR (Nov. 7, 2014), https://iapp.org/news/a/seattle-launches-citywide-privacy-initiative/ [https://perma.cc/H2FM-V6XY] (lauding the Seattle privacy initiative as one of the most progressive in the country).

practices, and determine how to assess compliance.[209] They were assisted by a Privacy Advisory Committee comprised of privacy researchers, practitioners, and community representatives, including privacy experts from the University of Washington and Microsoft.[210]

In 2015, the City released Privacy Principles governing its data collection and use practices.[211] This set of six principles provides an ethical framework for developing appropriate policies, standards, and practices regarding the public's personal information. They offer a local take on the FIPs and include (1) a statement valuing privacy; (2) collection limitations; (3) use limitations; (4) accountability; (5) disclosure limitations; and (6) accuracy.[212] The City also outlined a process for privacy reviews, consisting of a self-service assessment using a standardized questionnaire, then a privacy threshold analysis to be reviewed with a "Privacy Champion" appointed by each city department, followed by a full-scale privacy impact assessment.[213] Additionally, the city allocated resources in its 2016 budget to launch an online training and awareness program (required of anyone who interacts with the public's personal data), hire a full-time Chief Privacy Officer,[214] and adopt a citywide privacy statement that provides direction to all city departments about their obligations to follow the new principles, the privacy statement, and privacy review process.[215]

The Program's privacy policy specifically excludes surveillance technologies, as the city's surveillance ordinance already covers them.[216]

---

209. Press Release, Office of the Mayor, City of Seattle Launches Digital Privacy Initiative, *supra* note 207.

210. *Privacy Advisory Committee*, CITY OF SEATTLE, https://www.seattle.gov/tech/initiatives/privacy/privacy-advisory-committee [https://perma.cc/3JEW-SEBV].

211. Seattle City Council Res. 31570, *supra* note 207. The City of Seattle (along with the University of Washington) also joined a national network of university-city partnerships to work on "smart city" solutions, which was part of a Smart Cities Initiative under the Obama White House. *See Smart Cities – Seattle*, SMART CITIES LIBRARY, https://www.smartcitieslibrary.com/smart-cities-seattle/ [https://perma.cc/4CK9-FQDL].

212. DEP'T OF INFO. TECH., CITY OF SEATTLE, CITY OF SEATTLE PRIVACY PROGRAM 7 (2015) [hereinafter PRIVACY PROGRAM BROCHURE], http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf [https://perma.cc/J6N6-KBB5].

213. *Id.* at 8.

214. In May 2016, the city appointed its first Chief Privacy Officer, who has since been replaced. *See* Press Release, Seattle Information Technology, City of Seattle Hires Ginger Armbruster as Chief Privacy Officer (July 11, 2017) http://techtalk.seattle.gov/2017/07/11/city-of-seattle-hires-ginger-armbruster-as-chief-privacy-officer/ [https://perma.cc/RR3S-YGZD].

215. To date, Seattle has published nine PIAs. Its first PIA assesses a smart metering pilot project referred to as the Seattle City Light Advanced Metering Initiative (AMI). *See infra* text accompanying notes 362–67.

216. PRIVACY PROGRAM BROCHURE, *supra* note 212, at 35 (stating that data not falling under the

However, a year after announcing the Privacy Principles, the city began consolidating all information technology (IT) employees and tasks into a new IT department, with the goal of "establish[ing] consistent standards and priorities for IT investments" and protecting city resources against threats, "especially related to security and privacy risks."[217] This consolidation covers the IT activities of the SPD as well as civilian departments.[218] Thus, it would appear that all technologies acquired or used by the SPD are covered either by the revised surveillance ordinance or the city's Privacy Program.

The Open Data Program—Beginning in 2010 with its Open Data Program and *data.seattle.gov* portal, Seattle has led the nation in its embrace of public data sharing and open access datasets.[219] Former Mayor Murray expanded the program to all city agencies and departments in February 2016 when he announced a citywide Open Data Policy that makes all city data "open by preference"—meaning that the city favors making city data sets publicly available while reserving the right to withhold data if doing so would avoid harm to residents.[220] The 2016 executive order set limits on this default preference by making accessibility contingent on "screening for privacy and security considerations."[221] A year later, the city issued an Open Data Plan. One of the top five priorities in the plan was to complete a privacy risk assessment in partnership with the Future of Privacy Forum.[222]

The Future of Privacy Forum report speaks glowingly of Seattle's commitment to balancing privacy and transparency, while offering some recommendations for improvement.[223] Specifically, the report found that Seattle took seriously the risks of re-identification, data quality and accuracy, and bias, and that the city had "largely demonstrated that its

---

Program's protections included "[d]ata collection or use of technologies governed by the City's Surveillance Ordinance (SMC 14.18)").

217. *IT Consolidation*, CITY OF SEATTLE, https://www.seattle.gov/tech/initiatives/it-consolidation [https://perma.cc/M55W-A7SH].

218. *See* Colin Wood, *Seattle Begins Three-Year IT Consolidation*, GOV'T TECH. (Nov. 30, 2015), https://web.archive.org/web/20170824232241/http://www.govtech.com/Seattle-Begins-Three-Year-IT-Consolidation.html [https://perma.cc/D5BD-G8B4].

219. Seattle Mayor Exec. Order 2016-01 (Feb. 27, 2016), http://murray.seattle.gov/wp-content/uploads/2016/02/2.26-EO.pdf [https://perma.cc/8VZQ-PQLE].

220. *Id.*

221. *Id.*; *see also* FUTURE OF PRIVACY FORUM, CITY OF SEATTLE OPEN DATA RISK ASSESSMENT: JANUARY 2018 FINAL REPORT 6 (Jan. 2018) [hereinafter FPF SEATTLE OPEN DATA RISK ASSESSMENT].

222. SEATTLE INFO. TECH., CITY OF SEATTLE: 2017 OPEN DATA PLAN 8 (2017).

223. FPF SEATTLE OPEN DATA RISK ASSESSMENT, *supra* note 221.

procedures and processes to address privacy risks are fully documented and implemented."[224] While the report also suggested that Seattle could do more to formalize risk assessment of data sets and engage with privacy concerns during the data collection phase, the report concluded the City's Open Data Policy was "thoughtful and thorough" in its approach to protecting individual privacy and provided "a solid foundation for growth."[225]

B. New York City

New York City is the wealthy, thriving financial and cultural capital of the United States, if not the world. It is America's most populous city with an estimated 2017 population of over 8.6 million people.[226] Like Seattle, New York City has a lower crime rate than similarly-sized cities.[227] Indeed, the city now enjoys historically low crime rates.[228] In stark contrast with Seattle, where no major terrorist incidents have occurred, however, the September 11, 2001, attacks on New York City's World Trade Center (WTC) by the Islamist terrorist group al-Qaeda killed 2,753 people (including more than 400 first responders), injured thousands more, and caused an estimated $60 billion in damage to the WTC site, surrounding buildings, infrastructure, and subway facilities.[229] The attacks changed many things in the city, including how the NYPD understood its mission.[230] Following 9/11, then Police Commissioner Raymond A. Kelly quickly shifted NYPD resources from crime-fighting to counter-terrorism.[231] He established the first local Counter-Terrorism Bureau and expanded the existing Intelligence Bureau; he also recruited a Marine Corps general to run the former and a senior Central Intelligence Agency (CIA) official to take charge of the latter,[232] and created a controversial

224. *Id.* at 4.

225. *Id.* at 23–26. For a case study of open data in Seattle, see Whittington et al., *supra* note 23.

226. U.S. CENSUS BUREAU, ANNUAL ESTIMATES, *supra* note 121.

227. Jen Kirby, *New York City Had a Record-Low Crime Rate in 2016—But That's Not the Story in Other Cities*, N.Y. MAG: DAILY INTELLIGENCER (Jan. 4, 2017), http://nymag.com/daily/intelligencer/2017/01/new-york-city-had-record-low-crime-rate-in-2016.html [https://perma.cc/MJ8Z-L6UY].

228. Ashley Southall, *Crime in New York City Plunges to a Level Not Seen Since the 1950s*, N.Y. TIMES (Dec. 27, 2017), https://www.nytimes.com/2017/12/27/nyregion/new-york-city-crime-2017.html (last visited Oct. 27, 2018).

229. *9/11: Fast Facts About September 11*, CNN (Sept. 11, 2015, 1:56 PM), https://cw33.com/2015/09/11/911-fast-facts-about-september-11/ [https://perma.cc/3EY6-Z3XS].

230. KELLY, *supra* note 53, at 176.

231. *Id.*

232. *Id.* at 166, 171.

Demographics Unit, which was disbanded after being accused of spying on Muslim communities.[233] In his book, *Vigilance*, Kelly argues that these and related decisions helped to avert sixteen "active terror plots" during the almost twelve years of his second term as police commissioner.[234]

In New York City, the mayor appoints the chief of police, who serves at the mayor's pleasure.[235] The NYPD is the largest police force in the country, with over 36,000 sworn officers (about forty-two officers per 10,000 residents) and a 2016 budget of over $5 billion[236] out of a total city budget in 2016 of more than $80 billion.[237] Like Seattle, New York City is very liberal[238]; the state is less so.[239] Elected officials in New York City are partisan, and sometimes fiercely so, even between different factions of the same party. Although the present mayor, Bill de Blasio, is the first Democratic mayor since 1993,[240] he and Democratic Governor Andrew Cuomo do not always see eye to eye.[241]

The NYPD has a checkered history with respect to both political surveillance and biased policing. In 1981, the city settled a decade-long class action filed by members of various peace and black activist organizations alleging police infiltration of their groups and intimidation of, and spying on, their members.[242] The settlement decree outlined a

---

233. *See* Matt Apuzzo & Joseph Goldstein, *New York Drops Unit That Spied on Muslims*, N.Y. TIMES (Apr. 15, 2014), https://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html [https://perma.cc/2ZKQ-ZEPL].

234. KELLY, *supra* note 53, at 208–56 (discussing his 2002–2013 term).

235. N.Y. CITY CHARTER, § 431(a) (2018).

236. N.Y. CITY COUNCIL, REPORT ON THE FISCAL 2017 EXECUTIVE BUDGET: NEW YORK POLICE DEP'T 1–2 (May 23, 2016), http://council.nyc.gov/budget/wp-content/uploads/sites/54/2016/06/nypd.pdf [https://perma.cc/6Q8D-5VEJ].

237. Press Release, City of New York, Mayor de Blasio Releases FY 2017 Executive Budget (Apr. 26, 2016), http://www1.nyc.gov/office-of-the-mayor/news/396-16/fact-sheet-mayor-de-blasio-releases-fy-2017-executive-budget#/0 [https://perma.cc/TE29-QY7D].

238. Tausanovitch & Warshaw, *supra* note 127, at 609 fig.1 (identifying N.Y.C. as the eighth most liberal city in the country).

239. *See* N.Y. STATE BD. OF ELECTIONS, NYSVOTER ENROLLMENT BY COUNTY, PARTY AFFILIATION AND STATUS (Apr. 1, 2016), https://www.elections.ny.gov/NYSBOE/enrollment/county/county_apr16.pdf [https://perma.cc/PBK6-UE6W].

240. Michael Barbaro & David W. Chen, *De Blasio Is Elected New York City Mayor in Landslide*, N.Y. TIMES (Nov. 5, 2013), http://www.nytimes.com/2013/11/06/nyregion/de-blasio-is-elected-new-york-city-mayor.html (last visited Oct. 27, 2018).

241. Elizabeth Mitchell, *Cuomo vs. de Blasio: How a Friendly, Airtight Relationship Between the Democratic Heavyweights Turned Ugly. Is It Beyond Repair?*, DAILY NEWS (Oct. 29, 2016), http://interactive.nydailynews.com/2016/10/inside-the-cuomo-deblasio-feud/index.html (last visited Oct. 27, 2018).

242. Handschu v. Special Servs. Div., 605 F. Supp. 1384, 1417 (S.D.N.Y. 1985), *aff'd*, 787 F.2d 828 (2d Cir. 1986).

series of intelligence reforms known as the Handschu Guidelines, which imposed restrictions on political investigations and provided for civilian oversight of the NYPD's compliance. The settlement also created the Handschu Authority, a panel consisting of one civilian and two deputy commissioners, whose approval was required for investigations longer than thirty days.[243]

In 2003, the Southern District of New York agreed to modify the guidelines in the wake of the 9/11 terrorist attacks.[244] The 2003 Modified Handschu Guidelines, among other things, abolished the Authority's approval role and reduced its function to public complaint investigations and record reviews.[245] But this did not end the long-running controversy over NYPD spying on political (and religious) activity. In 2011, the Associated Press ran a series of articles demonstrating extensive NYPD surveillance and attempted infiltration of local Muslim communities and mosques,[246] which resulted in a new lawsuit and still further revisions to the modified guidelines.[247]

Nor have NYPD's stop-and-frisk practices fared well in the courts. In 2013, a federal judge found the practices unconstitutional, concluding that they violated New Yorkers' rights to be free from unreasonable searches and seizures and that the practices were racially discriminatory.[248] To remedy these violations, Judge Shira Scheindlin ordered a court-appointed monitor to oversee a series of reforms to NYPD policing practices and also created a mechanism for soliciting input from a variety of stakeholders, including the minority communities most directly affected by these practices. More recently, the court approved a pilot program that would outfit 1,200 police officers with body-worn cameras.[249]

---

243. *Id.* at 1420–24.

244. Handschu v. Special Servs. Div., 273 F. Supp. 2d 327, 349 (S.D.N.Y. 2003).

245. *Id.* at 350 (detailing modified guidelines approved by the court).

246. For a list of relevant references, see FRIEDMAN, *supra* note 67, at 377 n.4, 378 n.8.

247. David Kimball-Stanley, *Settling for More: The NYPD's New Oversight Deal*, LAWFARE (Mar. 8, 2017, 11:49 AM), https://www.lawfareblog.com/settling-more-nypds-new-oversight-deal [https://perma.cc/3E6Z-NRH6].

248. Joseph Goldstein, *Judge Rejects New York's Stop-and-Frisk Policy*, N.Y. TIMES (Aug. 12, 2013), http://www.nytimes.com/2013/08/13/nyregion/stop-and-frisk-practice-violated-rights-judge-rules.html (last visited Oct. 27, 2018).

249. Ashley Southall, *Judge Clears Way for Police Body Cameras in New York*, N.Y. TIMES (Apr. 21, 2017), https://www.nytimes.com/2017/04/21/nyregion/judge-police-body-cameras-new-york.html?_r=0 (last visited Oct. 27, 2018). For a discussion of the NYPD's body camera policy, see *infra* text accompanying note 279–304.

Finally, there have been dozens of NYPD incidents involving excessive use of force, including the July 2014 death of Eric Garner after a NYPD officer put him in a chokehold, an incident that was captured on a cell phone video showing Garner yelling "I can't breathe."[250] Three weeks later, a police officer in Ferguson, Missouri shot an unarmed black teenager named Michael Brown, leading to nationwide protests and the birth of the Black Lives Matter movement.[251]

1. New York City's Public Security Privacy Guidelines and Proposed Surveillance Ordinance

The DAS Guidelines—One of the steps Commissioner Kelly took to help protect New Yorkers against future terrorist attacks was creation of the DAS (Domain Awareness System), described above. The New York City Charter grants the NYPD plenary power to preserve order and enforce criminal law. The NYPD created the DAS by exercising that power, without need for any additional authority or direction by the city council.[252] However, the team responsible for developing and implementing the DAS anticipated that wide-scale police surveillance of public spaces would raise significant privacy concerns.[253] Accordingly, they released draft privacy guidelines for a thirty-day comment period in 2009,[254] and later that spring, published revised guidelines in final form.[255]

The DAS guidelines established policies and procedures serving two main goals: "to limit the authorized use of the Domain Awareness System and to provide for limited access to and proper disposition of stored data."[256] In keeping with the former, the guidelines prohibit targeting or

---

250. Al Baker et al., *Beyond the Chokehold: The Path to Eric Garner's Death*, N.Y. TIMES (June 13, 2015), https://www.nytimes.com/2015/06/14/nyregion/eric-garner-police-chokehold-staten-island.html (last visited Oct. 27, 2018).

251. Josh Hafner, *How Michael Brown's Death, Two Years Ago, Pushed #BlackLivesMatter into a Movement*, USA TODAY (Aug. 8, 2016, 7:50 PM), https://www.usatoday.com/story/news/nation-now/2016/08/08/how-michael-browns-death-two-years-ago-pushed-blacklivesmatter-into-movement/88424366/ [https://perma.cc/224Q-FAZA].

252. N.Y. CITY CHARTER § 435(a) (2018).

253. *See* N.Y. POLICE DEP'T, PUBLIC SECURITY PRIVACY GUIDELINES (2009) [hereinafter NYPD PRIVACY GUIDELINES], http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf [https://perma.cc/2VDT-FNMX].

254. N.Y. Police Dep't, Press Release, New York City Police Department Releases a Draft of the Public Security Privacy Guidelines for Public Comment (Feb. 25, 2009), http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/PressRelease-DraftPublicSecurityPrivacyGuidelines.pdf [https://perma.cc/mpr9-xjsl].

255. NYPD PRIVACY GUIDELINES, *supra* note 253.

256. *Id.* at 1.

monitoring by the DAS solely based on actual or perceived membership in protected categories, which are very broadly defined.[257] Additionally, while the DAS may be used to monitor public areas and activities "where no legally protected reasonable expectation of privacy exists," this must be limited to certain enumerated counter-terrorism purposes[258]; secondary uses beyond counterterrorism purposes and data sharing with a third-party require approval by a high ranking official.[259]

The DAS guidelines also adopt safeguards protecting the security of all sensitive data; limiting database access to authorized personnel who have received privacy training and signed a confidentiality agreement; and requiring the creation of an immutable data logs, which are subject to periodic compliance reviews by a NYPD integrity control officer.[260] Finally, data gathered via the DAS is typically destroyed at the end of an (unspecified) retention period for "routine review" unless further retention is approved (under unspecified criteria), and retention periods are established for different classes of data.[261]

The NYPD developed the DAS guidelines voluntarily using an informal version of notice-and-comment rulemaking.[262] This "rulemaking" procedure is hard to assess because there is no public record of the number of comments submitted, their content, or the NYPD's response. However, the comments of the Constitution Project are publicly available and give some idea of how civil libertarians viewed the DAS guidelines.[263]

The DAS guidelines take some important steps toward protecting privacy rights and civil liberties. While the NYPD deserves credit for developing the guidelines and even requesting comments, its informal approach to rulemaking only partially satisfies the City Administrative Procedure Act, which requires an agency proposing a rule to notify the public of the proposed rule, hold a public hearing to provide an

257. *Id.* at 3.

258. *Id.* at 2–3.

259. *Id.* at 4.

260. *Id.* at 6–7.

261. For example, the current retention periods are thirty days for video, five years for metadata related to the DAS, and five years for ALPR data. *Id.* at 2–4.

262. NYPD, Press Release, New York City Police Department Releases a Draft of the Public Security Privacy Guidelines for Public Comment, *supra* note 254.

263. *See* Sharon Bradford Franklin, CONSTITUTION PROJECT, *Comments of the Constitution Project Regarding the New York City Police Department's Proposed Public Security Privacy Guidelines for the Domain Awareness System* (Apr. 6, 2009), http://www.constitutionproject.org/wp-content/uploads/2012/09/137.pdf [https://perma.cc/VE26-SGR3] (suggesting needed improvements related to retention, access and auditing).

opportunity for public comment, review testimony including any written comments, and modify the rule, if necessary, before issuing a final rule.[264] Furthermore, the DAS guidelines are quite weak in two key areas beyond the concerns raised above. First, the guidelines fail to specify the criteria for approving data sharing with third-parties. Specifically, they do not address data-sharing arrangements with federal agencies such as DHS, which awarded New York a $25 million grant to help pay for the DAS and may have sought access to data in return.[265] Second, the guidelines provide for very limited oversight. They require periodic reviews of audit logs to ensure compliance with the stated rules, but NYPD counterterrorism officials conduct these reviews, which do not appear to be shared with the city council, the mayor's office, the general public, or with any externally-appointed oversight commission.[266] Enhanced transparency and oversight seem all the more necessary in light of the fact that the rules do not create any private right of action and lack other enforcement mechanisms.

The POST Act—On March 1, 2017, the New York City Council introduced a bill requiring the NYPD to disclose information about the high-tech surveillance tools it deploys for counterterrorism and law enforcement purposes.[267] The bill, called the Public Oversight of Police Technology (POST) Act, requires the reporting and evaluation of surveillance technologies used by the NYPD and broadly defines such technologies as any "equipment, software, or system capable of, or used or designed for, collecting, retaining, processing, or sharing audio, video, location, thermal, biometric, or similar information, that is operated by or at the direction of the department."[268] More specifically, the POST Act

---

264. *See Rulemaking Process 101*, N.Y.C., http://rules.cityofnewyork.us/content/rulemaking-process-101 [https://perma.cc/4EP4-6HLM].

265. In October 2007, the New York Civil Liberties Union submitted a Freedom of Information Law (FOIL) request for documents relating to New York City's plan to implement an earlier version of the DAS. The request included documents transmitted between the NYPD and DHS including, among other things, "the extent to which the information will be shared with other law enforcement agencies or other entities." N.Y. Civil Liberties v. N.Y.C. Police Dep't, 2009 N.Y. Misc. LEXIS 2542, at *3 (Sup. Ct. Jun. 26, 2009). The NYPD denied the FOIL request, and the denial was upheld despite a legal challenge. *Id.* at *9, *13–14.

266. N.Y. POLICE DEP'T, PRIVACY GUIDELINES, *supra* note 253, at 7.

267. Erin Durkin, *NYC Lawmaker Pushes Bill to Make NYPD Unveil All High-Tech Surveillance Tools Used*, N.Y. DAILY NEWS (Feb. 28, 2017), http://www.nydailynews.com/news/politics/pol-pushes-bill-nypd-unveil-high-tech-surveillance-tools-article-1.2985193 [https://perma.cc/8TH2-3EP7].

268. Public Oversight of Surveillance Technology Act, N.Y.C. Council, Int. No. 1482 (as introduced Mar. 1, 2017) [hereinafter POST Act], https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=2972217&GUID=0D8289B8-5F08-

requires the NYPD to issue a surveillance impact and use policy (the "SIU Policy"), which must describe the capabilities of covered surveillance technologies.[269] It also requires the NYPD to adopt policies relating to the retention, access, and use of data collected by such technology and any data sharing with local, state, federal, or private entities; safeguards and security measures designed to protect the information collected; internal audit and oversight mechanisms; and health and safety effects.[270] Upon publication of the draft SIU Policy, the Act requires a public comment period and consideration of these comments by the police commissioner, who then provides the final version of the policy to the city council, the mayor, and the public.[271] Finally, the bill requires the inspector general for the NYPD to audit the SIU Policy to ensure compliance with its terms and to recommend any revisions of the policy.[272]

Unlike the surveillance ordinances adopted in Seattle and other cities, the POST Act is not the product of any public outcry over newly-installed surveillance systems. Rather, the NYPD developed the DAS guidelines to head off privacy concerns, so the POST Act may reflect some combination of its sponsors' political ambitions and their reluctance to tie the hands of a police department that foiled numerous terrorist attacks in the years following 9/11.[273]

Clearly, the POST Act improves upon the DAS guidelines by imposing comprehensive reporting and oversight of all NYPD use of surveillance technologies. But this proposed local law is much weaker than its Seattle counterpart. It requires the NYPD Commissioner to prepare the SIU Policy after public comment and provide it to the city council and mayor, but does not require approval prior to any use of the technology in question.[274] While the POST Act forces the NYPD to become more transparent, it dispenses with enforcement mechanisms or penalties for non-compliance. Unlike the SPD, which did not oppose the Seattle ordinance, the NYPD condemned the POST Act on the grounds that its detailed descriptions of surveillance technologies would aid terrorists and criminals by disclosing "all sorts of confidential information about how these lawful surveillance techniques work."[275] The Bill's sponsors and

---

4E6F-A0D1-2120EF7A0DCA (last visited Nov. 21, 2018).

269. *Id.* § 1.

270. *Id.*

271. *Id.*

272. *Id.* § 2.

273. KELLY, *supra* note 53, at 208–56.

274. POST Act, *supra* note 268, § 2.

275. Ben Kochman & Erin Durkin, *NYPD Officials Argue 'Very Bad' City Council Bill Would Aid*

supporters rejected this criticism as wildly overblown, noting that "[t]he NYPD always resists transparency measures" and that it is unhelpful to mischaracterize the Bill as requiring the NYPD to disclose "operational details" on its technology.[276] As the Brennan Center pointed out, "the federal government routinely discloses its ground rules for using new technologies and strongly encourage[s] local agencies to be open to the public about the surveillance technologies they use."[277] The POST Act did not pass in 2017 but the Council introduced an identical bill early in 2018, which is still pending.[278]

The Body Camera Policy—In New York City, the police department was under somewhat fewer constraints than the SPD in establishing its own body-worn camera program. To begin with, New York is a "one-party" state and thereby avoids all party consent issues, so there is no need to obtain consent from other parties to a communication.[279] Additionally, the state public disclosure law does not require the NYPD to engage in massive release of police video footage.[280] Although the city council introduced a bill and held hearings in 2014 to create a task force to study disclosure issues, the bill did not advance.[281]

In 2014, prior to launching this mandatory pilot project, the NYPD conducted a small pre-pilot program in which fifty-four patrol officers volunteered to wear body cameras. Its purpose was to test body camera equipment, enhance NYPD's understanding of the information

---

Terrorists in Working Around High-Tech Surveillance Tools, N.Y. DAILY NEWS (Mar. 1, 2017), http://www.nydailynews.com/new-york/nypd-officials-bill-terrorists-dodge-surveillance-article-1.2986286 [https://perma.cc/U4JX-VBQE].

276. *Id.*

277. Michael Price, *New York City Is Making Its Citizens Safer by Overseeing Police Technology*, BRENNAN CTR. FOR JUSTICE (Apr. 3, 2017), https://www.brennancenter.org/blog/new-york-city-making-its-citizens-safer-overseeing-police-technology [https://perma.cc/WR5M-EF7M] (noting that DOJ and DHS have published policies on their use of "Stingrays" and that DHS has also been open about its use of facial recognition technologies and ALPRs); *see also* Written Testimony of Michael Price, Counsel for the Brennan Center for Justice, Hearing before the N.Y.C. Council Comm. on Pub. Safety (June 14, 2017), https://www.brennancenter.org/sites/default/files/analysis/Brennan-Center-Testimony-to-NYC-Council-on-Int-1482.pdf [https://perma.cc/L59H-AHXV].

278. N.Y.C. Council, Int. No. 487 (as introduced Feb. 14, 2018), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0&Options=ID|Text|&Search=487 (last visited Nov. 21, 2018)

279. N.Y. Penal Law §§ 250.00-.05.

280. *See* N.Y. POLICE DEP'T, NYPD RESPONSE TO PUBLIC AND OFFICER INPUT ON THE DEPARTMENT'S PROPOSED BODY-WORN CAMERA POLICY 24–26 (2017), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/body-worn-camera-policy-response.pdf [https://perma.cc/U5AD-HNKW].

281. N.Y.C. Council, Int. No. 607 (2014), http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=2103584&GUID=632A9A91-7FD5-424A-880D-7A4E0A8AD0B2 [last visited Nov. 21, 2018].

technology infrastructure necessary to support it, and gain insight on matters of policy and practical implementation.[282] The NYPD then issued Operations Order 48, which unilaterally set the rules for officers participating in this small pre-pilot.[283] In July 2015, the Inspector General for the New York City Police Department (OIG-NYPD), a unit of the Department of Investigation that operates independently of the NYPD, published an initial assessment of the pre-pilot and recommended several changes to the program prior to citywide implementation.[284]

This activity occurred in the shadow of *Floyd v. City of New York*,[285] a landmark federal class action lawsuit addressing the NYPD's controversial stop-and-frisk policies.[286] The federal court and the appointed monitor overseeing the stop-and-frisk settlement played a significant role in supervising the body-worn camera pilot project.[287] After the pre-pilot ended, and in preparation for distributing body-worn cameras more broadly as required by *Floyd*, the NYPD met with a broad range of stakeholders to obtain feedback; then revised its body-worn camera policy, sharing the proposed revisions with the police unions.[288] The Department also sought the assistance of the Policing Project at New York University (NYU) School of Law and the NYU Marron Institute to solicit public input on the draft policy from both members of the public and police officers, respectively.[289] At the close of the comment period, more

---

282. *See* N.Y. POLICE DEP'T, OPERATIONS ORDER 48, PILOT PROGRAM-USE OF BODY-WORN CAMERAS (2014).

283. *Id.*; *see also* OFFICE OF THE INSPECTOR GEN. FOR THE NYPD, BODY-WORN CAMERAS IN NYC: AN ASSESSMENT OF NYPD'S PILOT PROGRAM AND RECOMMENDATIONS TO PROMOTE ACCOUNTABILITY 45–52 (2015) [hereinafter OIG-NYPD, BODY-WORN CAMERAS], http://www1.nyc.gov/assets/oignypd/downloads/pdf/nypd-body-camera-report.pdf [https://perma.cc/RW9F-TYVD].

284. *See* OIG-NYPD, BODY-WORN CAMERAS, *supra* note 283, at 9–36.

285. 959 F. Supp. 2d 668 (S.D.N.Y. 2013).

286. *See generally id.* For other examples of stop-and-frisk class actions, see Ligon v. City of New York, 925 F. Supp. 2d 478 (S.D.N.Y. 2013), and Davis v. City of New York, 296 F.R.D. 158 (S.D.N.Y. 2015).

287. *Floyd*, 959 F. Supp. 2d at 676.

288. *See* Peter Zimroth, *Memorandum Regarding Approval of Policies for NYPD Body-Worn Camera Pilot Program* at 5–7 (Apr. 11, 2017), https://ccrjustice.org/sites/default/files/attach/2017/04/Monitor%204%2011%202017%20Memo%20to%20Court%20re%20Approval%20of%20BWC%20Op%20Order..pdf [https://perma.cc/SY4R-TU7B].

289. *Id.* at 6; *see also* POLICING PROJECT, N.Y.U. SCHOOL OF LAW, REPORT TO THE NYPD SUMMARIZING PUBLIC FEEDBACK ON ITS PROPOSED BODY-WORN CAMERA POLICY (2017), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/59ce7edfb0786914ba448d82/1506705121578/Report+to+the+NYPD+Summarizing+Public+Feedback+on+BWC+Policy.pdf [https://perma.cc/Q7PG-SB4K]; JONATHAN STEWART, NYU MARRON INST. OF URBAN MGMT., REPORT ON THE NYPD OFFICER BODY-WORN CAMERA QUESTIONNAIRE (Feb. 21, 2017),

than 25,000 members of the public and more than 5,400 uniformed officers had participated.[290]

The Department then made several changes to its proposed policy based on the feedback received through the comment process.[291] These included requiring rather than merely encouraging notice to individuals being recorded; adding "inventory searches" and "public interactions that escalate and become adversarial" to the list of events where recording is required; providing additional direction regarding the circumstances when an officer may view a recording related to a serious use of force or an allegation of misconduct; increasing the retention period from six months to one year; and requiring periodic inspections/audits to ensure compliance with the Department's procedures in the use of cameras and the resulting footage.[292] However, the NYPD did not accept the public's recommendations that more police interactions should be recorded, that officers should not be able to view body camera footage before writing a report on a use-of-force incident, and that body camera footage should be more readily accessible.[293]

NYPD body camera footage is a public record and thus subject to New York's freedom of information law (FOIL).[294] In comparison with Washington state's PRA, FOIL takes a more expansive view of when an unwarranted invasion of privacy exempts a public record from disclosure.[295] For example, when a TV station recently requested the release of NYPD body camera footage, the court delayed approval pending a hearing to determine whether reviewing and redacting the videos would be unduly burdensome.[296] In addition, civil rights and police reform advocates have expressed concerns about whether the NYPD

---

https://marroninstitute.nyu.edu/uploads/content/NYPD_Officer_BWC_Questionnaire_Report.pdf [https://perma.cc/GR8M-T7YM].

290. Zimroth, *supra* note 288, at 7.

291. *See* N.Y. POLICE DEP'T, *supra* note 280, at 4–25. The revised draft policy is available at N.Y. POLICE DEP'T, DRAFT OPERATIONS ORDER: PILOT PROGRAM—USE OF BODY-WORN CAMERAS (Mar. 22, 2017), https://www1.nyc.gov/assets/ccrb/downloads/pdf/investigations_pdf/oo_16_17.pdf [https://perma.cc/3QXB-CVWN].

292. N.Y. POLICE DEP'T, NYPD RESPONSE TO PUBLIC AND OFFICER INPUT ON THE DEPARTMENT'S PROPOSED BODY-WORN CAMERA POLICY, *supra* note 280, at 1.

293. Barry Friedman & Maria Ponomarenko, *Pulling the Public into Police Accountability*, GOTHAM GAZETTE (Apr. 13, 2017), http://www.gothamgazette.com/opinion/6869-pulling-the-public-into-police-accountability [https://perma.cc/ZBC7-U95C] (commending the NYPD, however, for the process it followed in obtaining public input).

294. N.Y. PUB. OFF. LAW §§ 84–90 (McKinney 2018).

295. *See id.* § 87(2)(b).

296. *See* Time Warner Cable News NY1 v. N.Y.C. Police Dep't, 53 Misc. 3d 657 (N.Y. Sup. Ct. 2016).

might alternatively rely on New York State's Civil Rights Law section 50-a[297] to block requests from news reporters or advocacy groups for the release of body-worn camera footage under FOIL.[298] This provision treats as confidential any personnel records of police officers used to evaluate performance toward continued employment and promotion.[299] In short, the NYPD is less exposed to massive requests for body camera footage than the SPD—and it knows it.[300]

In April 2017, the monitor in *Floyd* approved the revised policy as to those areas within the monitor's purview and without requiring any further changes.[301] Ten days later, the *Floyd* court approved the deployment of body-worn cameras to 1,200 officers.[302] This happened despite objections from the plaintiffs, who argued that the revised policy was likely to increase public surveillance, especially in the black and Latino communities that were harmed by racial profiling and aggressive stop-and-frisk tactics.[303] Going forward, the Department will determine whether the cameras made a difference to officer performance, civilian complaints, crime levels and prosecutions, and then decide whether to continue expanding the program.[304]

---

297. N.Y. CIVIL RIGHTS LAW § 50-a (2018).

298. *See generally* Meenakshi Krishnan, *New York's Section 50-a Shields Law Enforcement Records*, YALE L. SCH. MEDIA FREEDOM & INFO. ACCESS CLINIC (Oct. 26, 2016), https://law.yale.edu/mfia/case-disclosed/new-yorks-section-50-shields-law-enforcement-records [https://perma.cc/J2YX-7R7H].

299. *See* Molloy v. N.Y.C. Police Dep't, 50 A.D.3d 98 (N.Y. App. Div. 2008) (holding FOIL requests related to an investigation by the police would likely be exempt from disclosure under N.Y. CIVIL RIGHTS LAW § 50-a).

300. *See* N.Y. POLICE DEP'T, NYPD RESPONSE TO PUBLIC AND OFFICER INPUT ON THE DEPARTMENT'S PROPOSED BODY-WORN CAMERA POLICY, *supra* note 280, at 24 (stating—in obvious reference to Seattle's experiment with a YouTube channel—that FOIL "offers a process with privacy controls that, in our view, is far superior to the live-streaming of NYPD policing online, as some departments have tried to do with sometimes extremely harmful consequences").

301. *See* Southall, *Judge Clears Way for Police Body Worn Cameras in New York*, *supra* note 249.

302. *Id.*

303. *See* Press Release, Center for Constitutional Rights, Attorneys Challenge NYPD Body Camera Policy, Asks Judge to Order Changes (Apr. 25, 2017), https://ccrjustice.org/home/press-center/press-releases/attorneys-challenge-nypd-body-camera-policy-ask-judge-order-changes [https://perma.cc/RCQ7-3D85].

304. Ashley Southall, *Do Body Cameras Help Policing? 1,200 New York Officers Aim to Find Out*, N.Y. TIMES (Apr. 26, 2017), https://www.nytimes.com/2017/04/26/nyregion/do-body-cameras-help-policing-1200-new-york-officers-aim-to-find-out.html?mcubz=1&_r=0 (last visited Oct. 27, 2018).

2. *New York City Privacy Principles*

Until very recently, New York City did not undertake a privacy initiative of comparable breadth and depth to that of Seattle. In 2016, the Mayor's Office of Technology and Innovation announced a narrow set of guiding principles for smart cities that were limited in scope to the use of sensor technologies and other IoT deployments.[305] Although the privacy and transparency principles match up reasonably well with the FIPs, it is not clear if they impose binding obligations on city agencies.[306] Indeed, the guidelines may be nothing more than recommendations, rather than legally enforceable obligations.[307] Moreover, the IoT Guidelines seem to exempt law enforcement projects, noting that "[s]pecial circumstances and concerns may also exist for IoT systems and/or data related to public safety, security and law enforcement."[308]

In November 2017, however, the City Council enacted its first comprehensive privacy laws in the form of two bills designed to protect personal information collected by city employees and contractors in the course of providing services and benefits to local residents.[309] Local Law 245 requires every city agency to report on their data collection, retention, and disclosure policies and current practices.[310] It also establishes a Chief Privacy Officer (CPO) and interagency committee to review those reports and develop new, detailed protocols for protecting identifying information in cooperation with agency privacy officers.[311]

---

305. *See NYC Guidelines for the Internet of Things*, N.Y.C. (2018), https://iot.cityofnewyork.us/privacy-and-transparency/ [https://perma.cc/RFN3-Y7G9] [hereinafter IoT Guidelines].

306. The IoT Guidelines cross-reference several citywide polices and laws. For example, the privacy and transparency section cross-references three polices (data classification, encryption, and media re-use and disposal) and the NYC Open Data Law. *Id.* The guidelines do not refer to any citywide privacy policies or laws. *Id.*

307. *See Guidelines for the Internet of Things: FAQ*, N.Y.C. (2018), https://iot.cityofnewyork.us/faq/ [https://perma.cc/5PA3-EP6G] (describing the IoT Guidelines as supplemental and noting that "[c]ity agencies are responsible for implementing and enforcing the guidelines when deploying and managing IoT projects").

308. *Id.*

309. Prior to their enactment, the city had several laws and policies in place imposing mandatory security standards relating to personal information and creating the position of Chief Information Security Officer, but no privacy laws as such. For a description of these policies, see generally *Cybersecurity Requirements for Vendors & Contractors*, N.Y.C. (2018), https://www1.nyc.gov/site/doitt/business/it-security-requirements-vendors-contractors.page [https://perma.cc/X736-APXD].

310. N.Y.C. Council, Local Law 245, Int. No. 1557-A (2017) (codified at N.Y.C. CHARTER § 8 and N.Y.C. ADMIN. CODE §§ 23-1203, 23-1204, 23-1205 (2018)).

311. *Id.*

Local Law 247[312] requires city employees and contractors to protect all identifying information by limiting collection, disclosure, and retention, except where required by law.[313] Requests for the collection or disclosure of identifying information are processed by a newly established privacy officer within each agency who analyzes whether the collection or disclosure furthers the purpose or mission of the agency.

These new laws, which took effect in June 2018, are best understood through the lens of several citywide initiatives and programs that preceded and shaped them. For example, in 2008, the mayor's office launched an initiative known as HHS-Connect to provide "a more complete understanding of clients' needs and enable more efficient and effective service delivery."[314] HHS-Connect achieves this goal through data integration and exchange among multiple health and human services agencies. Participating agencies sign an "Inter-Agency Data Exchange Agreement" that, among other things, ensures the protection and confidentiality of all data exchanged or accessed by HHS-Connect systems.[315] A few years later, the city enacted the Open Data Law, mandating that by the end of 2018, the city make all "public" data sets freely available on a single web portal (i.e., any comprehensive collection of data that is maintained on a computer system by or on behalf of a city agency).[316] This law does not explicitly address data protection issues. Thereafter, the mayor issued an executive order creating the Mayor's Office of Data Analytics (MODA). MODA's responsibilities include collaborative, data-driven solutions, a citywide data platform, oversight for data projects, and implementation of the Open Data Law.[317] MODA also uses "analytics tools to prioritize risk more strategically, deliver services more efficiently, enforce laws more effectively and increase transparency," and has undertaken several initiatives—none of which emphasize maintaining privacy.[318]

---

312. N.Y.C. Council, Local Law 247, Int. No. 1588-A (Dec. 17, 2017) (codified at N.Y.C. ADMIN. CODE §§ 23-1201, 23-1202).

313. *Id.*

314. N.Y.C. Mayor Exec. Order No. 114 (Mar. 18, 2008), http://www.nyc.gov/html/om/pdf/eo/eo_114.pdf [https://perma.cc/9KES-F39G].

315. Inter-Agency Data Exchange Agreement, Agencies of the City of N.Y. (Nov. 2010), https://www1.nyc.gov/assets/hpd/downloads/pdf/interagency-mous/mou_between_hpd_and_city_agencies_for_hhs_connect.pdf [https://perma.cc/CDQ6-PSEF].

316. N.Y.C. Council, Local Law 11, Int. No. 29-A (Mar. 7, 2012) (codified at N.Y.C. ADMIN. CODE § 23-501 et seq.).

317. N.Y.C. Mayor Exec. Order No. 306 (Apr. 17, 2013), http://www.nyc.gov/html/om/pdf/eo/eo_306.pdf [https://perma.cc/EJF5-KSWA].

318. *About the Office of Data Analytics*, N.Y.C. (2018),

In 2015, the City Council held hearings on a proposed local law that would have required each city agency that collects personal information to develop a system to protect the privacy of that information. Agencies would have to adopt appropriate administrative, technical and physical safeguards to ensure the confidentiality of personal records and destroy those records once the purpose of collecting that information was achieved.[319] The bill did not advance, mainly because the mayor's office objected, stating that the bill would "inadvertently impede the delivery of critically needed services to New Yorkers . . . through legally authorized inter-agency data exchanges that are facilitated through technology."[320] The new privacy laws enacted in 2017 overcome this objection by balancing the privacy interests of those who rely on human services against the City's strong commitment to deliver these services in an efficient and effective manner.

Thus, the new laws set policies restricting the collection and disclosure of identifying information but also contain provisions facilitating data sharing in routine circumstances or where it serves the best interests of the City.[321] City agencies also must require contractors and subcontractors that obtain identifying information to apply these collection, disclosure, and retention requirements.[322] Another important goal of the new laws is to address any privacy concerns that might deter residents from seeking city services by defining "identifying information" in very broad terms.[323] Most definitions of personal information refer mainly to specific identifiers that may be used (individually or in combination) to identify or locate an individual (e.g., name, address, contact information, license plate numbers, and biometrics). In contrast, the term "identifying information" refers to identifiers as well as information related to various types of status including those enumerated in the NYCID program.[324] The new law imposes additional requirements for protecting identifying

---

https://www1.nyc.gov/site/analytics/about/about-office-data-analytics.page [https://perma.cc/49LB-HCJT].

319. *See* Personal Information Privacy, N.Y.C. Council, Int. No. 627 (as introduced Jan. 22, 2015).

320. Written Testimony of Mindy Tarlow, Director, N.Y.C. Mayor's Office of Operations, Hearing before the N.Y.C. Council Comm. on Tech. 3 (Feb. 1, 2016), legistar.council.nyc.gov/View.ashx?M=F&ID=4233458&GUID=87B6F563-96A0-433A-ACD8-B36BC7371D67 [https://perma.cc/29VX-25BF].

321. N.Y.C. ADMIN. CODE §§ 23-1202(c)-(e).

322. *See id.* § 23-1202(g).

323. *See id.* § 23-1201.

324. *See id.* It is more common in privacy circles to refer to these status categories as "sensitive information," which is a special subset of PII usually subject to additional obligations. *See generally* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015).

information as so defined including anonymization and limitations on how third-parties may use such information.[325]

The Open Data Program—In 2012, New York City followed Seattle's lead by amending the City's administrative code to mandate publication of city data online.[326] The City Council has amended and strengthened its Open Data Law several times since,[327] and an Open Data Team composed of members of MODA and the city information technology department is working with a government technology vendor to achieve the law's mandates.[328]

In contrast to Seattle, New York City's open data website explicitly disclaims the completeness and accuracy of the city's data for any particular purpose and notes that users must agree to certain terms of use imposed by individual agencies to access data made available on the central portal.[329] Although the City's Open Data Program shares many of the same goals as Seattle's—transparency, accountability, economic growth, and generating research insights—its publications about the program fail to explicitly mention the privacy risks inherent in smart city data publication activities. While both mention similar goals at various points, only Seattle's contains explicit descriptions of and plans to resolve privacy concerns.[330] Responsibility for privacy appears to be placed in the hands of each individual agency rather than handled in a more centralized manner.[331] The City appears to define privacy as beyond the scope of its Open Data program, noting that disclosure of information that "result[s] in an unwarranted invasion of personal privacy" is already exempt from public access under FOIL.[332] Other than noting the "open by default" policy stops where existing privacy law begins, New York City's strategy

325. N.Y.C. ADMIN. CODE §§ 23-1203(3), (5).

326. N.Y.C. Council, Local Law 11, Int. No. 29-A (mandating open data availability by the end of 2018).

327. *See NYC OpenData: Laws and Reports*, N.Y.C. (2017), https://opendata.cityofnewyork.us/open-data-law/ [https://perma.cc/C7WD-KZCQ] (discussing and citing amendments of November 2015, January 2016, and December 2017, to strengthen retention requirements, response timelines, and make permanent the original Open Data mandate).

328. *NYC OpenData: Overview*, N.Y.C. (2017), https://opendata.cityofnewyork.us/overview/ [https://perma.cc/N74J-QKUY].

329. *Id.* (discussing Open Data Terms of Use).

330. *Compare id.*, *with* SEATTLE INFO. TECH., 2017 OPEN DATA PLAN, *supra* note 222.

331. DEP'T OF INFO. TECH. & TELECOMM., N.Y.C., OPEN DATA POLICY AND TECHNICAL STANDARDS MANUAL § 4.4.2 (2016), https://www1.nyc.gov/assets/doitt/downloads/pdf/nyc_open_data_tsm.pdf [https://perma.cc/ES4S-UM3X].

332. *Id.* § 4.5(b).

for privacy protection in open data initiatives appears, at present, to lack an independent privacy apparatus.[333]

C. Assessing Privacy Localism in Seattle and New York City

It is too soon to offer any serious evaluation of the ongoing experiments with privacy localism in Seattle and New York City. To begin with, the surveillance ordinances are brand new, or still in the proposal stage, and the privacy program in New York City is just taking effect. In Seattle, the privacy program is several years old but there is still not enough data to assess its strengths and weaknesses. When sufficient data is gathered, an important question will be whether cities have sufficient expertise and resources to engage in privacy regulation as compared to their federal and state counterparts. After all, cities like Seattle and New York lack the kind of administrative infrastructure taken for granted when Congress delegates rulemaking, programmatic design, and ongoing supervisory duties to federal agencies. These agencies rely on institutional, organizational, and doctrinal mechanisms to produce, review, and approve a high volume of rules, licenses, permits, and so on. Lacking these mechanisms, officials in Seattle and New York City may be overwhelmed by the amount of work required to produce, review and/or approve a high volume of privacy-related applications, assessments, and reports.

A second issue is whether local surveillance laws risk isolating local police departments by disrupting regional and local partnerships with other agencies not subject to similar requirements. For example, during the hearings on the revised surveillance ordinance, the SPD raised concerns that extending the ordinance beyond surveillance technology to encompass surveillance data might jeopardize data sharing arrangements under regional partnerships for reducing gang activity and gun violence, and even turn Seattle into a data island.[334]

Finally, cities may rely too heavily on legal—as opposed to technological—instruments of privacy regulation. In their study of privacy governance, Professors Colin Bennett and Charles Raab distinguish legal instruments like self-regulatory principles and statutes from technological instruments including "privacy by design," i.e., cities

---

333. *Id.* § 3.4.1.

334. *See Gender Equity, Safe Communities, & New Americans Committee,* SEATTLE CHANNEL, at 1:21 to 1:22 (July 12, 2017), https://www.seattlechannel.org/mayor-and-council/city-council/2016/2017-gender-equity-safe-communities-and-new-americans-committee/?videoid=x78884 [https://perma.cc/L4R9-L4ZM] (statement of SPD Chief Technology Officer Brian Maxey).

imposing design requirements on vendors or only purchasing technology with certain privacy protective features.[335] To date, Seattle and New York City have relied almost exclusively on legal instruments to regulate technology deployments and data collection, use, and disclosure within their local governments and have largely done without technological instruments.

At this point, however, a preliminary assessment of the surveillance oversight and privacy governance programs under development in Seattle and New York City is feasible to determine whether they achieve their stated purposes. Section II.C thus considers to what extent privacy localism contributes to what Barry Friedman calls "democratic policing" and closes the two privacy gaps identified above.

1. Policing and Democratic Governance

Much of the commentary on urban policing and related privacy issues is a tale of competing narratives. One narrative centers on race, crime, and the fight for social justice. Thus, it tends to focus on controversial or abusive policing practice.[336] The other is a tale of terror that focuses on the unrelenting string of urban suicide bombings and violent assaults in New York, Moscow, Istanbul, Mumbai, Madrid, London, Nairobi, Boston, Brussels, Paris, and other cities.[337] These attacks have caused tens of thousands of deaths and many billions of dollars of economic losses.[338] Controversial policing practices are also part of this terrorism narrative. They range from changes in the mission of local police forces to the use of new surveillance technologies under broad authorities that do not require any showing of particularized suspicion, and—at least in the United States—a new emphasis on information sharing and unified action across multiple levels of government via fusion centers and Joint Terrorism Task Forces.[339]

---

335. *See* COLIN BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY 117–204 (2006).

336. *See supra* text accompanying note 67.

337. *See* Robert Muggah, *Is Urban Terrorism the New Normal? Probably*, WORLD ECON. F. (Jan. 17, 2016), https://www.weforum.org/agenda/2016/01/is-urban-terrorism-is-the-new-normal-probably/ [https://perma.cc/WZG6-LN2B].

338. This is only a partial listing and it omits smaller but frequent attacks in multiple cities in countries such as Afghanistan, Egypt, Iraq, Israel, Lebanon, Libya, Nigeria, and Pakistan; these too wreak havoc in their own devastating way. *See generally Global Terrorism Database (GTD)*, UNIV. MD. (June 2017), http://www.start.umd.edu/gtd/ (last visited Nov. 21, 2018) (listing statistics and trends in terror attacks around the world).

339. *See generally* STEPHEN GRAHAM, CITIES, WAR, AND TERRORISM: TOWARDS AN URBAN GEOPOLITICS (2004); MICHAEL PRICE, BRENNAN CTR. FOR JUSTICE, NATIONAL SECURITY AND LOCAL POLICE (2013); Muggah, *supra* note 337.

In his recent work on democratic policing, Professor Friedman advances the argument that these two narratives—racial bias in police tactics and intelligence gathering via panvasive surveillance—are not isolated issues but rather two sides of a single phenomenon: the complete breakdown of democratic control over policing.[340] Friedman begins by observing that due to overbroad enabling statutes, most policing occurs without any clear rules or policies in place; or, if they do exist, they are not readily accessible to the public.[341] Legislators do not have much incentive to change this given the powerful special interest groups, like police unions, that have a stake in opposing such regulation and the political weakness of the victims of out-of-control policing, such as minorities and the poor.[342] Finally, Friedman contends that courts have failed to properly supervise policing procedures mainly because judicial remedies, such as the exclusionary rule and damages actions, are ineffective.[343] Moreover, judicial review is ill-equipped to deal with the recent shift from reactive and investigative policing based on particularized suspicion, to proactive and programmatic policing targeting larger populations and entire neighborhoods or ethnic groups, who are subjected to dragnet forms of surveillance.[344] Friedman and Ponomarenko sum up these governance failures as constituting a kind "police exceptionalism" within the administrative state.[345] Friedman contends that what is urgently needed to overcome police exceptionalism is not more oversight but rather "rules that are written *before* officials act, rules that are *public*, rules that are written with *public participation*."[346] In short, the democratic polity must insist on "transparent democratic processes such as legislative authorization and public rulemaking"[347] as applied to policing.

Is democratic policing an achievable goal? Friedman is undoubtedly correct in suggesting that recent events have forced police to do a better job of soliciting public input. In the wake of multiple police killings of African-Americans in cities across the country, police chiefs have started to listen to local citizens about a range of policy issues. It is more common

340. FRIEDMAN, *supra* note 67, at 6–14; *see also* Friedman & Ponomarenko, *supra* note 119.

341. Friedman & Ponomarenko, *supra* note 119, at 1844.

342. FRIEDMAN, *supra* note 67, at 101–03.

343. *Id.* at 81–86.

344. Friedman & Ponomarenko, *supra* note 119, at 1871–75; *see also* Renan, *supra* note 68; Slobogin, *Panvasive Surveillance*, *supra* note 68.

345. Friedman & Ponomarenko, *supra* note 119, at 1837.

346. FRIEDMAN, *supra* note 67, at 20.

347. Friedman & Ponomarenko, *supra* note 119, at 1832.

than ever before for local police forces to hear from a variety of stakeholders (civil liberties groups and privacy advocates as well as local residents) before formulating policies on the use of surplus military equipment,[348] drones,[349] and body-worn cameras.[350]

That said, democratic policing will not be easily achieved. Difficult questions will need to be addressed about how to scale public rulemaking to communities and police forces of various sizes. After all, there are more than 13,000 U.S. police departments serving both large cities and smaller communities—with more than half of these departments serving communities with fewer than 10,000 residents—and there is a high degree of variance in police department size.[351] For example, the median local police department has only eight full-time officers, while the NYPD has 36,000. The availability of model rules from various sources should help ease the burden of smaller communities having to draft rules from the ground up.[352] Lastly, Friedman and Ponomarenko note that "[b]y virtue of their *closeness* to the citizenry, local governments are already adept at fielding input from the community, be it through school boards, zoning boards, arts commissions, or neighborhood councils."[353] Of course, it follows that local police may develop policies that vary in significant ways from one locale to the next, but as Friedman sees it this is "the sign of a healthy democratic process at work."[354]

The local surveillance ordinances described in this Article epitomize what Friedman has in mind by democratic policing. To begin with, the primary goals of the surveillance ordinances adopted (or under consideration) in Seattle and New York City are transparency and accountability, which are also the primary mechanism for achieving secondary goals such as adapting to changes in technology, restoring and maintaining public trust, and balancing public safety and civil liberties. Both surveillance ordinances are well-designed to achieve these goals by requiring the SPD and NYPD to prepare and make publicly available detailed reports describing their use of covered surveillance technologies (and surveillance data in Seattle) as well as related rules, policies, and practices. Such transparency allows privacy advocates to generate

348. FRIEDMAN, *supra* note 67, at 96–98.

349. *Id.* at 98.

350. *Id.* at 313–15.

351. Friedman & Ponomarenko, *supra* note 119, at 1886–87.

352. *See generally* POLICING PROJECT (2017), https://policingproject.org/ [https://perma.cc/YVB3-CFLH].

353. Friedman & Ponomarenko, *supra* note 119, at 1888 (emphasis added).

354. FRIEDMAN, *supra* note 67, at 96.

politically relevant information about privacy protection. This, in turn, fosters research and analysis and allows advocates working behind the scenes to assist the SPD and NYPD in improving their practices, commenting on proposed uses, and, when necessary, exerting leverage through the threat of bad publicity.[355]

The Seattle and New York City ordinances differ in two important respects: the former defines surveillance technology and data very broadly and establishes an approval process for numerous items, while the latter ignores data and relies solely on transparency without a separate process of approval by a political branch. In effect, the POST Act tries to force the police to "own" any decision to rely on new surveillance technology by requiring disclosures that might prove controversial or embarrassing if publicized. It is too soon to say which approach will prove more effective. The Seattle process gives elected representatives the final word but imposes significant costs and potential backlogs and delays in securing approvals. The New York City process may force the NYPD to beef up privacy protections to avoid negative publicity. But if the NYPD views a new surveillance technology as essential for securing public safety, it may be willing to absorb the bad press given the lack of political oversight. Moreover, since the proposed bill includes audits but no penalties for non-compliance, the NYPD is subject to little risk if its internal cost-benefit calculations favor pushing the envelope to the outer boundaries of what the POST Act allows.

The Seattle and New York City policies concerning the use of body-worn cameras and the use, retention, and disclosure of related video footage also demonstrate the power of local policymaking. In both cities, a court-appointed monitor supervised the policymaking process under the terms of a consent decree; in Washington, state law sets minimum requirements for body-worn camera policies. And yet both cities engaged in extensive consultation with stakeholders and followed highly democratic processes in shaping policies that remain subject to future revision based on further experience and review.

2. Closing the Public Surveillance Gap

One of the main virtues of local surveillance ordinances is that they close the public surveillance gap by developing transparency and accountability mechanisms free of Fourth Amendment doctrinal constraints present in recent cases such as *Jones* and *Carpenter*. These mechanisms apply even when the government uses panvasive

355. *See* COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 95–132 (2008) (describing these and other modes of privacy advocacy).

technologies. They are also independent of federal and state electronic surveillance laws with their obscure and outdated definitions of electronic communications and services. Rather, the local surveillance ordinances apply to (almost) all surveillance technologies, irrespective of whether they monitor public or private spaces. These ordinances require law enforcement to prepare and submit impact reports on a technology-by-technology basis, thereby allowing elected officials or the public to determine whether it is appropriate for a city to acquire and use such technology.[356] This is a remarkable and welcome development in U.S. surveillance law.

How broadly do these surveillance ordinances apply? In particular, do they apply to video surveillance and the other components of the DAS? The answer both varies by city and remains to be seen based on local practices, interpretations, legal challenges, and political oversight. For example, the Seattle ordinance excludes body-worn cameras, but the SPD has a separate body-worn camera policy.[357] The ordinance also excludes cameras installed for a single purpose—such as solely to record traffic violations, for security purposes, or to protect the physical integrity of city infrastructure.[358] The POST Act similarly excludes "cameras installed to monitor and protect the physical integrity of city infrastructure."[359] These exceptions will have to be interpreted and applied, although they seem narrow enough to avoid a blanket exemption for something like the DAS.[360]

3. Closing the Fair Information Practices Gap

As for data governance, the two cities rely on a similar set of privacy principles, although Seattle's ordinance covers collection, use, and disclosure limitations as well as accuracy and accountability, while New York City's chiefly addresses the collection, retention, and disclosure of identifying and sensitive information. Seattle has a more expansive program than New York City, not so much in terms of breadth (both laws apply to all city departments) but rather in terms of depth (Seattle places a much a greater emphasis on PIAs). However, both the PIA process in Seattle and the biennial city agency reports in New York City serve a very

356. *See supra* sections II.A.1, II.B.1.

357. *See supra* text accompanying notes 173–206.

358. *See supra* note 161.

359. POST Act, *supra* note 268.

360. The Santa Clara County surveillance ordinance avoids this issue by defining "surveillance technology" in extremely broad terms and supplying examples that match up with every component of the DAS. *See* SANTA CLARA COUNTY, CAL., CODE OF ORDINANCES div. A40, § A40-7(c) (2018).

similar purpose to SORNs and PIAs under the federal Privacy Act and the related E-Government Act. As noted above, these laws apply exclusively to federal agencies. Furthermore, New York's Privacy Act does not require any processes similar to SORNs or PIAs, whereas Washington does not even have a Privacy Act. Thus, it falls to the Seattle and New York City privacy laws to ensure that both cities take advantage of these processes at the local level.

It seems likely that Seattle's program will yield superior results to that of New York City's thanks to its reliance on PIAs. To date, Seattle has published nine PIAs on a range of programs.[361] The first PIA addressed smart meter deployment by Seattle City Light (the city-owned electric utility).[362] Privacy activists initially objected to this program, fearing that smart meters might be "misused to act as data collection devices which make previously private activities inside our dwellings subject to unauthorized official and criminal surveillance."[363] Seattle City Light responded by developing an opt-out option and limiting data collection and transmission.[364] The Seattle CPO not only prepared a PIA, but it also hired an outside law firm to suggest actions to mitigate potential privacy risks.[365] Nevertheless, the ACLU-WA voiced significant concerns about the smart meter program, criticizing the smart meter PIA as unclear, inadequate, and incomplete.[366] A year later, the Seattle City Council passed a new ordinance prohibiting the sale of utility consumers' sensitive personal data and limiting its use only for utility service and related purposes.[367] More recent PIAs have not resulted in similar controversies.

---

361. *Technology Privacy Impact Assessments*, CITY OF SEATTLE (Aug. 27, 2018), https://data.seattle.gov/City-Business/Technology-Privacy-Impact-Assessments/5mii-56rx [https://perma.cc/FCF6-P6VD].

362. CITY OF SEATTLE, CITY OF SEATTLE PRIVACY IMPACT ASSESSMENT (2017), https://www.seattle.gov/Documents/Departments/Tech/AMI-PIA-FINAL-Rev2.pdf [https://perma.cc/VB47-ED7E].

363. *See, e.g.*, Molly Connelly & Jan Bultmann, *Seattle City Light: Seattleites Need an Opt-In Policy for Smart Meters*, SEATTLE PRIVACY COAL. (Mar. 3, 2014), https://www.seattleprivacy.org/advanced-metering-devices-and-customer-choice/ [https://perma.cc/L95N-4YJQ].

364. *Advanced Metering: Opt-Out Policy*, CITY OF SEATTLE, http://www.seattle.gov/light/ami/opt-out.asp [https://perma.cc/626F-H8D8].

365. CITY OF SEATTLE, CITY OF SEATTLE PRIVACY IMPACT ASSESSMENT, *supra* note 362; *About the Privacy Program*, CITY OF SEATTLE, http://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program [https://perma.cc/38F8-MUDA].

366. Letter from Shankar Narayan, Tech. & Liberty Project Dir., ACLU Wash., to Kshama Sawant, Energy & Env't Comm. Chair, Seattle City Council (May 25, 2017) (discussing Seattle City Light's Advanced Meter Program), https://www.aclu-wa.org/file/101692/download?token=ujQJA9l9 [https://perma.cc/7TXC-VCTJ].

367. *Seattle City Council Adopts Nation's Strongest Law to Protect Utility Customer Personal*

III. THE CHALLENGES OF PRIVACY LOCALISM

As the previous discussion demonstrates, privacy localism—as exemplified by Seattle and New York City's adoption of local surveillance laws or policies and citywide privacy principles—responds to longstanding deficiencies in federal and state privacy protection and helps close the public surveillance and fair information practices gaps in privacy law. Despite these achievements, privacy localism remains vulnerable to objections on multiple fronts. To begin with, skeptics may ask: why analyze local privacy regulation in terms of localism rather than federalism? How are they different? And even though a few cities have taken tentative steps to regulate local surveillance activity and local government data practices, do cities have sufficient power to pursue or sustain local solutions to pressing privacy issues? Isn't this unlikely given the threat of federal or state legislation eventually preempting these local efforts? This Part moves beyond the details of local privacy regulation in Seattle and New York City to explore two conceptual challenges: the distinction between localism and federalism and the factors enabling privacy localism to sustain its momentum in face of the dual threats of federal preemption and limited power and immunity from state preemption. This Part concludes that despite these threats, privacy localism is more robust than one might think.

A. Localism or Federalism?

Cities—including Seattle and New York City—are beginning to experiment with innovative approaches to protecting the privacy of their local residents in the face of inadequate federal and state privacy laws. These cities understand that pervasive public surveillance and massive data collection erode civil liberties and engender mistrust of local government, including (most crucially) local police departments. And they recognize that the time for action is now, especially in view of the public surveillance gap and the fair information practices gap.

Additionally, these innovative cities are experimenting with a novel approach. On the surveillance side, they are not mimicking one-off state laws by addressing specific invasive technologies in response to public outcry.[368] Rather, they have devised comprehensive, iterative methods for reviewing all surveillance technologies prior to purchasing or deploying

---

Data, ACLU WASH. (Aug. 6, 2018), https://www.aclu-wa.org/news/seattle-city-council-adopts-nation%E2%80%99s-strongest-law-protect-utility-customer-personal-data [https://perma.cc/VTU2-JYYJ].

368. *See infra* section III.D.1.

them, using procedures that not only capture emerging technologies but allow cities to reassess prior decisions in light of new threat assessments and other changes in local conditions. On the smart city side, they are adopting risk-based principles and methodologies that support privacy-protective data-sharing programs consistent with their ambitious goals to achieve growth, sustainability, resiliency, and equity. Finally, these cities are proceeding in the best tradition of local autonomy. They are experimenting with diverse solutions that reflect key differences in how their political leaders weigh the social costs of surveillance against the risk of catastrophic losses of a potential terrorist attack,[369] or the tradeoffs between maximizing openness and minimizing privacy risks.[370] This sounds a lot like federalism, or federalism with a local flavor, or perhaps just localism. Although the literature on federalism is vast, the following section briefly highlights a few key ideas and situates privacy localism within mainstream accounts of dual sovereignty and cooperative federalism.

In *Gregory v. Ashcroft*,[371] Justice O'Connor identified five advantages of "our federalism":

> It [1] assures a decentralized government that will be more sensitive to the diverse needs of a heterogeneous society; [2] it increases opportunity for citizen involvement in democratic processes; [3] it allows for more innovation and experimentation in government; . . . [4] it makes government more responsive by putting the States in competition for a mobile citizenry . . . . Perhaps the principal benefit of the federalist system is [5] a check on abuses of government power.[372]

Privacy localism, as described in the Seattle and New York City case studies, certainly exhibits diversity, increased participation, experimentation and innovation, responsiveness, and accountability. But Justice O'Connor embedded these instrumental values in a theory of federalism known as "dual sovereignty."[373] There are several reasons to

---

369. It is not surprising that New York City's surveillance law contemplates a less onerous review process than the one adopted in Seattle, given the former's sheer size, the number and importance of its landmark buildings, its losses in the 9/11 attack, and the human and symbolic importance of keeping the city safe from future attacks.

370. *See supra* text accompanying notes 219–25 and 326–33.

371. 501 U.S. 452 (1991).

372. *Id.* at 458; *see* Richard Briffault, *What About the 'Ism'?" Normative and Formal Concerns in Contemporary Federalism*, 47 VAND. L. REV. 1303, 1305 (1994) (analyzing the instrumental values of federalism).

373. *Gregory*, 501 U.S. at 457 ("We begin with the axiom that, under our federal system, the States possess sovereignty concurrent with that of the Federal Government, subject only to limitations

disentangle these values from dual sovereignty in formulating a theory of privacy localism.

To begin with, the traditional concerns of dual sovereignty have little bearing on privacy regulation with the exception of *Reno v. Condon*,[374] a decision in which the U.S. Supreme Court rejected a Tenth Amendment challenge to the Driver's Privacy Protection Act (DPPA),[375] a federal law regulating the privacy of state motor vehicle records.[376] In *Condon,* the state of South Carolina challenged the DPPA, which regulates the sale and distribution by state Departments of Motor Vehicles (DMVs) of personal information in motor vehicle records.[377] The DPPA prohibits DMV personnel from disclosing driver's personal information in motor vehicle records without the subject's consent, requires certain disclosures of personal information for public safety purposes, enumerates permissible uses, and restricts the resale and re-disclosure of such information by private persons who have lawfully obtained that information from a state DMV.[378] Apart from *Condon*, there is scant evidence of legislatures, courts, or scholars treating government restrictions on the collection, use, and disclosure of personal data as a power reserved to the states for their exclusive control or viewing federal lawmaking in this area as necessarily intruding upon state sovereignty.[379]

In upholding the DPPA, the *Condon* Court overturned lower court decisions invalidating this law as incompatible with the anti-commandeering doctrine as developed in *New York v. United States*[380] and *Printz v. United States*[381] The Court distinguished these cases on two

---

imposed by the Supremacy Clause." (alteration omitted) (citing Tafflin v. Levitt, 493 U.S. 455, 458 (1990)). *See generally* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 256 (5th ed. 2015).

374. 528 U.S. 141 (2000).

375. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (codified as amended at 18 U.S.C. §§ 2721–2725 (2012)).

376. *Condon*, 528 U.S. at 141–42.

377. *Id.*

378. *Id.* at 144.

379. The privacy torts are the obvious exception. Tort law is primarily state law, not federal law. *See generally* RESTATEMENT (SECOND) OF TORTS § 625A (AM. LAW INST. 1977); SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 1, at 32–33. However, the privacy torts play little role in addressing the concerns raised by local surveillance or local government data practices.

380. 505 U.S. 144, 188 (1992) (invalidating a federal law regulating the disposal of radioactive wastes on the grounds that "[t]he Federal Government may not compel the States to enact or administer a federal regulatory program").

381. 521 U.S. 898, 935 (1997) (striking down a federal law requiring state and local law enforcement personnel to conduct background checks before issuing permits for firearms and reaffirming that "[t]he Federal Government may neither issue directives requiring the States to

grounds: first, that the DPPA was prohibiting, not requiring state government actions; and, second, that the statute is generally applicable because it "regulates the universe of entities that participate as suppliers to the market for motor vehicle information."[382] Many commentators have criticized the first argument as resting on a dubious distinction between affirmative and negative duties.[383] After all, most duties can be characterized either way. The second argument is more compelling, although as Professor Chemerinsky notes skeptically, it leaves open the possibility that Congress could reenact the laws at issue in *New York* and *Printz* "by making sure that some private conduct was regulated by them also."[384] But apart from this single decision, disputes over the limits of federal power have almost no bearing on the evolution of privacy law at the federal, state, or local level.

Another problem with dual sovereignty is that it tends to evoke a conservative political agenda and the use of "States' rights" to deprive individuals of their civil and voting rights, especially in the Jim Crow South.[385] But as Dean Heather Gerken observes, "[i]t is a mistake to equate federalism's past with its future."[386] Gerken and others have developed a progressive theory of federalism that not only reconceptualizes intergovernmental relations but also seeks to demonstrate the benefits of decentralization for achieving progressive goals.[387] She argues that "[s]tate and local governments have become sites of empowerment for racial minorities and dissenters" who can wield more

---

address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program").

382. *Condon*, 528 U.S. at 151.

383. *See, e.g.*, Erwin Chemerinsky, *Right Result, Wrong Reasons:* Reno v. Condon, 25 OKLA. CITY U. L. REV. 823, 827–28 (2000).

384. *Id.* at 828.

385. Heather K. Gerken, *A New Progressive Federalism*, DEMOCRACY (2012), https://democracyjournal.org/magazine/24/a-new-progressive-federalism/ [https://perma.cc/LA5L-BCQU].

386. *Id.*

387. Heather K. Gerken, Keynote Address at the New York University School of Law's Thomas M. Jorde Symposium: Federalism 3.0 (Mar. 1, 2017); *see also* Richard Thompson Ford, *The New Blue Federalists: The Case for Liberal Federalism*, SLATE (Jan. 6, 2005, 5:56 PM), https://www.slate.com/articles/news_and_politics/jurisprudence/2005/01/the_new_blue_federalists.html [https://perma.cc/2DJU-NSY2] (noting that "the legal arguments once used to invalidate liberal policies are equally applicable to federal laws favored by conservatives"); Ernest A. Young, *Welcome to the Dark Side: Liberals Rediscover Federalism in the Wake of the War on Terror*, 69 BROOK. L. REV. 1277, 1279 (2004) (analyzing state and local non-cooperation with federal anti-terrorism measures).

electoral power at the local level than at the national level, allowing them to become "efficacious political actors."[388]

Professor Richard Schragger makes a similar argument about the need to decouple "the rhetoric of decentralization" from "anti-government conservatives" while emphasizing the role of cities in advancing progressive policy developments.[389] Schragger describes a surge in local activity across a range of controversial policy issues such as workers' rights, healthcare, campaign finance, climate change, marriage equality, and immigration, which he attributes to two main factors: the growing dissatisfaction among progressives with the national responses to these problems and the renewed economic growth and political clout of cities.[390] In advocating for what he calls a "progressive decentralism," he argues that "[t]he localness of regulatory initiatives is their greatest strength, permitting regulatory innovation to start small and develop as efforts are made and programs are improved upon."[391] Privacy localism has far more in common with Gerken's "progressive federalism" and Schragger's "progressive decentralism" than with stale theories of dual sovereignty.

Schragger describes municipal policy developments that respond to specific political dynamics. Some policy developments (like living wage campaigns and health care mandates) mainly respond to the absence of federal or state activity.[392] Others (like campaign finance, climate change, and marriage equality) mainly attempt to spur policy activity at higher levels of government by experimenting at the local level.[393] Still, others (like immigration policy) mainly reflect tensions between federal and state or local authorities over which level of government controls the

388. Gerken, A New Progressive Federalism, *supra* note 385. Gerken elaborates on these themes in Heather K. Gerken, *Dissenting by Deciding*, 57 STAN. L. REV. 1745 (2005); Heather K. Gerken, *The Supreme Court, 2009 Term—Foreword: Federalism All the Way Down*, 124 HARV. L. REV. 4 (2010).

389. Richard C. Schragger, *The Progressive City*, *in* WHY THE LOCAL MATTERS: FEDERALISM, LOCALISM, AND PUBLIC INTEREST ADVOCACY 39–46 (Rachel Deutsch et al. eds., 2008).

390. *Id.* at 39, 40–44.

391. *Id.* at 42.

392. Upper levels of government may be inactive due to political gridlock, uncertainty over the wisdom of uniform state or national treatment, or the greater salience of the issue in question in some localities but not others. *See* Richard Briffault, *Local Leadership and National Issues*, *in* WHY THE LOCAL MATTERS: FEDERALISM, LOCALISM, AND PUBLIC INTEREST ADVOCACY, *supra* note 389, at 67, 74–79.

393. As Professor Richard Briffault observes: "Local successes can build political support for state or national actions, and local failures can spark the search for different solutions." *Id.* at 79.

relevant policy domain.[394] The point is that there are not only a range of local policy initiatives but also many different localisms.[395]

Finally, while the dual sovereignty doctrine often leads to constitutional disputes over the limits of federal power and hence the policing of federal-state relations by the U.S. Supreme Court, localism turns on the regulatory authority of local governments. And this mostly boils down to the subtle interplay of empowerment and immunity that local governments enjoy under state "home rule" provisions,[396] which are discussed below in section III.C. Thus, privacy localism is far removed from traditional concerns over the limits of federal power or the desirability of maintaining separate federal and state spheres of power and authority.

As to cooperative federalism, the leading alternative to dual sovereignty, one might expect that privacy localism would have more in common with this doctrine given that it seeks to capture the benefits of decentralization and local autonomy while preserving the primacy of the federal government in setting national priorities and prescribing standards through which to advance those priorities.[397] But this is not the case. Cooperative federalism—and alternative accounts like Professors Bulman-Pozen and Gerken's "uncooperative federalism"[398] or Professor Davidson's "cooperative localism"[399]—amount to top-down accounts of the role local governments play in carrying out, dissenting from, or modifying federal programs. In sharp contrast, privacy localism requires

394. *See* Christina M. Rodriguez, *Negotiating Conflict Through Federalism: Institutional and Popular Perspectives*, 123 YALE L.J. 2094, 2095–98 (2014).

395. *See, e.g.*, Joseph Blocher, *Firearm Localism*, 123 YALE L.J. 82, 124–29 (2013) (arguing that Second Amendment doctrine and state preemption laws should incorporate differences between urban and rural gun use and regulation); Olivier Sylvain, *Broadband Localism*, 73 OHIO ST. L.J. 725, 800–11 (2012) (objecting to state laws prohibiting local governments from creating their own broadband infrastructure to fill the service gap left by major broadband providers); *see also* Nestor M. Davidson, *Localist Administrative Law*, 126 YALE L.J. 564, 596 (2017) (identifying three structural dimensions of local government: vertical local-state relationships; horizontal local-local relationships; and internal relationships within a single local government). This Article focuses almost exclusively on the vertical dimension.

396. Davidson, *supra* note 395, at 570–71.

397. *See* Nestor M. Davidson, *Cooperative Localism: Federal-Local Collaboration in an Era of State Sovereignty*, 93 VA. L. REV. 959, 966 (2007).

398. Jessica Bulman-Pozen & Heather K. Gerken, *Uncooperative Federalism*, 118. YALE L.J. 1256 (2009). The co-authors coin the term to emphasize that federal and state governments may be understood, not only in terms of rivalry (dual sovereignty) or collaboration (cooperative federalism), but also in terms of dissent and resistance.

399. Davidson, *Cooperative Localism*, *supra* note 397. Davidson coins this term to emphasize the importance of direct federal-local relations as opposed to the almost exclusive interest in federal-state interactions that still dominates debates over dual sovereignty.

a bottom-up account of how local law shapes local government activity in connection with potential challenges and conflicts from federal and state law.

A related point is that the federal government has created many privacy laws but has not implemented them by designing and funding federal regulatory programs. Obviously, there are many privacy laws addressing the data practices of federal agencies and specific sectors of the economy as well as the confidentiality of communications sought by law enforcement or national security agencies. But these laws do not create or require state officials to administer and implement federal privacy programs in the way that they administer and implement federal welfare, environmental, health care, immigration, or law enforcement programs.

Federal regulatory programs typically work by setting standards that must be satisfied to obtain federal funding.[400] These programs are not usually analyzed in terms of dual sovereignty but rather under the rubric of cooperative federalism, which rejects the idea of separate national and state spheres of powers and responsibilities in favor of more collaborative federal-state relationships in a variety of regulatory contexts.[401] Under cooperative federalism, federal agencies rely on state assistance in carrying out federal regulatory programs. As Professor Spencer Admur notes, this may entail "state entities disbursing federal funds, federal and state regulators developing joint regulatory standards, or collaborative enforcement."[402] A striking feature of cooperative federalism is that federal agencies use "inducement strategies" to secure state and local assistance and aid such as solicitation, offers, trades, threats, prohibitions and mandates.[403] These, in turn, raise numerous and complex constitutional issues regarding constraints on federal power under the commandeering prohibition and the newly-minted coercion

400. Medicaid is an obvious example. States operate their Medicaid programs within federal standards and a wide range of state options in exchange for federal matching funds. *See* Samantha Artiga et al., *Current Flexibility in Medicaid: An Overview of Federal Standards and State Options*, KFF (Jan. 31, 2017), https://www.kff.org/medicaid/issue-brief/current-flexibility-in-medicaid-an-overview-of-federal-standards-and-state-options/ [https://perma.cc/DRM5-Y4G3].

401. *See* Philip J. Weiser, *Federal Common Law, Cooperative Federalism, and the Enforcement of the Telecom Act*, 76 N.Y.U. L. REV. 1692, 1695–96 (2001).

402. Spencer E. Admur, *The Right of Refusal: Immigration Enforcement and the New Cooperative Federalism*, 35 YALE L. & POL'Y REV. 87, 90 n.10 (2016).

403. *Id.* at 88.

prohibition.[404] Very few federal privacy programs employ such inducement strategies.[405]

As noted above, *Condon* turns on the fact that "[t]he DPPA regulates the States as the owners of data bases."[406] But this is the sole case suggesting that principles of federalism are relevant to the interaction of federal and state/local regulation of privacy. No other federal privacy statute so directly regulates state programs. Nor have there been any successful challenges to federal privacy laws on the grounds that they violate the anti-commandeering doctrine.[407] One reason for this is that both *Condon* and *Printz* articulate the anti-commandeering doctrine as a limit on what Congress can force states to do regarding federal regulatory programs. As the Court emphasizes, Congress can neither "compel the States to enact or enforce a federal regulatory program" nor command state officials "to administer or enforce a federal regulatory program."[408] When it comes to privacy law and policy, however, there are few if any "federal regulatory programs" whose primary concern is the disclosure or safeguarding of personal information.

For example, there are no programs that promote privacy by providing federal funds to train chief privacy officers in how to establish and manage a privacy program or conduct effective privacy impact assessment

---

404. *See* Nat'l Fed'n of Indep. Bus. v. Sebelius, 567 U.S. 519 (2012) (striking down the provision of the Affordable Care Act (ACA) that conditioned all of a state's Medicaid funding on its acceptance of the statute's expansion of Medicaid because this limit on conditional spending was unconstitutionally coercive).

405. One of the few exceptions is the State Health Information Exchange (HIE) Cooperative Agreement Program, which is a federally funded program "to rapidly build capacity for exchanging health information across the health care system both within and across states." Office of the Nat'l Coordinator for Health Info. Tech., *State Health Information Exchange*, HEALTHIT.GOV (Mar. 14, 2014), https://www.healthit.gov/policy-researchers-implementers/state-health-information-exchange [https://perma.cc/9DF9-4Y5S].

406. Reno v. Condon, 528 U.S. 141, 151 (2000).

407. *See* Int'l Sci. & Tech. Inst. Inc. v. Inacom Commc'ns, Inc., 106 F.3d 1146, 1150 (4th Cir. 1997) (upholding the Telephone Consumer Protection Act's grant of exclusive enforcement jurisdiction to state courts against a New York challenge); Ameritech Corp. v. McCann, 308 F. Supp. 2d 911, 925 (E.D. Wis. 2004), *vacated on other grounds*, 403 F.3d 908 (7th Cir. 2005) (rejecting a *Printz* commandeering challenge against the ECPA); Nat'l Fed'n of Republican Assemblies v. United States, 218 F. Supp. 2d 1300, 1344 (S.D. Ala. 2002) (upholding IRS provision that required political organizations to disclose state and local political contributions or lose federal filing status); Ass'n of Am. Physicians & Surgeons, Inc. v. U.S. Dep't of Health & Human Res., 224 F. Supp. 2d 1115, 1126 (S.D. Tex. 2002) (sustaining HIPAA-related privacy regulations); Citicasters, Inc. v. McCaskill, 883 F. Supp. 1282, 1288 (W.D. Mo. 1995) (rejecting challenge to the Privacy Protection Act of 1980, which forbade disclosure of materials seized in law enforcement investigations to third parties); Michigan v. Meese, 666 F. Supp. 974, 979–80 (E.D. Mich. 1987), *aff'd*, 835 F.2d 295 (6th Cir. 1988) (per curiam) (rejecting Tenth Amendment challenge to the ECPA).

408. *Condon*, 528 U.S. at 149.

techniques based on risk analysis or the design and development of privacy-preserving technologies.[409] And while a few federal agencies do engage in such activities—notably, the Federal Trade Commission (FTC), the National Institute of Standards (NIST), and the National Science Foundation (NSF)—they do so by bringing enforcement actions, issuing guidelines and, holding workshops (FTC); issuing standards and conducting research (NIST); and funding academics to engage in privacy engineering research (NSF). They do not carry out these tasks by creating regulatory programs that state and local officials administer and implement with federal funding. They could, but they do not.[410]

Of course, there are federal programs that require federal-state cooperation and raise privacy concerns. Most of these are domestic intelligence programs that rely very heavily on local actors to conduct surveillance, profiling-based investigation, and data collection and sharing. A few such programs condition grants and funding on federal guidelines "such as information-sharing protocols to promote uniformity as well as privacy standards."[411] But a closer look at these privacy standards shows that they amount to little more than assistance in developing a privacy policy—and no one who works in the privacy field would confuse posting a privacy policy with a full-fledged "privacy program." This may sound like hairsplitting. But domestic intelligence programs are not about privacy. They are about national security and consist of federal efforts to promote local national security activities by (1) providing "resources and training to state and local police forces to help them establish intelligence units, build databases, and develop standards for intelligence gathering"[412] or (2) funding state-operated fusion centers to "compile, analyze, and route electronically stored law enforcement and investigative information, including public as well as private sector data."[413] That said, the privacy aspects of national security programs have resulted in a limited set of disputes between federal and

409. COMPUTING CMTY. CONSORTIUM, PRIVACY BY DESIGN—ENGINEERING PRIVACY (2015), https://cra.org/ccc/wp-content/uploads/sites/2/2015/12/PbD3-Workshop-Report-v2.pdf [https://perma.cc/P2E4-XDPR].

410. *See* Crump, *supra* note 23, at 1658 (noting that "the federal government could require that all federally funded surveillance technology be governed by a data management protocol that addresses the fundamental questions of data collection, retention, use, and sharing"). This would amount to a federal privacy program.

411. Waxman, *supra* note 48, at 312.

412. *Id.* at 307.

413. *Id.* at 308.

state or local officials that resemble conflicts over federalism.[414] But they are weak examples at best of federal privacy programs.

To sum up: the two most prominent conceptions of federalism—dual federalism and cooperative federalism—make assumptions about the interaction of federal, state, and local government officials and the existence of federal regulatory programs that do not match up very well with the current structure of privacy law. Cooperative federalism is clearly better suited than dual sovereignty for the task of understanding top-down federal programs in which Congress provides the basic legal framework and delegates to a federal agency the power to administer the program in collaboration with state and local officials.[415] While this model sheds light on the workings of domestic intelligence programs, both cooperative (and uncooperative) federalism seem far less useful in understanding bottom-up programs in which local governments use their own regulatory powers to overcome gaps in federal policy.[416] Privacy localism, in contrast, does not depend on local government prevailing in disputes with state (or federal) authorities but instead tends to (1) fill gaps in existing federal and state privacy law or (2) where such laws exist, raises the floor established by federal or state constitutional or statutory rules.

Perhaps the best approach to federalism for purposes of understanding local privacy regulation is that of Professor Cristina Rodriguez, who sees federalism as consisting not in a "fixed set of relationships" but instead treats its parameters as "subject to ongoing negotiation by the players in the system, according to the advantages each might accrue from a particular set of relations."[417] This more flexible approach enables Rodriguez to focus on how debates over controversial social welfare issues like immigration, marriage equality, drug policy, and healthcare reform—and perhaps local surveillance and smart city initiatives as

414. Several scholars have argued that so-called "anti-Patriot Act resolutions" show state and local officials relying on the anti-commandeering doctrine to push back against federal policies that threaten individual liberty. *See generally* Ann Althouse, *The Vigor of the Anti-Commandeering Doctrine in Times of Terror*, 69 BROOK. L. REV. 1231, 1232–34 (2004); Bulman-Pozen & Gerken, *supra* note 398; Young, *supra* note 364.

415. *See* Weiser, *supra* note 401, at 1695–1703.

416. Although Bulman-Pozen and Gerken offer an account of the ways in which state and local officials can resist mandates and challenge federal authority, their theory of uncooperative federalism shares certain assumptions with cooperative federalism as to the primacy of federal regulatory programs. *See* Bulman-Pozen & Gerken, *supra* note 398, at 1271 (stating that "[m]uch of uncooperative federalism takes place in the interstices of federal mandates").

417. Rodriguez, *supra* note 394, at 2095.

well—play out in what she calls "the discretionary spaces of federalism."[418]

B. Federal Preemption

Congress's broad preemption power allows it to block, limit, or invalidate local privacy laws; federal preemption may be express or implied.[419] Implied preemption covers both field preemption, where federal regulation is so pervasive that Congress leaves no room for state laws on the subject, and conflict preemption, where compliance with both federal and state law is impossible, or state laws undermine the accomplishment of Congressional objectives.[420]

The leading privacy casebook implicates twenty-four relevant federal privacy statutes.[421] A review of these statutes shows that none of them interfere with the city-level privacy regulation under consideration in this Article; indeed, only two sufficiently overlap with local privacy laws to require extended analysis.[422] The two are ECPA, the federal electronic

---

418. *Id.* at 2097–98.

419. *See* Gade v. Nat'l Solid Waste Mgmt. Ass'n, 505 U.S. 88, 96–98 (1992).

420. *Id.*

421. SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 1, at 37–40. The total of twenty-four privacy statutes requires subtracting from the co-authors' list several laws that merely amend or expand existing laws and adding in several laws that are considered elsewhere in their case book such as the Freedom of Information Act (FOIA), *supra* at 609–12, and the Federal Trade Commission (FTC) Act, *supra* at 865.

422. Twelve of the twenty-four statutes may be dispensed with immediately because they only apply to federal agencies, see Freedom of Information Act, 5 U.S.C. § 552 (2012); Privacy Act of 1974, 5 U.S.C. § 552a; Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a, or to exclusively federal activity like foreign intelligence gathering, see Foreign Intelligence Surveillance Act of 1978, 15 U.S.C. §§ 1801–1811 (2012); USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended under scattered sections of 12 U.S.C.) (amending FISA and ECPA, and the FISA Amendments Act of 2008). Others only apply to specific sectors such as banks, see Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114-2 (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C.), or telecommunication providers, see Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §§ 1001–1010 (2012), or they may govern all federal, state, and local governmental agencies in a very narrow sphere, see Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401; Privacy Protection Act of 1980, 42 U.S.C. § 2000aa, or all employers in a narrow sphere, see Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105, or restrict permissible uses of a very limited type of record, see Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725, or criminalize certain conduct not at issue here, see Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028, Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801. Nine more of the remaining twelve statues fall away because they regulate commercial data held by private firms, either via sectoral laws, see Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (see also the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in scattered sections of 15 U.S.C.) (amending and updating the FCRA)), Cable Communications Policy Act of 1984, 47 U.S.C. § 551; Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710–2711,

surveillance statute, and HIPAA, the federal statute governing the privacy of certain medical records.[423] Few federal privacy laws include express preemption clauses[424] and those that do typically establish a "floor"—that is, a minimum standard that states may exceed.[425] Both ECPA and HIPAA lack preemption clauses and establish a federal floor that states may exceed.

ECPA has three parts: an updated version of the Wiretap Act; the Stored Communication Act (SCA); and the Pen Register Act (PRA).[426]Although state wiretap laws have been in existence for nearly the same period as the Wiretap Act, the federal law does not preempt these state enactments. To the contrary, looking to the legislative history of the Wiretap Act, the Senate Report states: "The proposed provision envisions that States would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation."[427] Rather, the Wiretap Act is a classic example of a federal privacy floor.[428] Nearly every state

---

Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227, Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506, Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801–6809, CAN-SPAM Act of 2003,15 U.S.C. §§ 7701–7713, or consumer protection laws, and thus have little to do with the privacy aspects of government activity, see Federal Trade Commission Act, 15 U.S.C. § 45; Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001–2009. Finally, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g(a)(4)(A), is mainly a federal conditional funding law, which also protects the privacy of student records containing personal information directly related to a student and maintained by any educational agency or institution. But FERPA establishes a federal floor for student record confidentiality and access that does not preempt states from enacting more privacy-protective restrictions. *See id.*

423. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in 42 U.S.C. and 29 U.S.C.).

424. *See* SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS, *supra* note 112, at 187–93 (identifying CAN-SPAM, COPPA, FCRA, and the PPA as privacy statutes that contain a preemption clause).

425. Schwartz, *Preemption and Privacy*, *supra* note 45 at 919–22.

426. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C §§ 2510–2522, 2701–2709.

427. *See* S. Rep. No. 90-1097, at 98 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2187. At least one court has held that ECPA preempts California's wiretap law, see *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 155–56 (C.D. Cal. 2007), but the court's reasoning seems flawed. *See* PROSKAUER ON PRIVACY, *supra* note 103, § 6.2.6.

428. *See* Schwartz, *Preemption and Privacy*, *supra* note 45, at 919–20. Schwartz points out while the VPPA and GLB Act also set a federal "floor" for privacy, "federal privacy legislation has also preempted state legislation with the effect of weakening existing state standards," citing FACTA as an example. *Id.* But FACTA was a trade-off between the credit industry and consumer advocates, with the former motivated to support several measures that strengthened consumer credit laws in exchange for making permanent certain preemption provisions in FCRA that were otherwise set to expire. *See Federal Law Targets ID Theft*, CONSUMER ACTION (Sept. 1, 2004), http://www.consumer-action.org/news/articles/fall_2004#Topic_02.pdf [https://perma.cc/7NUL-8KUD]. Indeed, FACTA is the *only* example of a federal privacy law that reverses existing state safeguards.

has its own surveillance laws closely patterned on the Wiretap Act,[429] and a dozen states have laws that exceed federal standards by enacting "all party" consent laws that are more restrictive than the "one party" rule under the Wiretap Act.[430] As for the SCA, most states do not protect communications held in storage by an electronic service (such as an email provider) in the same manner as the SCA.[431] Rather, similar protections are more commonly found in state privacy, consumer protection, or utilities regulation laws. Circuits are split regarding the preemptive effect of the SCA.[432] Finally, about half the states have laws regulating devices that capture outgoing or incoming phone calls and many of these laws are modeled on the PRA.[433] A review of these laws confirms that they closely resemble the PRA. Like the Wiretap Act, the PRA does not preempt stricter state laws.[434] In short, ECPA imposes few, if any, limits on states wishing to enact electronic communications legislation that is more protective than federal law.

HIPAA applies to health plans, healthcare clearinghouses, and healthcare providers and therefore regulates government agencies that engage in covered activities including local governments. The statute is quite clear that it provides a baseline of privacy protections but does not preempt more stringent state laws.[435] HIPAA also regulates disclosure of "protected health information" to law enforcement, permitting disclosure without consent or authorization if required by a court order, warrant, or subpoena when certain additional requirements are met.[436]

In short, the only two federal privacy laws that arguably overlap with local privacy laws do not actually prevent states or cities from enacting more stringent requirements. Further, local governments are not especially active in separately regulating electronic surveillance or protected health information, likely because ECPA and HIPAA already do so; there is little evidence that cities are seeking to innovate in these arenas by enacting local laws. Rather, local government officials follow

---

429. PROSKAUER ON PRIVACY, *supra* note 103, at § 6.2.5.

430. Schwartz, *Preemption and Privacy*, *supra* note 45, at 920.

431. The exception is Pennsylvania. *See* 18 PA. STAT. AND CONS. STAT. ANN. § 5741 (West 2018) (criminalizing unauthorized access to stored data).

432. *See* Prohibited Voluntary Disclosure under Stored Communications Act, 18 U.S.C.A. §§ 2701–2712 (2012), 9 A.L.R. Fed. 3d Art. 6 §§ 93–94 (2016).

433. *See* Bellia, *supra* note 45, at 882 n.50 (2009).

434. The main prohibition in the PRA begins with the phrase: "Unless prohibited by State Law," which suggests that Congress anticipated states enacting stricter standards. *See* 18 U.S.C. § 3122(a)(2). The Bill's legislative history supports this position as well. *See* S. Rep. No. 99-541, at 46 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3600.

435. *See* 45 C.F.R. § 160.203(A) (2018).

436. *See id.* § 164.512(2)(B).

the law of each higher level of government within the federal-state-local hierarchy, thereby meeting the federal floor or exceeding it when the applicable state standard is more protective. Thus, these two federal privacy laws are controlling when city officials can access, collect, use, or disclose electronic communications or protected health information. But in the absence of preemptive provisions and given the lack of activity at the local level, these laws do not seem to constrain local efforts to regulate surveillance technology or data governance practices.

C. The Threat of State Overrides Due to Lack of City Power

Do cities have sufficient power to regulate privacy at the local level? At first glance, it appears not. Of the three levels of government in the United States, city government is certainly weaker than federal or state government in terms of political power, fiscal resources, and constitutional standing.[437] Indeed, the conventional view is that, as sub-national governments, cities enjoy only those specific powers granted to them under state constitutions and statutes, with the result that governors and state legislatures inevitably play an ongoing role in city governance.[438] States may also exercise powers over cities free from federal constitutional constraints or injunctive relief.[439] Thus, states can and do control or stymie urban initiatives even when they have the strong backing of powerful mayors.[440]

Local government autonomy has two aspects: the ability to initiate policy and the ability to resist encroachment from another governmental entity or from a private party.[441] Both aspects of local autonomy rest on what is known as "home rule."[442] Until the early twentieth century, many states limited the power of local governments to undertake independent action without a specific delegation of authority under a doctrine known

---

437. *See generally* GERALD E. FRUG & DAVID J. BARRON, CITY BOUND: HOW STATES STIFLE URBAN INNOVATION (2008); RICHARD SCHRAGGER, CITY POWER: URBAN GOVERNANCE IN A GLOBAL AGE (2016).

438. Barron, *supra* note 24, at 390; Richard Briffault, *Our Localism* (pt. 1), 90 COLUM. L. REV. 1, 7–8 (1990).

439. *See* FRUG & BARRON, *supra* note 437, at 44; SCHRAGGER, *supra* note 407, at 79.

440. *See* FRUG & BARRON, *supra* note 437, at ix–xiii (describing the New York State constraints on New York City's (former) Mayor Michael Bloomberg's power to alleviate Manhattan traffic by introducing congestion pricing).

441. Professor Nestor M. Davidson refers to these two aspects as *empowerment* and *immunity*, respectively. Nestor M. Davidson, *Cooperative Localism*, *supra* note 397, at 967 (2007); *see also* RICHARD BRIFFAULT & LAURIE REYNOLDS, STATE AND LOCAL GOVERNMENT LAW 346 (8th ed. 2016) (describing two aspects of home rule, which they refer to as "initiative" and "immunity").

442. FRUG & BARRON, *supra* note 437, at 31–43.

as "Dillon's Rule."[443] Home rule reverses the presumption in Dillon's Rule by giving local government the authority to take many kinds of action without state permission. Today, over forty states delegate this authority to local governments.[444] Home rule may be constitutional or statutory or a mixture of the two. Whatever the structure a state adopts, home rule empowers local governments by delegating broad—but by no means unlimited—regulatory and spending authority.[445]

Cities generally have sufficient power to make policy decisions about (1) local policing including surveillance activities and (2) local municipal services including any privacy safeguards applicable to the collection, use, and disclosure of personal data by local government agencies. Local policing is the paradigm case of regulatory power or what is more commonly referred to as "police power," the term used to describe state and local government's general authority over health, safety, and welfare.[446] Police power encompasses creating and managing a local police force and providing and managing municipal services. Arguably, this is true in every state, city, and town in the United States. It is certainly true in both Seattle and New York City.

D. State Preemption

Unlike federal preemption and lack of city power, state preemption of local privacy regulation poses a more serious and ongoing threat to privacy localism. Although state preemption of local laws generally follows the same analytic model as federal preemption,[447] there are over 700 state privacy statutes,[448] which make for a crowded regulatory arena that may leave little room for local privacy law. As noted above, progressive cities are increasingly taking the lead on a broad range of policy issues—but some states are fighting back. States have preempted local authority in areas ranging from labor and employment (such as local

---

443. *See* Paul A. Diller, *Intrastate Preemption*, 87 B.U. L. REV. 1113, 1140 (2007); Hugh D. Spitzer, *Home Rule vs. Dillon's Rule for Washington Cities*, 38 SEATTLE U. L. REV. 809, 813–24 (2015).

444. RICHARD BRIFFAULT ET AL., AM. CONSTITUTION SOC'Y FOR LAW & POLICY, THE TROUBLING TURN IN STATE PREEMPTION: THE ASSAULT ON PROGRESSIVE CITIES AND HOW CITIES CAN RESPOND 3 (2017), https://www.acslaw.org/wp-content/uploads/2017/09/ACS_Issue_Brief_-_Preemption_0.pdf [https://perma.cc/56NC-GWVQ].

445. *Id.*

446. *See* Diller, *supra* note 443, at 1123 n.47.

447. *Id.* at 1140 (noting differences in a few states not relevant here).

448. *See generally* ROBERT E. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (2015).

minimum wage rules), to civil rights (local anti-discrimination laws), to environmental protection (local fracking rules), to public health (local tobacco regulation), to immigration law (sanctuary cities).[449] Thus, both now and in the future, the greatest challenge to privacy localism comes from the possibility of state preemption.

In general, state law preempts local law in two situations: when a statute includes explicit language establishing a statewide scheme of regulation, or by implication when the state and local powers materially conflict.[450] Additionally, courts may limit preemptive effect where state law inadequately protects a right recognized in a state constitution.[451]

Apart from these general rules, there is no one-size-fits-all answer to which state privacy laws preempt city privacy regulations. Rather, most state privacy preemption issues begin (and end) with an analysis of the interaction of specific state privacy laws and specific city privacy regulations. For present purposes, this requires identifying and reviewing laws in Washington and New York that regulate specific surveillance technologies insofar as they may overlap with Seattle and New York City's local surveillance ordinances. At a minimum, this includes Washington and New York state laws regulating video cameras and/or facial recognition, ALPRs, and drones. Additionally, it is necessary to identify and review Washington and New York's laws that regulate government records or personal data collected by government agencies insofar as they overlap with Seattle and New York City's locally-adopted data governance rules.

449. *See* BRIFFAULT ET AL., *supra* note 444, at 5–8.

450. State courts decide when a conflict arises under state law and this is often a question of legislative intent. *See* Diller, *supra* note 443, at 1155.

451. In theory, this would include the right of privacy, which ten states have recognized in express constitutional provisions protecting personal privacy. *See* SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS, *supra* note 112, at 126–27 (identifying the ten states as Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington). The author has not found any cases limiting preemptive effect based on a right to privacy as enumerated in a state constitution.

This task is large but manageable. The analysis begins with a discussion of state regulation of a few specific surveillance technologies[452] and then turns to local government data laws.[453]

1. Laws Regulating Specific Surveillance Technologies

a. Video Surveillance and Facial Recognition

Video cameras observe and record activity in public spaces for many purposes, including: crime prevention and detection, security and safety, and counter-terrorism. They may be mounted on building facades, lamp posts, utility poles, or inside businesses and public facilities in any area that requires monitoring including airports, ATMs, banks, city streets, convenience stores, hotels, public transportation, and schools.[454] The first generation of video surveillance cameras (also referred to as closed-circuit television or CCTV) stored footage locally on analog videotapes. This meant that investigators had to physically retrieve and manually play back the tapes, which was cumbersome and inefficient. Today, advanced surveillance cameras take full advantage of digital formats, cloud storage, remote viewing, and controls. Most importantly, these new devices are compatible with video content analysis, which detects movement and even anomalous patterns of movement, and facial recognition

452. The state preemption analysis omits certain surveillance technologies which are available to SPD and NYPD: StingRay tracking devices (devices that simulate a cell tower and detect cell phone signals) and electronic toll collection systems (like Sound Transit's ORCA pass or the Metropolitan Transit Authority's MetroCard). StingRays are omitted because federal policy applies across the board, thereby avoiding localism issues. *See* U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 2–5 (2015), http://www.justice.gov/opa/file/767321/download [https://perma.cc/CT5N-5WQE] (explaining that Stingrays are regulated by a 2015 DOJ policy requiring federal, state, and local law enforcement to obtain a search warrant before using the device); *accord* Jones v. United States, 168 A.3d 703, 709–10 (D.C. 2017); Maryland v. Andrews, 134 A.3d 324, 328 (Md. 2016). Washington State also requires a warrant for the use of StingRays. *See* Cyrus Farivar, *Cops Must Now Get a Warrant to Use Stingrays in Washington State*, ARS TECHNICA (May 12, 2015, 6:49 AM), https://arstechnica.com/tech-policy/2015/05/cops-must-now-get-a-warrant-to-use-stingrays-in-washington-state/ [https://perma.cc/K3V5-MNX6]. Electronic toll collection systems are omitted because the fare cards in Seattle and New York City are not issued by the city but rather by regional transportation authorities, which are beyond the scope of this paper.

453. The rules governing acquisition of data by government agencies from other government agencies is beyond the scope of this Article. In future work, the author plans to analyze police department data sharing with other city agencies, with regional, state, or federal agencies, and with private sector firms.

454. *See* CONSTITUTION PROJECT, *supra* note 101.

applications, which automatically match a face in a digital image or a video frame to a person in a facial database.[455]

In recent years, surveillance cameras have become more prevalent in U.S. cities, thanks to lower costs and easier installation as well as the availability of government grants for cities to install surveillance camera networks.[456] Although proponents of video cameras argue that they enhance public safety by preventing or deterring crime and assisting in criminal prosecutions, there have been few credible studies,[457] and the evidence supporting these claims is mixed at best,[458] which only serves to heighten privacy-related concerns.

One of these concerns is the risk of abuse. There are documented cases of police officers using video data for criminal abuse (like blackmail), institutional abuse (such as spying on or harassing political activists), personal abuse (such as stalking women), discriminatory targeting (such as targeting black or Latino youth who enter a majority-white neighborhood), and voyeurism (such as male operators viewing or sharing video feeds of scantily clad women or acts of intimacy).[459] Additionally, video surveillance may capture (and store for later analysis) ordinary citizens exercising their First Amendment rights, thereby creating a chilling effect on political and religious expression.[460] Regardless of any

---

455. *See generally* LOREN SIEGEL, ROBERT A. PERRY & MARGARET HUNT GRAM, N.Y. CIVIL LIBERTIES UNION, WHO'S WATCHING?: VIDEO CAMERA SURVEILLANCE IN NEW YORK CITY AND THE NEED FOR PUBLIC OVERSIGHT (2006), https://www.nyclu.org/sites/default/files/publications/nyclu_pub_whos_watching.pdf (last visited Oct. 26, 2018).

456. *See* Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES (Oct. 14, 2013), https://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html (last visited Oct. 26, 2018). New York City's Domain Awareness System has about 9,000 video surveillance cameras linked together in a sophisticated network that also permits video content analysis. *See infra* text accompanying notes 55–59.

457. *See* U.S. GEN. ACCOUNTING OFFICE, GAO-03-748, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C. 29 (2003) ("There is general consensus among CCTV users, privacy advocates, researchers, and CCTV industry groups that there are few evaluations of the effectiveness of CCTV in reducing crime . . . .").

458. An exhaustive study of the effectiveness of San Francisco's video surveillance program found no evidence of an impact on violent crime and a decline in overall homicides in areas near the cameras but an increase in areas far from the cameras and statistically significant and substantial declines in property crime within view of the cameras. *See* JENNIFER KING ET AL., CITRIS REPORT: THE SAN FRANCISCO COMMUNITY SAFETY CAMERA PROGRAM (2008), www.popcenter.org/library/scp/pdf/219-King.pdf [https://perma.cc/9JBR-V5ZG].

459. *What's Wrong with Public Video Surveillance*?, ACLU (2018), https://www.aclu.org/other/whats-wrong-public-video-surveillance [https://perma.cc/AQ6H-X6UQ].

460. As Justice Sotomayor observed in a related context, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her

First Amendment concerns, the Fourth Amendment's reasonable expectation of privacy test has little application to silent video surveillance in public spaces.[461]

When law enforcement combines video surveillance systems with facial recognition technology (FRT), these privacy concerns are greatly increased. Although early experiments with the use of FRT in criminal investigations or airport security were disappointing, the technology is starting to improve and local police departments are renewing their interest in adopting FRT.[462] While still far from perfect, FRT is steadily improving in quality as recent advances in 3D imaging and machine learning have increased the reliability of the identification process.[463] Moreover, facial databases are expanding and now include not only mug shots but also driver's licenses and other types of ID photos; a recent study estimates that "law enforcement face recognition affects over 117 million American adults."[464]

Professor Laura Donohue argues that facial recognition represents the first of a series of next generation biometrics that when paired with surveillance of public space, transforms identification techniques in several ways. According to Donohue, "immediate" biometric identification is "focused (1) on a single individual; (2) close-up; (3) in relation either to custodial detention or in the context of a specific physical

---

familial, political, professional, religious, and sexual associations . . . . The Government can store such records and efficiently mine them for information years into the future." United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring) (citations omitted).

461. *See* SLOBOGIN, *supra* note 71, at 89–90. Several circuit courts have held that the Fourth Amendment requires heightened specificity for video surveillance warrants but only in non-public settings. *See, e.g.*, United States v. Williams, 124 F.3d 411 (3d Cir. 1997); United States v. Falls, 34 F.3d 674 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992); United States v. Torres, 751 F.2d 875 (7th Cir. 1984).

462. Clare Garvie & Alvaro Bedoya, *Smile! You've Just Been Identified by Face Recognition Technology*, N.Y. DAILY NEWS (Mar. 27, 2017), http://www.nydailynews.com/opinion/smile-identified-face-recognition-article-1.3008512 [https://perma.cc/9HBU-7GRQ] (noting that the NYPD has been using facial recognition technology in criminal investigations since 2011 and as of last year has conducted "more than 8,500 facial recognition investigations, with over 3,000 possible matches, and approximately 2,000 arrests" and plans to expand it use of this technology in the future (citations omitted)).

463. Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 554 (2012).

464. CLARE GARVIE ET AL., GEORGETOWN LAW CTR. ON PRIVACY & TECH, THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA (2016), https://www.perpetuallineup.org/background [https://perma.cc/N5R4-9W6Q]; *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-267, FACIAL RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 48 (2016) (stating that the FBI has access to more than 411 million facial images, including driver's license photos from sixteen states as well as visa application and passport photos from the State Department).

area related to government activity; (4) in a manner often involving notice and often consent; and (5) in a one-time or limited occurrence."[465] In contrast, "remote" biometric identification provides the government "the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner."[466] The intrusiveness of these remote techniques presents a unique challenge to liberty because they enable prolonged surveillance that will also occur more frequently yet require significantly fewer resources than existing systems.[467]

State Regulation of Video Surveillance—Most states do not regulate video surveillance of public spaces. Washington State's eavesdropping law does not cover silent video recording,[468] and its criminal procedure laws are non-specific regarding video surveillance warrants, which may fall within general warrant procedures requiring probable cause.[469] New York criminal procedure requires detailed warrants for individualized video surveillance.[470] These standards reflect heightened Fourth Amendment protections for video surveillance established by the Second Circuit because of the technology's capacity to capture large volumes of information.[471] But such procedures are limited to situations where warrantless surveillance would infringe on reasonable expectations of privacy, which the courts do not recognize in public places, making New York's procedural requirements inapplicable to video surveillance of streets and sidewalks.[472] Professor Susan Freidwald argues that all video surveillance implicates the same privacy concerns as wiretapping because it is "hidden, intrusive, indiscriminate and continuous" and thus should be subject to constitutional constraints.[473] Despite these and other calls to

---

465. Donohue, *supra* note 463, at 415–16 (2012).

466. *Id.* at 415.

467. *Id.* at 529.

468. *See* Haymond v. Wash. Dep't of Licensing, 73 Wash. App. 758, 761, 872 P.2d 61, 63 (Wash. App. 1994) (holding that WASH. REV. CODE § 9.73.030 "does not apply to the operation of a video camera without an audible sound recording").

469. WASH. REV. CODE § 10.79.035 (2018).

470. *See* N.Y. CRIM. PROC. LAW §§ 700.10–70 (McKinney 2018); 7-28 BENDER'S NEW YORK EVIDENCE § 28.30(2) (2018).

471. *See* United States v. Biasucci, 786 F.2d 504, 507–09 (2d Cir. 1986).

472. *See, e.g.*, Rodriguez v. United States, 878 F. Supp. 20, 25 (S.D.N.Y. 1995) (finding no protection from video surveillance of apartment building entrance by DEA from public street). *See generally* Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. TECH. L. REV. 589 (2012).

473. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 6 (2007).

impose limits on surveillance of public spaces, courts have yet to respond. But recognition of the "mosaic" capabilities of new technologies may well prove a catalyst for future change.[474]

State Regulation of Facial Recognition—A few states have been active in regulating commercial uses of biometrics, which under some definitions includes face scans.[475] In June 2017, Washington enacted a law regulating businesses that collect and use biometric identifiers for commercial purposes.[476] However, this law applies solely to biometric identifiers in commercial databases and excludes facial recognition data from the definition of such identifiers.[477] Although the Washington Legislature enacted a second bill regulating *state agency* collection, use, and retention of biometric identifiers (including facial recognition data),[478] this law applies to state, but not local, agencies[479] and exempts all "general authority Washington law enforcement agencies." [480] Thus, it does not apply to local police departments.

However, Seattle has stepped up to this regulatory task by developing strict controls restricting the SPD's use of facial recognition software to comparisons of unidentified images and jail mug shots.[481] SPD policy also requires reasonable suspicion that the person in the image has committed a crime and prohibits using the software to connect with live camera systems.[482] SPD developed this policy with input from ACLU-WA, secured approval of the policy by an independent body (the Seattle City Council), and published the policy online, all of which makes this policy unique among U.S. cities that regulate facial recognition technology.[483]

---

474. *See* Levinson-Waldman, *supra* note 101, at 539–42.

475. For example, the 2008 Illinois Biometric Information Privacy Act, 740 ILCS 14/1, requires that before collecting and storing any biometric identifier (defined as including face scans), the subject of collection must receive notice in writing of the specific purpose of collection and the length of time the identifier will be stored and must execute a written release before any biometric information is captured. However, these restrictions only apply to a "private entity" and this term "does not include a State or local government agency." *Id.*

476. H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017).

477. WASH. REV. CODE § 19.375.010 (2018).

478. H.B. 1717, 65th Leg., Reg. Sess. (Wash. 2017); WASH. REV. CODE § 40.26.020.

479. WASH. REV. CODE § 40.26.020(7)(a).

480. *Id.* § 40.26.020(8).

481. *See* Steven Miletich, *Seattle Police Win Praise for Safeguards with Facial-Recognition Software*, SEATTLE TIMES (Oct. 19, 2016), https://www.seattletimes.com/seattle-news/crime/seattle-police-wins-praise-for-safeguards-with-facial-recognition-software/ (last visited Oct. 26, 2018).

482. *Id.*

483. *Id.* The SPD policy is published in the Seattle Police Department Manual. SEATTLE POLICE DEPARTMENT MANUAL, *supra* note 130, § 12.045.

New York also introduced a bill modeled on the Illinois law, but it did not advance out of committee.[484] The NYPD, which has been using facial recognition technology since 2011, has been much less transparent than Seattle regarding its policies and procedures.[485]

b. Automatic License Plate Readers

ALPRs are computer-controlled, high-speed camera systems that automatically capture an image of every license plate that comes into view.[486] Many police departments now use them mounted on patrol cars or fixed objects (e.g., light poles, bridges, overpasses).[487] There are also applications that allow police officers to scan license plates with their smartphones.[488] When a license plate enters the camera's field, ALPRs capture an image of the car and its surroundings, and convert the image of the license plate into machine-readable alphanumeric text, which may be checked for matches against manually entered plate numbers and "hot lists" of the plate numbers of stolen cars, AMBER alerts, felony arrest warrants, registered sex offenders or people who are on supervised release.[489] ALPRs record and store data on each scanned licensed plate (regardless of whether a match or "hit" is generated), including the plate number and the date, time and place of recording.[490] It is also possible to aggregate ALPR data in centralized databases and trace a vehicle's past movements by plotting all of the license plate reads associated with a vehicle's owner or passenger. Additionally, ALPRs allow police to identify each vehicle seeking to enter a specific geographical area and construct a virtual fence around it.

As with any surveillance technology, the use of ALPRs by law enforcement presents a risk of abuse if officers use data to stalk,

---

484. *See* S.B. 4887, 238th Leg. Sess. (N.Y. 2015).

485. *See* Ava Kofman, *NYPD Refuses to Disclose Information About Its Face Recognition Program, so Privacy Researchers Are Suing*, INTERCEPT (May 2, 2017, 5:36 PM), https://theintercept.com/2017/05/02/nypd-refuses-to-disclose-information-about-its-face-recognition-program-so-privacy-researchers-are-suing/ [https://perma.cc/AZB7-DK9V].

486. ACLU, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS (2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/4MHS-DAAG].

487. DHS and DOJ are key sources of funding for the acquisition of license plate readers by local police departments. *Id.*

488. *See* Levine, *supra* note 55.

489. *See Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND., https://www.eff.org/sls/tech/automated-license-plate-readers [https://perma.cc/D5VT-LY52].

490. *Id.*

embarrass, or otherwise spy on innocent parties or engage in discriminatory targeting. This is especially problematic if police departments lack policies limiting access to license plate data or lack audit or other mechanisms for ensuring accountability.[491] Because ALPRs capture and retain information about every vehicle that crosses their path, rather than limiting such collection and retention to vehicles that generate a hit, they enable law enforcement to gain significant insight into people's movements over a span of months or even years. As discussed below, this would raise issues under both concurrences in *Jones* if the extended use of ALPRs is of sufficient duration and pervasiveness to constitute "long-term monitoring."[492] On the other hand, the police certainly treat current Fourth Amendment doctrine as permitting law enforcement use of ALPRs in any single instance because "an observation made by a police officer without a physical intrusion into a constitutionally protected area does not implicate the Fourth Amendment or require a search warrant."[493]

State Regulation of ALPRs—Over a dozen states permit the use of ALPRs by law enforcement but limit retention periods and sale to third parties, while exempting ALPR data from disclosure under state public record laws.[494] Washington has not regulated ALPRs, although the SPD has developed its own policy guidelines requiring certification and training of operators in the proper use of this technology, limiting the use of ALPRs to routine patrol and criminal investigations, and restricting access to ALPR data.[495] Seattle's surveillance ordinance does not apply to ALPRs because, as previously noted, it specifically excludes both cameras installed in or on police vehicles and certain stationary cameras.

In contrast, the New York State Senate is considering a bill prohibiting businesses and individuals from using ALPRs and limiting allowable uses

---

491. *See generally* Jennifer Lynch, *Automated License Plate Readers Threaten Our Privacy*, ELEC. FRONTIER FOUND. (2013), https://www.eff.org/deeplinks/2013/05/alpr?from=sls [https://perma.cc/54VT-PCY3].

492. *See supra* text accompanying notes 98–100; KEITH GIERLACK ET AL., RAND CORP., LICENSE PLATE READERS FOR LAW ENFORCEMENT: OPPORTUNITIES AND OBSTACLES 37–38 (2014), https://www.ncjrs.gov/pdffiles1/nij/grants/247283.pdf [https://perma.cc/9VXX-JEFY].

493. DIV. OF CRIMINAL JUSTICE SERVS., STATE OF N.Y., SUGGESTED GUIDELINES: OPERATION OF LICENSE PLATE READER TECHNOLOGY 10 (2011), http://www.criminaljustice.ny.gov/crimnet/ojsa/motor-vehicle/LPR-Operation-Suggested-Guidelines-2011.pdf [https://perma.cc/2QUV-EE73].

494. *See Automated License Plate Readers: State Statutes Regulating Their Use*, NAT'L CONF. ST. LEGISLATURES (Jan. 2, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx [https://perma.cc/7JR6-UJKN].

495. SEATTLE POLICE DEPARTMENT MANUAL, *supra* note 130, § 16.170.

by law enforcement agencies.[496] Additionally, the bill would limit the retention of captured plate data to no more than 180 days with certain exceptions. Finally, the bill would require law enforcement agencies to destroy evidence gathered with ALPRs unless they "apply for a court order for disclosure of captured plate data" while offering "specific and articulable facts showing that there are reasonable grounds to believe that the captured plate data is relevant and material to an ongoing criminal or missing persons investigation."[497] Both the Senate bill and (weaker) Assembly bill remain in committee.

c. Drones

"Unmanned aerial vehicles" (UAVs), commonly known as drones, raise surveillance issues because they are often equipped with digital recorders, microphones, and other sensors. UAVs range from small "quadcopters" that can hover near ground level to high-altitude planes with extremely powerful cameras. Many cities in the United States have acquired the smaller UAVs for non-controversial purposes such as handling bomb threats, search and rescue missions, and crime-scene photography.[498] But UAVs also facilitate ubiquitous government surveillance, combining cost-effectiveness with high levels of technical capability.[499] Commentators suggest that U.S. law enforcement is expanding its use of drones for surveillance purposes,[500] while drone use by hobbyists and commercial firms raises separate but related privacy concerns ranging from voyeurism to corporate espionage. As Professor Ryan Calo reminds us, "George Orwell specifically describes small flying devices that roam neighborhoods and peer into windows."[501] Orwell's

496. S.B. S23, 2017–2018 Leg., Reg. Sess. (N.Y. 2018). The amended version of a companion bill in the N.Y. State Assembly all but eliminates the requirements on law enforcement. *See* Shane Trejo, *Fail: New York Assembly Committee Guts Bill to Limit Automatic License Plate Readers*, TENTH AMENDMENT CTR. (June 1, 2016), http://blog.tenthamendmentcenter.com/2016/06/fail-new-york-assembly-committee-guts-bill-to-limit-automatic-license-plate-readers/ [https://perma.cc/U4ZA-A592].

497. Additionally, New York has set out suggested guidelines for the operation of ALPR technology in the form of best practices that sought to "provide authorized users with the information necessary to ensure public safety while protecting individual privacy rights." *See* DIV. OF CRIMINAL JUSTICE SERVS., *supra* note 493.

498. *See* Marc Jonathan Blitz et al., *Regulating Drones Under the First and Fourth Amendments*, 57 WM. & MARY L. REV. 49, 54–55 (2015).

499. *See id.* at 56–59.

500. *See Domestic Drones*, ACLU (2016), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones [https://perma.cc/T8KC-VH83].

501. *See* M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 32 (2011).

1984 is the starting point for imagining the level of intrusion society may expect from silent, low-cost, low-profile, highly maneuverable devices, outfitted with digital cameras and microphones, and wireless connections to the cloud. But the end point may look more like the constant surveillance of *Blade Runner 2049*.[502]

State Regulation of Drones—Almost two-dozen states regulate drone privacy, requiring law enforcement agencies to obtain a warrant prior to their use for surveillance.[503] In Washington, the legislature passed a bill that would have placed limits on the use of drones for law enforcement purposes.[504] But the governor vetoed the bill citing concerns about conflicting provisions on public disclosure and the definition of public information, while simultaneously announcing the creation of a task force to study surveillance technology and postponing any purchasing of UAVs pending completion of the study.[505] In 2016, Washington's Chief Privacy Officer issued drone guidelines encouraging law enforcement officials to use drones only in connection with properly authorized investigations and activities, respect existing state and federal laws and regulations regarding the privacy of personal information, and respect civil rights.[506]

In New York, the legislature has introduced three bills to regulate the use of drones by law enforcement. The strictest bill bans drone surveillance in "locations where a person would have an expectation of privacy," with exceptions for the use of drones in "exigent circumstances"

---

502. BLADE RUNNER 2049 (Warner Bros. 2017).

503. *See* Allie Bohm, *Drone Legislation: What's Being Proposed in the States?*, ACLU (Mar. 6 2013, 3:15 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/drone-legislation-whats-being-proposed-states [https://perma.cc/4L7H-5DX7]. At the federal level, the Federal Aviation Administration (FAA) regulates UAVs with respect to commercial use, safety, and licensing, but not privacy. *See* Stephanie Condon, *FAA Sued for Lack of Drone Privacy Rules*, ZDNET (Aug. 24, 2016, 1:00 PM), http://www.zdnet.com/article/faa-sued-for-lack-of-drone-privacy-rules/ [https://perma.cc/4PFQ-WE5D]. Congress has considered a number of drone privacy bills, including several versions of the Drone Aircraft Privacy and Transparency Act, a bill that would "require law enforcement agencies . . . to describe how they plan to minimize the collection and retention of data that's unrelated to a crime investigation" and "to obtain a warrant before conducting surveillance" subject to certain exceptions. *See* Jennifer Martinez, *Markey Introduces Drone Privacy Bill*, HILL (Dec. 18, 2012, 7:54 PM), http://thehill.com/policy/technology/273519-markey-introduces-drone-privacy-bill [https://perma.cc/7QSZ-4MTA].

504. *See* H.B. 2789, 63d Leg., Reg. Sess. (Wash. 2014). A bill that is similar to H.B. 2789 is now pending in the state legislature. *See* H.B. 1102, 65th Leg., Reg. Sess. (Wash. 2017).

505. *See* Leilani Leach, *Washington Gov. Jay Inslee Vetoes Drone Bill*, GOV'T TECH. (Apr. 18, 2014), http://www.govtech.com/state/Washington-Gov-Jay-Inslee-Vetoes-Drone-Bill.html [https://perma.cc/T7FN-SSB2].

506. OFFICE OF PRIVACY & DATA PROT., STATE OF WASH., WASHINGTON STATE POLICY GUIDELINES FOR UNMANNED AIRCRAFT SYSTEMS (2016), http://www.wsdot.wa.gov/NR/rdonlyres/AC738BE5-FDCE-4FD9-A173-6C913FDABE24/0/DronePolicyGuidelines.pdf [https://perma.cc/CFS7-KTMQ].

or pursuant to a search warrant in investigations of serious crimes.[507] A second bill imposes similar restrictions on law enforcement use but contains additional privacy restrictions applicable to all state agencies.[508] A third bill bans warrantless use of UAVs (with a few exceptions) and voids the use of such evidence in criminal proceedings.[509] All three bills were introduced in earlier sessions but did not advance.

2. Laws Regulating the Privacy of Government Records

Few states regulate the data governance practices of state agencies in a manner comparable to the Privacy Act or have anything resembling the Privacy Act's requirement for publishing SORNs or PIAs.[510] This broad generalization requires further clarification. All fifty states have public record or freedom of information laws requiring government agencies to disclose certain information to people upon request.[511] Most of these are patterned after FOIA. These state counterparts typically apply to both state and local agencies; this is certainly true in both Washington and New York.[512] These laws generally include some form of privacy exemption, which may be similar (or more restrictive) than the two privacy exemptions in FOIA.[513]

The Washington Public Records Act (PRA) is unusual in that it combines a very broad public disclosure requirement[514] with a very narrowly construed privacy exemption that parallels the elements of the tort of public disclosure of private facts.[515] Thus, an agency exempting information from a record must do so based upon an independent statute that creates a right to privacy and that outweighs the PRA's broad policy

---

507. S.B. 1174, 2017 Leg., Reg. Sess. (N.Y. 2017).

508. A.B. A3396, 2017 Gen. Assemb., Reg. Sess. (N.Y. 2017).

509. S.B. 2913, 2017 Leg., Reg. Sess. (N.Y. 2017).

510. *See supra* notes 114 and 115.

511. For a list of all fifty laws, see SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS, *supra* note 112, at 119–21.

512. *See, e.g.*, Washington Public Records Act, WASH. REV. CODE § 42.56.010(1) (2018); N.Y. PUB. OFF. LAW § 86(3) (McKinney 2017).

513. *See* Freedom of Information Act, 5 U.S.C. §§ 552(b)(6)–(b)(7)(C) (2012).

514. *See, e.g.*, WASH. REV. CODE § 42.56.030 (stating that the public disclosure requirements "shall be liberally construed and its exemptions narrowly construed" to promote the policy of an informed public); *see also* Sargent v. Seattle Police Dep't, 179 Wash. 2d 376, 385, 314 P.3d 1093, 1097 (2013) (discussing how the PRA mandates "broad public disclosure").

515. *See* WASH. REV. CODE § 42.56.050 (limiting exemptions to disclosures of personal information that are highly offensive to a reasonable person and not of legitimate concern to the public).

in favor of disclosing records.[516] In *Does v. King County*,[517] the Washington Court of Appeals found that individuals did not have a right to privacy when they were captured on surveillance video of a public area.

New York's FOIL also provides citizens with access to records related to government operations subject to various exemptions. This includes a standard privacy exemption for information that "if disclosed would constitute an unwarranted invasion of personal privacy."[518] The statute offers several examples of unwarranted invasions[519] and in cases beyond these explicit terms courts "must decide whether any invasion of privacy . . . is 'unwarranted' by balancing the privacy interests at stake against the public interest in disclosure of the information."[520] New York law also includes a provision that broadly exempts police and other uniformed officers from the reach of the FOIL,[521] which arguably blocks the public disclosure of footage from body-worn cameras.[522]

Finally, Washington and New York both have several narrower state privacy laws that may affect how cities treat specific records including school records,[523] medical records concerning HIV/AIDS status,[524] and library records.[525]

In sum, the threat of state preemption of local privacy regulation turns out to be less severe than anticipated. Most states (including Washington and New York) either do not regulate law enforcement's use of the surveillance technologies highlighted above or impose requirements that would not conflict with local surveillance laws. Only ten states (including New York but not Washington) regulate the data governance practices of state agencies but none of these laws apply to local governments. It follows that both Seattle and New York City have a relatively free hand in regulating surveillance technologies and devising local data governance policies and practices. Most importantly, even if New York enacted pending ALPR or drone bills, these laws would likely set state floors on

---

516. For example, personal information in agency employee files is exempt if disclosure would violate the employee's right to "privacy." *See* WASH. REV. CODE § 42.56.230(3).

517. 192 Wash. App. 10, 366 P.3d 936 (2015).

518. N.Y. PUB. OFF. LAW § 87(2)(b) (McKinney 2017).

519. *Id.* § 89(b)(2)(b).

520. *In re* New York Times Co. v. N.Y.C. Fire Dep't, 829 N.E.2d 266, 269–70 (N.Y. Ct. App. 2005).

521. N.Y. CIVIL RIGHTS LAW § 50-a (2018).

522. *See* Cynthia Conti-Cook, *Open Data Policing*, 106 GEO. L.J. ONLINE 1, 3 (2017).

523. WASH. REV. CODE § 28A.605.030 (2018); N.Y. EDUC. LAW § 3222.

524. WASH. REV. CODE § 70.02.220; N.Y. PUB. HEALTH LAW § 2782.

525. WASH. REV. CODE § 42.56.310; N.Y.C.P.L.R. § 4509.

local activity without preventing the city from strengthening these privacy protections or devising more comprehensive regulatory schemes governing all surveillance technology and all local government data.

Finally, suppose that Washington or New York were to enact laws directly covering surveillance technologies or local data governance? Wouldn't such laws preempt the local privacy regulations under consideration in Part II and render them superfluous? In fact, one need not look further than California to determine what a state law on surveillance technology might look like and how it would affect local surveillance ordinances in Santa Clara County, Oakland, Berkeley, and Palo Alto. Senate Bill 21 (S.B. 21) requires transparency and accountability in decisions about the use of surveillance technology.[526] It is highly consistent with local surveillance ordinances already in effect in California's cities and preserves their underlying structure by requiring all local law enforcement agencies to develop use polices for surveillance technologies and seek executive approval at the local or regional level before deployment. Indeed, as one legislator stated, S.B. 21 "is inspired in part by a Santa Clara County ordinance . . . passed in 2016."[527] Once again, the California legislature serves as a laboratory for policy experimentation, in this case by responding to innovative city regulations by emulating them, not supplanting them, and enacting a state law mandating local or regional approval. Of course, one can also imagine state legislatures doing the opposite by passing laws to prevent cities from enacting surveillance ordinances, arguing that they stymie law enforcement efforts. But so far this has not been the case in the seventeen states that have passed or considered local surveillance ordinances.[528]

CONCLUSION

Seattle and New York City have begun to experiment with local privacy regulation in a thoughtful and innovative fashion, cognizant both of gaps in federal and state privacy law and the importance of working within their limited power and immunity as local governments. It is too soon to determine the extent to which these surveillance ordinances and city privacy principles will achieve their stated goals, or whether they will require further refinement in response to emerging issues. Nevertheless, it is already clear that both cities have embraced a novel approach to regulating local surveillance that transcends the limitations of modern

526. S.B. 21, 2017–2018 Leg., Reg. Sess. (Cal. 2017).

527. Hearing on S.B. 21 Before the Assemb. Comm. on Privacy and Consumer Protection, 2017–2018 Leg. (July 10, 2017) (written summary by Ed Chau, Comm. Chair).

528. For a map of these states, see *supra* note 20.

Fourth Amendment doctrine, related federal statutes, and piecemeal state legislation. Both cities have taken important steps toward appropriately balancing the potential benefits of smart city and open data programs and the public demand for transparency, privacy, and trust in elected officials. While obstacles remain, these cities are less susceptible to federal or state override because they are acting well within their "police powers" and enacting laws that either do not conflict with federal or state statutes or exceed the floor these statutes establish.

Other cities, too, are embracing privacy localism as described in this Article. Assuming the Seattle and New York City experiments achieve their promise of more democratic policing and smarter but more trustworthy municipal services, these trends may expand to additional locales as well. At the very least, the potential success of privacy localism may inspire federal and state regulators to develop more robust privacy frameworks that benefit everyone regardless of locale. Thus, privacy localism has the potential to shape emerging privacy norms in a world that is increasingly urban and increasingly focused on harnessing big data to serve the public good.