October 28, 2017 Draft
(Please do not redistribute)

Privacy Localism

Ira Rubinstein

Senior Fellow, Information Law Institute, New York University School of Law
Senior Fellow, Future of Privacy Forum

Dear Conference Attendees,

This is a substantially revised version of an earlier draft presented at the June 2017 Privacy Law Scholars Conference. However, it is still a work in progress. The discussion of body camera policies in Part III is missing s is the concluding section of Part IV.C and the Conclusion. And the footnotes need to be finalized. But I think there is enough here for a productive discussion and I look forward to your thoughts and comments.

Many thanks.

Ira Rubinstein

TABLE OF CONTENTS

INTRODUCTION
I. LOCALSIM AND FEDERALISM
A. Privacy and the Principles of Federalism
B. Federal Preemption of Local Privacy Law
1. Three Federal Privacy Statutes: ECPA, FERPA, and HIPAA
2. New Federal Privacy Laws?
II. EMPOWERMENT AND IMMUNITY IN LOCAL GOVERNMENT
A. City Power to Regulate Privacy
B. State Preemption of City Privacy Regulation
1. Public Surveillance Technology
a. Video Cameras/Facial Recognition Technology
b. Automatic License Plate Readers
c. Drones
2. Data Governance Practices
III. CASE STUDIES: PRIVACY IN THE CITY
A. Seattle
1. Seattle's Surveillance Ordinance
2. Seattle's Privacy Principles and Processes
B. New York City
1. NYC's Public Security Privacy Guidelines and Proposed Surveillance Ordinance
2. NYC's Privacy Principles
IV. THE CASE FOR PRIVACY LOCALISM
A. Assessing Local Privacy Regulation in Seattle and New York
1. Anticipated Benefits
2. Policy Concerns
B. The Public Surveillance Gap
1. Privacy in Public
2. The Fourth Amendment Gap
3. The Statutory Gap
4. Closing the Gap
C. Policing and Democratic Governance
CONCLUSION

INTRODUCTION

Privacy law in the United States is a curious amalgam of constitutional protections under the First, Fourth, and Fourteenth Amendments; federal statutory protections related to government records, law enforcement, and national security; federal sectoral laws protecting privacy in health care, financial services, Internet services and other sectors of the national economy; and hundreds of state privacy laws covering law enforcement, government records, medical and genetic information, financial privacy, consumer data, business records, and data security.[1] One thing not mentioned in any privacy case book or treatise, however, is local privacy laws and regulations. Nor is this surprising. To date, cities have played but a minor role in information privacy law. This is beginning to change for several reasons.

American cities, especially large urban centers, are data-rich environments. Obviously, cities have large populations and city dwellers generate a vast amount of data through their daily interaction with cameras and sensors as they crisscross public spaces, their encounters with local police, and their use of 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, police dashboard and body cameras, and gunfire location services to assist them in maintaining public order, enforcing criminal laws, and safeguarding citizens against terrorist attacks.

In New York and a few other cities, these surveillance efforts take place at a very broad scale.[2] Every city also offers a diverse range of services touching almost every resident. They collect data related to transportation, education, child welfare, housing, health and other social services. And many cities are transforming themselves into "smart" cities.[3] As such, they collect and analyze massive data sets to make municipal services more efficient and effective, and they are starting to deploy Internet of Things (IoT) devices, smart grid systems, and related mobile apps, thereby ensuring that smart services are more readily accessible to city residents (while collecting ever more data in the process).[4] Whether police take advantage of smart city data for law enforcement purposes is unknown. In any case, both local police forces and civilian agencies now must grapple with similar privacy issues regarding the collection, use, sharing, access to, and retention of personal data (although they may handle these common issues under separate regulatory regimes).

Federal and state privacy laws regulate some of this activity although significant gaps remain in the regulatory coverage of old and new surveillance technologies when they are used to monitor public spaces. Cities are beginning to fill this regulatory gap and have emerged as a new player in privacy policy making. Cities are active in two distinct arenas: public surveillance and local government data. 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

---

[1] *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW, 5th ed. 37-41 (2015). By contrast, in Europe and the rest of the world, privacy law is comprehensive rather than sectoral, with one statute regulating all data processing; *id.* at 1096-98.

[2] http://fortune.com/2016/07/17/big-data-nypd-situational-awareness/

[3] *See* Kelsey Finch and Omer Tene*, Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town,* 41 FORDHAM URB. L.J. 1581, 1606 (2015).

[4] *See, e.g.,* Steven E. Koonin and Michael J. Holland, *The Value of Big Data for Urban Science*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD (2014); Robert M. Goerge, *Data for the Public Good: Challenges and Barriers in the Context of Cities, in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD, *id.;* STEPHEN GOLDSMITH AND SUSAN CRAWFORD, THE RESPONSIVE CITY: ENGAGING COMMUNITIES THROUGH DATA-SMART GOVERNANCE (2014).

tempting terror targets on earth."[5] Before doing so, it adopted voluntary privacy guidelines covering its use of this new surveillance system. Over the next decade, Seattle, New York and about a dozen other cities (and counties) have enacted or introduced local ordinances regulating the funding, acquisition, and use of surveillance technologies.[6] These ordinances generally require city departments and police forces to prepare and publish protocols addressing their intended use and deployment of surveillance technology including data collection, use, access, retention, and sharing with other governmental entities and to obtain city council approval prior to acquisition and use.[7]

Additionally, Seattle, New York, Chicago and many other cities have developed privacy principles addressing smart city/IoT data practices or, even more broadly, covering all data collection and use by city agencies. Seattle has emerged as a leader in local privacy policy making, having recently announced city-wide privacy principles covering any personal data it collects or processes and requiring partners and vendors to follow the same guidelines. The city was also the first in the nation to appoint a chief privacy officer, whose duties also include managing open data projects that make city data available to the public for a range of beneficial purposes subject to privacy protections.[8]

What accounts for this new privacy activism at the local level? Three broader societal trends have prompted cities to champion local privacy: first, the war on terror; second, the smart cities phenomenon; and, third, the post-Ferguson scrutiny of policing tactics and policies.

Although the federal government plays the leading role in U.S. counter-terrorism efforts, policy makers quickly realized their mutual dependence on state and especially local officers to serve as the "eyes and ears" of the intelligence community.[9] Federal counter-terrorism officials interact with local law enforcement mainly in two ways. 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 counterterrorism and law enforcement activity, subject to various federal conditions and requirements.[10] Additionally, many cities participate in Joint Terrorism Task Forces (JTTFs) designed to coordinate counter-terrorism activity across multiple levels of government,[11] as well as

---

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

[6] *See* ACLU, Community Control Over Police Surveillance, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (identifying almost 20 cities that have adopted or considered local surveillance laws).

[7] For a discussion of local surveillance ordinances in Seattle and New York, *see infra* Parts III.A.1 and III.B.1, respectively.

[8] For a discussion of city privacy principles in Seattle and New York, *see* Parts III.A.2 and III.B.2, respectively.

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

[10] Cite. 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, Gregory T. Nojeim, & Ronald D. Lee, *Systematic Access to Private-Sector Data in* BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA (Fred H. Cate & James. X. Dempsey eds., 2017) (describing a range of NSA surveillance programs); Ira Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 UNIV. CHICAGO L. REV. 261 (2008) (discussing the TIA program).

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

"fusion centers" designed to generate and share local intelligence using sophisticated monitoring and information gathering techniques.[12]

Not surprisingly, New York City has been a leader in deploying a broad range of surveillance technologies and taking additional steps to secure the city in the wake of the 9/11 attacks. When the NYPD decided to expand its existing surveillance capabilities, it co-designed with Microsoft a citywide network of sensors, databases, devices, software, and related infrastructure known as the "Domain Awareness System" (DAS).[13] Initially, the DAS included video security cameras, automatic license plate readers (ALPRs), and radiation sensors. Later on, the NYPD added geocoded criminal records and, with help from Microsoft, integrated the network surveillance capabilities of DAS with analytic methods designed to inform both tactical decisions (e.g., sending automatic alerts when gunshots were detected or forecasting future locations of a watch-listed vehicle) and strategic decisions (such as using predictive policing algorithms to help allocate police resources.[14] Recognizing the 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.[15] 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.[16] This is truly police surveillance of public spaces at the scale of big data[17] As noted, the NYPD understood from the outset that the sheer size and scope of the DAS would raise serious privacy concerns and adopted privacy guidelines accordingly.

There are many definitions of "smart cities" but for present discussion the term may be understood as denoting an instrumented, interconnected, and intelligent city.[18] Working from a similar definition of smart cities as growing networks of connected technologies generating actionable data about the city and its residents, Kelly Finch and Omer Tene 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."[19] 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

---

[12] *See* Danielle Keats Citron & Frank A. Pasquale, *Network Accountability for the Domestic Intelligence Apparatus* 62 HASTINGS L. J. 1441 (2011).

[13] https://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito.

[14] E. S. Levine, Jessica Tisch, Anthony Tasso & Michael Joy, *The New York City Police Department's Domain Awareness System,* 47 INTERFACES 75-76 (2017); *see also* https://www.theguardian.com/world/2012/aug/08/nypd-microsoft-surveillance-system.

[15] *Id.* at 73. *See also* https://www.wsj.com/articles/future-of-nypd-keeping-tab-let-s-on-crime-data-1393985801

[16] Brennan Ctr. For Justice, Faiza Patel & Michael Price, *Keeping Eyes on NYPD Surveillance* (March 1, 2017), https://www.brennancenter.org/blog/ny-city-council-needs-increase-scrutiny-nypd%E2%80%99s-surveillance-arsenal.

[17] Levine, *supra* note , at __ (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").

[18] Colin Harrison, et al., *Foundations for Smarter Cities,* 54 IBM J. RES. & DEV. 1 (2010). According to this study, instrumentation enables 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." *Id.* Interconnection means the integration of those data into an enterprise computing platform and the communication of such information among the various city services. Intelligence refers to the inclusion of complex analytics, modeling, optimization, and visualization in the operational business processes to make better operational decisions.

[19] Finch & Tene, *supra* note , at 1606.

balance the gains from civic innovation against the risks of re-identification and associated privacy harms;[20] 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.[21] 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.

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 including stop and frisk, racial profiling, excessive use of force, police perjury, police militarization, and—most tragically—multiple incidents of police shootings of unarmed civilians.[22] Sadly, the common factor in these practices is their malignant effect on racial minorities, immigrants, the poor, and the most vulnerable in our communities.

This Article examine the origins, motivations, and outcomes of city-based privacy regulation in response to these three trends. It closely analyzes privacy policymaking in two contrasting cities, Seattle and New York. The case studies in Part III focus mainly on the use of surveillance technologies by local police forces and secondarily on the collection, use, and disclosure of personal data by other government departments in the course of delivering municipal services (both the everyday kind and the smart city kind). This attention to city-level privacy regulation is almost unique in recent privacy scholarship.[23]

So, too, is this Article's examination of local privacy regulation through the prism of federalism and localism. As sub-federal units of government, cities have the least power within the federal-state-city hierarchy. Their local privacy regulations are subject to both federal and state preemption. And while federal and state bureaucrats have enormous resources at their disposal, city regulators seemingly lack the expertise and personnel to enter the already crowded field of privacy regulation and make any significant contributions. This Article rejects any such dismissive view of what cities can contribute. Rather, it offers three arguments in favor of privacy localism: first, privacy issues are highly salient to cities for the reasons given above; second, due to the paucity of federal and state laws addressing *public* surveillance or the data governance practices of *local* government, cities have sufficient flexibility to exercise their police powers under state law while largely avoiding both federal and state preemption;[24] and, third, cities are ideally suited to regulate police use of surveillance technology and local data practices because of their willingness to try out innovative privacy protections.[25]

---

[20] *Id.* at .

[21] *Id.* at .

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

[23] Two complementary studies of local privacy regulation that also rely on case studies of major cities are Catherine Crump, *Surveillance Policy Making By Procurement,* 90 WASH. L. REV. 1595 (2016) (Seattle, Oakland, San Diego); Jan Whittington, et al*., Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government*, __ BERK. TECH. L. J. __ (2015) (Seattle).

[24] For a discussion of federal and state preemption of local privacy laws, *see infra* Parts I.B and II.B, respectively. 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. *Id.*

[25] *See infra* Part IV.A, B.4 & C.

Local surveillance systems share certain common characteristics with better known federal surveillance programs. To begin with, all the information collected by these systems is "born digital" or converted from analogue into digital format, thereby enabling efficient, computer-based data processing, storage and transmission.[26] In addition, this digitization facilitates what Katherine Strandburg refers to as "datafication—long-term storage in a format that is searchable, computationally manipulable, and [that] may be aggregated with [other] information."[27] Finally, both federal and local programs and systems exhibit an insatiable appetite for data, the raw material from which counter-terrorism and law enforcement agencies alike extract meaning or detect suspicious linkages or patterns that may help them to identify and preempt terrorist attacks or predict crime.[28] As a result, both the intelligence community and local police departments now collect data indiscriminately and in bulk, regardless of whether the individuals whose data is collected and stored are suspected of any illegal activity. For example, the TIA program sought to possess all data without qualification as long as it fell with the so-called "transaction space" of terrorist tracking.[29] The NSA's telephony metadata program required telecommunication carriers to disclose call records on all calls by hundreds of millions of Americans.[30] And the NYPD's DAS records video images of every passerby and license plate seen on NYC streets and roads within camera range on an ongoing basis.

These characteristics—digitization, datafication, and bulk collection—add up to what Christopher Slobogin calls "panvasive" surveillance, a term he coined to capture the idea that that mass surveillance techniques are "pervasive, invasive, and affect large numbers of people, most of whom police know are innocent of wrongdoing."[31] And for reasons that Slobogin and other scholars have readily identified, "the Fourth Amendment is not implicated by most types of panvasive surveillance."[32]

This Article argues that local surveillance ordinances go a long way to closing this gap in Fourth Amendment law along with a comparable gap in electronic surveillance law.[33] These ordinances directly address public surveillance. They require transparency and accountability for all surveillance

---

[26] For example, the DAS digitizes all of the video and audio feeds it receives and integrates them with license plate numbers, vehicle and location data from electronic toll collection systems, and real-time audio from gunfire-detection systems. *Id.*

[27] *See* Katherine J. Strandburg, *Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context, in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD 11 (2014) (noting that "Datafication opens up the potential for uses that may have been unanticipated or even technologically infeasible at the time of collection and are qualitatively different form the original purpose of the surveillance by making monitoring more efficient and effective" and thereby "heightens privacy concerns and changes the trade-offs involved in monitoring and its regulation").

[28] *See* Rubinstein, Lee & Schwartz, *supra* note (discussing terrorist profiling); Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. UNIV. L. REV. 1113 (2017) (discussing predictive analytics as a policing strategy).

[29] Pell 175 (noting that this transaction space "included …

[30] My article n. 23

[31] Christopher Slobogin, *Policing as Administration,* 165 UNIV. PENN. L. REV. 1, 3. n. 5 (2016). Other scholars have recognized the same phenomenon but call it by different names. *See, e.g.,* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 Stan. L. Rev. 1039, 1051-53 (2016) (distinguishing "transactional" surveillance (where police justify investigations based on probable cause determination involving a particular suspect, time and place) from "programmatic" surveillance (which is typically ongoing, cumulative and fluid); Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 286 (2016)(distinguishing "investigative" ("suspicion-based") searches from "programmatic" ("suspicion-less") searches and arguing that each requires different protections against arbitrary police discretion).

[32] Christopher Slobogin, *Panvasive Surveillance, Political Process Theory and the Nondelegation Doctrine,* 102 Georgetown L. J. 1722, 1723 (2014).

[33] For a discussion of the public surveillance gap, *see infra* Part IV.B.

technologies in use on city streets, even if they monitor public spaces. A few states have begun to address specific surveillance technologies like automatic license plate readers and drones but no state (except California)[34] has sought to address public surveillance as broadly as Seattle, New York, and a dozen or so other cities have in their local ordinances. Finally, this Article argues that city privacy activity intersects with the "administrative turn" in privacy scholarship, that is, the new emphasis on administrative law to overcome and supplement federal legislative failures and Fourth Amendment doctrinal weaknesses.

The Article proceeds as follows: Part I explores privacy regulation in the context of localism and federalism and concludes that federal preemption of local privacy law is not an obstacle to city efforts at regulating privacy in the two chosen areas. Part II takes up the more problematic issues of whether cities have sufficient power to regulate in these areas under state law and whether state privacy laws (generally and in Washington and New York in particular) preempt local privacy laws. Part III is a case study of local privacy regulation in Seattle and New York. Part IV lays out the case for privacy localism by identifying the anticipated benefits and likely problems with local privacy regulation in Seattle and New York, showing how these local regulations help close the public surveillance gap, and relating them to the administrative turn in police studies. The Article then concludes.

I. LOCALISM AND FEDERALISM

This Part introduces the idea of localism as a prism for viewing the two case studies of local privacy regulation in Part III. In normative terms, localism refers to a preference for local control of government functions,[35] while the law of localism describes the relations between states and their local governments.[36] Thus, *privacy* localism refers to local control over the collection, use, and disclosure of the personal data of city residents. More specifically, 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. Privacy *localism*, on the other hand, emphasizes the benefits of local autonomy and decentralization.

Localism is enjoying a revival thanks in part to progressive cities taking the lead on a host of controversial policy issues usually handled at the federal or state level. These include local regulation of public health (including restrictions on the sale or use of tobacco, sugary dinks, and trans-fat foods); campaign finance; living wages; climate change; marriage equality; and immigration.[37] A

---

[34] *See infra* text accompanying note.

[35] The European term for localism is "subsidiarity"; *see* STEPHEN BREYER, MAKING OUR DEMOCRACY WORK: A JUDGE'S VIEW 123 (2010) (stating that "Subsidiarity insists that government power to deal with a particular kind of problem should rest in the hands of the smallest unit of government capable of dealing successfully with that kind of problem").

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

[37] *See, e.g.,* Richard Briffault, *Local Leadership and National Issues* __ (Papers from the Eleventh Annual Liman Colloquium at Yale Law School, Why the Local Matters: Federalism, Localism, and Public Interest Advocacy, 2008); Richard C. Schragger, *The Progressive City, id.* For a discussion of state-local conflicts, *see* Richard Briffault, Nestor Davidson, Paul A. Diller, Olatunde Johnson, & Richard C. Schragger, The Troubling Turn in State Preemption: The Assault on Progressive Cities and How Cities Can Respond, Amer. Const. Soc. (ACS) For Law & Policy (September 2017) [hereinafter "ACS Issue Briefing"].

natural byproduct of these local initiatives is a growing scholarly interest in localism.[38] Olivier Sylvain has written on broadband localism[39] and Joseph Blocher on firearm localism.[40] The term "privacy localism" is meant to evoke these trends and suggest that cities can play an equally progressive role on surveillance and data privacy issues.

As David Barron notes, the values associated with localism and decentralization include "promoting responsive and participatory government by bringing the government closer to the people; fostering diversity and experimentation by increasing the fora for expressing policy choices and creating a competition for a mobile citizenry; and providing a check against tyranny by diffusing power that would otherwise be concentrated."[41] One of the questions the case studies seek to answer is how well local privacy regulation achieves these benefits.

According to Barron, local autonomy is also a more complex concept than we often acknowledge due to the absence of a clear baseline definition of local autonomy. And this baseline problem arises in part because "the local sphere is part and parcel of a larger coordinated system of local jurisdictions that is structured by less visible background central-law rules."[42] This Part explores the intersection of privacy localism and these "central-law rules" in the context of federalism and federal preemption of city privacy regulation. Part II addresses city empowerment under state law and state preemption of city privacy regulation.

A. Privacy and the Principles of Federalism

"Dual federalism" is the view the federal and state governments are separate sovereigns, with their own sphere of authority and activity, and that the Supreme Court must protect the zone of activities reserved to the states.[43] Although the U.S. system of dual sovereignty is reflected in many provisions of the Constitution,[44] since the 1990s the Court has developed this doctrine mainly in cases relying on the Tenth Amendment. In *Reno v. Condon,* however, the Court rejected a Tenth Amendment challenge to a federal privacy law.[45] Apart from this case, the dual-sovereign paradigm has little bearing on regulating the collection, use and disclosure of personal data. There is scant evidence that legislatures, courts, or scholars think of privacy regulation as a power reserved to the states for their exclusive control, or that federal law making in this area necessarily intrudes upon state sovereignty.[46]

---

[38] *Id. See also* Nestor M. Davidson, *Cooperative Localism: Federal-Local Collaboration in an Era of State Sovereignty*, 93 VA. L. REV. 959, 967 (2007); Nestor M. Davidson, *Localist Administrative Law*, 126 YALE L. J. 564 (2017).

[39] Olivier Sylvain, *Broadband Localism,* 73 OHIO STATE L. J. __ ().

[40] Joseph Blocher, *Firearm Localism*, 123 YALE L. J. __ (2013).

[41] Barron, *supra* note , at 378.

[42] Barron, *id.* at Barron identifies three dimensions to the baseline problem: the relation of cities to other cities and states (horizontal federalism); the relation of the city to broader market forces (competitive decentralization); and how the central government structures these relations (vertical federalism). This Article focuses almost exclusively on issues of vertical federalism.

[43] ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES, 5th ed. 256 (2015).

[44] Printz v. United States 521 U.S. 898, 919 (1997).

[45] 528 U.S. 141 (2000).

[46] The obvious exception are the privacy torts. Tort law is primarily state law, not federal law. While nearly all fifty states recognize the privacy torts, there are relatively few federal laws that cover the same set of rights. However, the privacy torts are not relevant to local surveillance laws or government data practices.

In a series of cases in the 1990s, the Supreme Court began to articulate a principle of federalism contained in the Tenth Amendment and known as the anti-commandeering doctrine. In *New York v. United States*, the Court invalidated 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."[47] In *Printz* v. *United States,* the Court struck down a federal law requiring state and local law enforcement personnel to conduct background checks before issuing permits for firearms, reaffirming that "[t]he Federal Government may neither issue directives requiring the States to address particular problems, nor command the States' officers, or those of their political subdivisions, to administer or enforce a federal regulatory program."[48]

The intersection of the anti-commandeering doctrine and privacy legislation occurred in 2000 when the state of South Carolina mounted a Tenth Amendment challenge to the Driver's Privacy Protection Act of 1994 (DPPA).[49] The DPPA regulates the sale and distribution by state Departments of Motor Vehicles (DMVs) of personal information in motor vehicle records. Congress enacted the DPPA in response to a notorious incident that received a great deal of media attention—the murder of an actress by a stalker who obtained her address indirectly from a state DMV.[50] The DPPA prohibits DMVs (and their officers and employees) from disclosing driver's personal information in motor vehicle records without the subject's consent.[51] Additionally, the law requires certain disclosures of personal information for public safety purposes and restricts other disclosures by enumerating permissible uses.[52] It also restricts the resale and re-disclosure of such information by private persons who have obtained that information from a state DMV.[53]

In *Reno,* the Court overturned lower court decisions invalidating the DPPA as incompatible with the federalism principles announced in *New York* and *Printz*. The Court distinguished these cases on two 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."[54] Many commentators have criticized the first argument as resting on a dubious distinction between affirmative and negative duties.[55] After all, most duties can be characterized either way. The second argument is a little more compelling although as Chemerinsky skeptically notes, 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."[56]

Reno is also important to the present discussion because it treats the DPPA as a valid exercise of Congress' authority to regulate interstate commerce under the Commerce Clause. As the Court observes, States sell motor vehicle information which is then used by "insurers, manufacturers, direct marketers, and others engaged in interstate commerce to contact drivers with customized

[47] 505 U.S. 144, 188 (1992).
[48] 521 U.S. 898, 935 (1997).
[49] Pub. L. No. 103-322, 18 U.S.C. §§ 2721-2725.
[50] S&S, 664-65.
[51] 18 U.S.C. § 2724(a).
[52] 18 U.S.C. § 2721(b) (identifying 14 permissible uses for public and private entities and individuals).
[53] 18 U.S.C. § 2721(c).
[54] Reno v. Condon, 528 U.S. at 151.
[55] *See, e.g.,* Erwin Chemerinsky, *Right Result, Wrong Reasons: Reno v. Condon*, 25 Oklahoma City Univ. L. Rev. 823, 827 (2000).
[56] *Id.* at 828. Chemerinsky agrees with the holding in *Reno* but argues that the Court should have overruled the anti-commandeering principle or recognized a compelling interest exception. *Id.*

solicitations" as well as by "various public and private entities for matters related to interstate motoring."[57] This holding does not distinguish *New York* or *Printz* but it is entirely consistent with the fact that Congress has enacted numerous sectoral privacy laws covering a wide range of commercial activities.[58]

Apart from *Reno* and the DPPA, principles of federalism have very little bearing on privacy legislation at the federal, state or local level. *Reno* turns on the fact that "[t]he DPPA regulates the States as the owners of data bases."[59] But no other federal privacy statute so directly regulates state programs. Nor have there been any successful challenges of federal privacy laws on the grounds that they violate the anti-commandeering doctrine.[60] One reason for this is that both *New York* 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."[61] But there are few if any "federal regulatory programs" whose primary concern is the disclosure or safeguarding of personal information.

To be clear, I do not mean to say that there are few federal *laws* addressing these issues. There are many such laws.[62] But they do not create any federal regulatory *programs* or require state officials to implement federal law, in the sense that the federal law requires that states administer and implement state welfare, environmental, health care, immigration, or law enforcement programs that are federally funded and that must satisfy federal standards. What scholars refer to as "cooperative federalism" rejects the idea of separate national and state spheres of powers and responsibilities in favor of a more collaborative understanding of federal-state relationships in a variety of regulatory contexts.[63] Under cooperative federalism, federal agencies rely on state assistance in carrying out federal regulatory programs. As Spencer Admur notes, this may entail "state entities disbursing federal funds, federal and state regulators developing joint regulatory standards, or collaborative enforcement."[64] A striking feature of cooperative federalism is that federal agencies use what Admur calls "inducement strategies" to secure such state and local assistance and aid,[65] which in turn raise numerous and complex constitutional issues regarding constraints on federal power under the commandeering prohibition and the newly minted coercion prohibition.[66] It is hard to think of a single case of a federal privacy program in which inducement strategies play a role.

This requires further clarification. There are certainly federal programs that both rely on federal-state cooperation and raise privacy concerns. For example, there are many domestic intelligence programs that rely very heavily on local actors to conduct surveillance, profiling-based investigation, and data

---

[57] Reno v. Condon, 528 U.S. at 148.
[58] *See infra* text accompanying notes __.
[59] Reno v. Condon, 528 U.S. at 151.
[60] String cite
[61] *Id.* at 149.
[62] *See* Part II.C.
[63] Philip Weiser,
[64] Spencer E. Admur, *The Right of Refusal: Immigration Enforcement and the New Cooperative Federalism,* 35 YALE L. & POL. REV. 87 (2016).
[65] *Id.* at (describing various forms of inducement strategies including solicitation, offers, trades, threats, prohibitions and mandates).
[66] *See National Federation of Independent Business v. Sebelius*, 132 S. Ct. 2566 (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).

collection and sharing. As Matthew Waxman observes, some of these programs condition grants and funding on federal guidelines "such as information-sharing protocols to promote uniformity as well as privacy standards."[67] 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 2ith a full-fledged "privacy program."[68] This may sound like hair-splitting but the point is that domestic intelligence programs are not about privacy. They are about national security and they consist in federal efforts to promote local national security activities by providing "resources and training to state and local police forces to help them establish intelligence units, build databases, and develop standards for intelligence gathering"[69] or 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."[70] In other words, these programs do not consist in federal efforts to promote privacy by providing training to chief privacy officers in how to establish and manage a privacy program or funding for research into effective privacy impact assessment techniques based on risk analysis or the design and development of privacy-preserving technologies. And while a few federal agencies do engage in such activities—notably, the Federal Trade Commission, the National Institute of Standards (NIST), and the National Science Foundation (NSF)—they do so by bringing enforcement actions, issuing guidelines, holding workshops (FTC), issuing standards and conducting research (NIST), and funding academics to engage in privacy engineering research (NSF). These agencies do not by create regulatory programs that state and local officials administer and implement with federal funding.[71]

Admittedly, the privacy aspects of national security programs have resulted in a small number of disputes between federal and state officials that resemble conflicts over federalism. For example, in 2005 Portland became one of the few cities to remove itself from a JTTF due to a disagreement over applicable surveillance standards, although it later decided to rejoin the task force under revised terms of engagement.[72] State governments have also resisted some federally supported data-sharing initiatives that they viewed as too invasive of privacy or too costly.[73] However, one of the few major controversies involving local or state objections to federal counter terrorism policies (not programs) centered on the USA PATRIOT Act (the Patriot Act).[74] Passed in haste by Congress shortly after the 9/11 terrorist attacks, the Patriot Act significantly increased the surveillance and investigative powers of U.S. law enforcement agencies by amending over fifteen existing statutes. These amendments expanded various surveillance authorities by providing broader access to Internet communications, lowering standards for foreign intelligence surveillance, and granting access to a wider range of business records without a showing of "probable cause" and subject to severe non-

---

[67] *See* Waxman, *supra* note .

[68]

[69] *See* Waxman, *supra* note , at 307.

[70] *Id.* at 308.

[71] That said, federal officials working on privacy and data security issues have a synergistic relationship with state Attorney Generals in part because state AGs have the power to enforce federal privacy regulations related to healthcare, children's online activities, and credit reporting agencies; *see* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General.* 92 NOTRE DAME L. REV. 747, ___ (2016).

[72] *Id.* at 316-17. *See also* Herman, *supra* note .

[73] *Id.* at 317, n. 155 (describing the demise of the Multi-State Anti-Terrorism Information Exchange (MATRIX) program after sixteen states dropped out due to "privacy and cost-efficiency concerns").

[74] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56.

disclosure and secrecy requirements.[75] The law quickly became a lightning rod for controversy over the balance between civil liberties and national security.[76]

This included a campaign to oppose the Patriot Act through local political action.[77] In all, eight states and 406 cities and counties (in 35 states) passed resolutions or ordinances critical of the Patriot Act.[78] Most of the resolutions opposed the Patriot Act for unduly burdening civil liberties guaranteed by the federal and state constitutions.[79] Almost all of them were "expressive" in the sense that their goal was to "reaffirm support for civil liberties and diversity, express particular concerns about the Patriot Act and other national, anti-terror polices, and urge state or local officials to uphold the rights of their citizens."[80] Others might be described as "regulatory" because they also included language prohibiting local officers from cooperating with federal officials in enforcing Patriot Act measures that violated federal constitutional rights and/or creating specific procedures for handling requests for cooperation. A few cities and states took a more aggressive stance. For example, several California cities adopted local ordinances requiring city council approval of requests for cooperation or assistance under the Patriot Act.[81] And several states adopted resolutions prohibiting state officials from cooperating with federal officials seeking information under the Patriot Act absent a showing of reasonable suspicion of criminal activity,[82] or probable cause,[83] even though these standards were much higher than the showing required by the Patriot Act.[84]

A few scholars have commented on these anti-Patriot Act resolutions in the Tenth Amendment context and they all agree that the resolutions represent a liberty-enhancing use of federalism. According to Ann Althouse, the resolutions show state and local officials relying on the anti-commandeering doctrine to push back against federal policies that threaten individual liberty. As she explains: "The limitation asserted in the resolution [to a higher standard than required by the Patriot Act] is … a robust interpretation of the meaning of constitutional rights" and a form of "true resistance to the federal program, not merely a bland statement of a truism about the superiority of the Constitution over other federal law."[85] Similarly, Ernest Young views the anti-commandeering doctrine as creating "the constitutional space for state and local governments to vindicate their own, possibly broader understanding of [First and Fourth Amendment] rights by refusing to participate in federal enforcements they consider suspect."[86] Young also emphasizes the expressive function of these resolutions as a form of political dissent on behalf of local residents.[87] Jessica Bulman-Pozen and Heather Gerken treat these resolutions as illustrative of what they call

---

[75]

[76]

[77] *See* https://rightsanddissent.org/news/happy-birthday-patriot-act-fifteen-years-done-best-crush-democracy/

[78] For a relatively complete listing, *see* http://www.discoverthenetworks.org/viewSubCategory.asp?id=849; REBECCA STEFOFF, THE PATRIOT ACT 102 (2011).

[79] *See* Ann Althouse, *The Vigor of the Anti-Comandeering Doctrine in Times of Terror*. 69 BROOK. L. REV. 1231, 1253-57 (2004); Ernest A. Young, *Welcome to the Dark Side: Liberals Rediscover Federalism in the Wake of the War on Terror*, 69 BROOK. L. REV. 1277, 1282 (2004).

[80] Young, *id.,* at 1282.

[81] *See, e.g.,* City of Arcata, Ordinance No. 1339, https://www.aclu.org/other/arcata-ca-ordinance (which also imposed a fine of $57 for violating the ordinance); San Francisco Ordinance No. 51-05 (2005), adding Section 2.20 to the San Francisco Administrative Code.

[82] California, Colorado, Idaho, Montana

[83] Alaska

[84] *See infra* note text accompanying note .

[85] Althouse, *supra* note , at 12__.

[86] Young, *supra* note , at 1288.

[87] *Id.* at 1295-1301.

"uncooperative federalism," which is their term for describing how states sometimes use the powers conferred on them by federal regulatory programs not to carry out federal policy but rather to resist or challenge it.[88] They take Young's idea a step further by interpreting the anti-Patriot Act resolutions as a form of "uncooperative behavior, akin to civil disobedience."[89]

These views have merit insofar as they emphasize the expressive force of these anti-Patriot Act resolutions and the political implications of the anti-commandeering doctrine for local governments intent on making their own decisions about the constitutionality of the Patriot Act. But any suggestion that these resolutions also carry regulatory force is overstated. Althouse and Young rightly concede that under the Supremacy Clause, local officials are barred from interfering with federal investigations that comply with federal law, even if they have well-founded objections.[90] But Bulman-Pozen and Gerken go too far in suggesting that states "use their policymaking authority to thwart the Patriot Act's provisions, something that is possible only because the federal government relies on the states for enforcement assistance."[91]

To the contrary, in using its authorities under the Patriot Act, the federal government does not need to rely on state officials. Take, for example, Section 215 of the Patriot Act. In its original form, Section 215 authorized the FBI to obtain books, records, papers, documents and other items for ongoing foreign intelligence, counterintelligence, or international terrorism investigation.[92] In 2006, Congress amended this section to provide that the FBI's application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation ... to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[93] Clearly, this provision does not require the FBI to show probable cause (or any reason) to believe that the target of a 215 order is a criminal suspect or foreign agent. Although anti-Patriot Act resolutions that impose a higher standard set the stage for a potential legal conflict with the FBI, such a conflict that has never materialized. The most likely reason for the absence of any test cases or even disputes involving these resolutions is that the FBI relies on Section 215 and related authorities to obtain records from *private* entities such as U.S. telecommunication companies holding telephone records on virtually every American.[94] Thus, the FBI has no need to seek the assistance of state or local officials because the records sought by the FBI are in the hands of businesses, not state or local governments.[95] In this scenario, then, the resolutions are toothless and the FBI has largely ignored them.[96] This contrasts sharply with the legal and political battles that have arisen between

---

[88] Jessica Bulman-Pozen & Heather K. Gerken, *Uncooperative Federalism*, 118. YALE L. J. 1256, 1278-80 (2009).
[89] *Id.* at 1278.
[90] *See* Althouse, *supra* note , at ; Young, *supra* note , at ; Herman, *supra* note , at 949.
[91] Bulman-Pozen and Gerken, *supra* note , at 1280.
[92] *See* Section 215 of the Patriot Act, adding a new § 501 to FISA. § 1861(b)(2).
[93] *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192; § 1861(b)(2)(A).
[94] The same holds true for the financial and travel records the FBI obtains from private entities using National Security Letters.
[95] Local governments do maintain library records, but the Attorney General John Ashcroft has stated that Section 215 had never been used to access library records; *see* SOLOVE & SCHWARTZ, *supra* note , at 441.
[96] See *News Hour with Jim Lehrer: Deadly Attack; Too Tough* (PBS television broadcast, Aug. 19, 2003) (statement of Viet Dinh, former assistant attorney general, Office of Legal Policy at the Justice Department, describing these resolutions as meaningless gestures with no legal effect).

federal immigration enforcement agencies and state and local governments over immigration sanctuary policies.[97]

*****

In sum, contemporary debates over federalism may not contribute very much to our understanding of privacy localism. The two most prominent conceptions of federalism—dual federalism and cooperative federalism—make assumptions about the interaction of government officials in the three levels of government and the existence of federal regulatory programs that do not match up very well with the current structure of privacy law. In particular, cooperative federalism seems much better suited to understanding top-down federal programs in which Congress provide the basic legal framework and delegates to a federal agency the power to administer the program in collaboration with state and local officials. As noted above, this model sheds light on the workings of domestic intelligence programs. But cooperative (and uncooperative) federalism seem far less useful in understanding bottom-up programs in which local governments use their own regulatory powers to fill in the gaps in federal policy.[98] Perhaps the best approach to federalism for understanding local privacy regulation is that of Cristina Rodriguez, who sees federalism as consisting not in a "fixed set of relationships" but instead treats its parameters as "subject to ongoing negotiations by the players in the system, according to the advantages each might accrue from a particular set of relations."[99] This more flexible approach enables Rodriguez to focus on how debates over controversial social welfare issues like immigration, marriage equality, drug policy, and health care reform—and perhaps local surveillance and smart city initiatives as well—play out in what she calls "the discretionary spaces of federalism."[100]

---

[97] Hundreds of cities have enacted ordinances that constrain local law enforcement from cooperating fully with federal authorities on immigration enforcement. Some of these ordinances instruct local officers to refrain from asking about the immigration status of victims, or witnesses, or even suspects unless arrested and charged with serious crimes. As Bill Ong Hing observes, the motivations behind these "don't ask" policies "is to encourage the entire community—including immigrant members—to trust and cooperate with the police to promote public safety for everyone." *See* Bill Ong Hing, *Immigration Sanctuary Policies: Constitutional & Representative of Good Policing & Good Public Policy*, 2 UC IRVINE L. REV. 247, 249 (2012). Federal immigration authorities and their supporters in Congress treat these sanctuary policies as a serious obstacle to immigration enforcement for the obvious reason that deporting undocumented immigrants requires locating them and federal agents lack the manpower to locate millions of undocumented immigrants in the interior regions of the U.S. Thus, without local cooperation, these agents would be stymied in carrying out their enforcement duties. Congress understood this problem when it enacted a federal anti-sanctuary law in 1996. *Id.* at __. New York City then challenged this law as applied to the city's sanctuary policy, raising anti-commandeering arguments, which the Second Circuit rejected. *See* City of New York v. United States, 179 F. 3d 29, 31-34 (2nd Cir. 1999). The details of the dispute needn't concern us here. Rather, the point is that Immigration and Customs Enforcement agents depend on local officers to help them enforce federal immigration law in a way that the FBI does not depend on local officers to investigate terrorism under the Patriot Act (notwithstanding federal-local cooperation under other homeland security programs). More recently, the Trump Administration threatened to revoke law enforcement funding from states, cities and localities that withhold information from federal authorities regarding the status of undocumented immigrants in their custody. *See* https://www.nytimes.com/2017/03/27/us/politics/sanctuary-cities-jeff-sessions.html; https://www.nytimes.com/2017/04/25/us/judge-blocks-trump-sanctuary-cities.html In short, sanctuary city policies have disrupted federal enforcement and led to Congressional activity, constitutional battles in federal court, and Presidential threats of funding cut-offs. Nothing of the kind has resulted from the anti-Patriot Act resolutions.

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

[99] Cristina M. Rodriguez, *Negotiating Conflict Through Federalism: Institutional and Popular Perspectives*, 118. YALE L. J. 2094, 2095 (2009).

[100] *Id.* at 2097.

B. Federal Preemption of Local Privacy Law

Congress has broad powers of preemption and hence the ability to block, limit, or invalidate local privacy laws. Federal preemption of state and local laws may be express (explicitly stated in a statute's language) or implied (contained in its structure and purpose).[101] There are two types of implied preemption: 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 undermines the accomplishment of Congressional objectives).[102]

There are over two dozen federal privacy statues[103] yet relatively few of them interfere with the city-level privacy regulation under consideration in this Article. This is less surprising than it might seem at first. Although the leading privacy law case book identifies twenty-four federal privacy statutes, relevant to this analysis,[104] most of them may be summarily eliminated from the analysis. Twelve of the twenty-four may be dispensed with immediately because they apply only to federal agencies;[105] or to exclusively federal activity like foreign intelligence gathering; [106] or only to banks [107] or telecommunication providers;[108] or govern all federal, state and local governmental agencies in a very narrow sphere,[109] or all employers in a narrow sphere,[110] or restricts permissible uses of a very limited type of record by public or private entities;[111] or criminalize certain conduct not at issue here.[112] Nine more of the remaining twelve statues fall away because they regulate commercial data held by private firms, either via sectoral laws[113] or consumer protection laws, and thus have little to do with the

---

[101] *See* Gade v. National Solid Waste Management Assn., 505 U.S. 88, 98 (1992). For an overview of federal preemption of state and local laws, *see generally* Chemerinsky, 412-13.

[102] *Id.*

[103] SOLOVE & SCHWARTZ, *supra* note , at 37-40 (identifying twenty-five federal privacy statutes).

[104] *Id.* at . Why twenty-four? The co-authors identify twenty-five statutes by this total includes several that amend or expand upon other laws and exclude (for consideration elsewhere in their case book) the Freedom of Information Act (FOIA) and the Federal Trade Commission (FTC) Act. When these adjustments are made, the new total of twenty-four results from subtracting the three laws that amend or expand existing laws, an adding FOIA and the FTC Act, which equals twenty-four. This total ignores federal privacy statutes enacted after the case book's publication date of 2015. The most important new legislation includes the USA Freedom Act (which chiefly amends the USA Patriot Act) and the Judicial Redress Act, which amends the PA. Thus, neither needs to be added to the analysis for the reasons that apply to the laws they amend.

[105] Freedom of Information Act, Pub. L. __, 5 U.S.C. § 552 (FOIA); Privacy Act of 1974, Pub. L. No. 93-579, 5 U.S.C. § 552a (PA); Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100503, 5 U.S.C. § 552a.

[106] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 15 U.S.C. §§ 1801-1811 (FISA) (*see also* the USA-PATRIOT Act of 2001, Pub. L. No. 107-56, which amends FISA and ECPA, and the FISA Amendment Act (FAA) of 2008). When Congress enacted FISA, the Patriot Act amendments to FISA (such as Section 215), and various other post 9/11 national security laws, it clearly demonstrated its intention to occupy the field of national security and foreign intelligence. *See* Pennsylvania v. Nelson, 350 U.S. 497, 502 (1956) (finding preemption appropriate where "the scheme of federal regulation is so pervasive as to make reasonable the inference that Congress left no room for the states to supplement it").

[107] Bank Secrecy Act of 1970, Pub. L. No. 91-508.

[108] Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414.

[109] Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 12 U.S.C. §§ 3401-s; and Privacy Protection Act of 1980, Pub. L. No. 96-440, 42 U.S.C. § 2000aa (PPA).

[110] Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193 (requiring the collection of personal data from all new employees)

[111] Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 18 U.S.C. §§ 2721-2725.

[112] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 18 U.S.C. § 1028 and Video Voyeurism Prevention Act of 2004, Pub. L. No. 108-495, 18 U.S.C.

[113] Fair Credit Reporting Act of 1970, Pub. L. No. 90-32, 15 U.S.C. §§ 1681 et seq. (FCRA) (*see also* the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (FACTA), which amends and updates the FCRA); Cable

privacy aspects of government activity.[114] This leaves only three federal privacy laws that are directly relevant to the present analysis: the Electronic Communications Privacy Act (ECPA), the federal electronic surveillance statute;[115] the Family Educational Rights and Privacy Act (FERPA, which limits the release of education records without prior authorization of the student and/or parent; and, the Health Insurance Portability and Accountability (HIPAA),[116] which governs the privacy of certain medical records, whether held by public or private entities.

Before analyzing the implications of these three laws for local privacy regulation, it is important to note that relatively few federal privacy laws include express preemption clauses[117] and those that do typically establish a "floor'—that is, a minimum standard that states may exceed.[118] All three of the remaining federal privacy laws under discussion—ECPA, FERPA, and HIPAA—lack preemption clauses.

1. Three Federal Privacy Statutes: ECPA, FERPA, and HIPAA

ECPA has three parts: an updated version of the Wiretap Act; the Stored Communication Act (SCA); and the Pen Register Act (PRA). 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.[119] Rather, the Wiretap Act is a classic example of a federal privacy "floor."[120] Nearly every state has its own surveillance laws closely patterned on the Wiretap Act,[121] and a dozen states have strengthened federal standards by enacting "all party" consent laws that are more restrictive than the "one party" rule under the Wiretap Act.[122] 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

---

Communications Policy Act of 1984, Pub. L. No. 98-549, 47 U.S.C. § 551; Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 18 U.S.C. §§ 2710-2711; Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 47 U.S.C. § 227; Children's Online Privacy Protection Act of 1998, Pub. L. No. 106-170, 15 U.S.C. §§ 6501-6506; Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102 15 U.S.C. §§ 6801-6809 (GLB Act); CAN-SPAM Act of 2003, Pub. L. No. 108-187.

[114] Federal Trade Commission Act, 15 U.S.C. § 45; Employee Polygraph Protection Act of 1988, Pub. L. No. 100-347, 29 U.S.C. §§ 2001-2009.

[115] ECPA, see *infra* text accompanying notes to .

[116] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (*see also* the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009, Pub. L. No. 111-5, which amends HIPAA).

[117] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS: 2017 187-93 (2017) (identifying CAN-SPAM, COPPA, FCRA, and the PPA as privacy statutes that contain a preemption clause).

[118] Paul M. Schwartz, *Preemption and Privacy,* 118 YALE. L. J. 902, 919-22 (2009).

[119] To the contrary, the legislative history of the Wiretap Act 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." *See* S. REP. NO. 1097, at 98 (1968), *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 (C.D. Cal. 2007), but the court's reasoning seems flawed. *See* PROSKAUER ON PRIVACY, § 6.2.6.

[120] Schwartz, *Preemption and Privacy, supra* note , 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* https://www.consumer-action.org/news/articles/fall_2004#Topic_02. It should also be noted that federal legislation setting a "floor" for privacy is the more common scenario and that FACTA is the *only* example of a federal privacy law that reverses existing state safeguards.

[121] PROSKAUER ON PRIVACY, § 6.2.6.

[122] Schwartz, *Preemption and Privacy, supra* note , at 920. Washington has an all-party consent statute, *see* WASH. REV. CODE ANN. § 9.73.070..

manner as the SCA.[123] Rather, the more common approach is to include similar protections in state privacy, consumer protection, or utilities regulation laws. Although there is one case holding that the SCA preempts a weaker state law, the circuits are split on this question of the preemptive effect of the SCA.[124] Finally, about half the states have laws regulating pen register and trap and trace devices and many of these laws are modeled on the PRA.[125] A review of these laws confirms that they closely resemble the PRA. Like the Wiretap Act, the PRA does not preempt stricter state laws.[126] In short, ECPA imposes few if any limits on states wishing to enact more protective legislation protecting electronic communications.

The FERPA protects the privacy of student records containing personal information directly related to a student and maintained by any educational agency or institution, whether public or private.[127] Although FERPA prohibits disclosure of student records without written consent,[128] it exempts disclosures to "school officials" with a "legitimate educational interest" and to appropriate persons in order to protect the health or safety of students or others, as well as to a number of other entities and officials.[129] These provisions would apply to local governments seeking access to educational records for educational and other legitimate purposes. Under standard preemption doctrines, FERPA would preempt conflicting state laws addressing the disclosure of educational information, although it would not preempt state legislature's authority to enact more privacy-protective limitations on access to education records by state or local officials. In fact, many state laws provide more stringent privacy protections for students than FERPA.[130]

The HIPAA regulates the privacy and security of certain kinds of medical information. It applies to "covered entities" (defined as health plans, healthcare clearinghouses, and healthcare providers) and therefore would regulate local governments insofar as they perform any of these functions. The statute is quite clear that it provides a baseline of protections but does not preempt more stringent state laws.[131] HIPAA also regulates the disclosure of "protected health information" (PHI) to law enforcement. It permits disclosure without consent or authorization if required by a court order, warrant, or subpoena if certain additional requirements are met.[132]

In short, all three statutes set a federal privacy "floor" that still allow states to pass more stringent requirements. As important for present purposes is the fact that local governments are not especially active in separately regulating electronic surveillance as defined in ECPA, education records as defined in FERPA, or PHI as defined by HIPAA. There is little evidence that cities are seeking to innovate in these arenas by enacting local laws. Rather, local government officials follow the law of each higher level of government within the federal-state-local hierarchy, thereby always meeting the federal floor or exceeding this floor if the applicable state standard is more protective. Thus, the

---

123 The exception is Pennsylvania; *see* 18 Pa. Stat. and Cons. Stat. Ann., § 5741 (West) (criminalizing unauthorized access to stored data).

124 *See* Prohibited Voluntary Disclosure under Stored Communications Act, 18 U.S.C.A. §§ 2701 et seq., 9 A.L.R. Fed. Art. 6 § 93-94 (3d ed.).

125 *See* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 882 n. 50 (2009).

126 The main prohibition in the PRA, 18 U.S.C. § 3122(a)(2), begins with the phrase "Unless prohibited by state law," which suggests that Congress anticipated states enacting stricter standards. The legislative history supports this position as well; *see* S. Rep. 99-541, 46, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3600.

127 20 U.S.C. § 1232g(a)(4)(A).

128 20 U.S.C. § 1232g(b).

129 20 U.S.C. § 1232g(b)(1).

130

131 *See* 45 C.F.R. § 160.203(b).

132 *See* 45 C.F.R. § 164.512(f).

three federal privacy law are controlling when city officials access, collect, use or disclose electronic communications, education records, or PHI. But in the absence of preemptive provisions and given the lack of activity at the local level, the three laws do not seem to constrain local efforts to regulate surveillance technology or data governance practices.

2. New Federal Privacy Laws?

Between 1970 and the mid-2000s, Congress enacted over two dozen mostly sector-specific federal privacy laws.[133] Since enacting the CAN-SPAM Act in 2003, however, Congress has exhibited little capacity to enact new privacy laws. This is not say that Congress has been passive. Laws have been introduced on numerous subjects—spyware, cybersecurity, online behavioral tracking, and cell phone tracking to name a few—and committees have held hearing. But none of these proposed laws have advanced very far. Congress has also taken up omnibus privacy legislation five times between 1999 and 2012 but without success.[134] In the meantime, the states have emerged as "especially important laboratories for innovation in information privacy law."[135]

There are reasons to be skeptical that the 115th Congress will enact, or even take up, major new sectoral privacy laws much less an omnibus law. To begin with, many observers view the Republican Congress under President Trump as having trouble accomplishing much at all.[136] On the privacy front, Congress succeeded in *withdrawing* the Obama Administration broadband privacy rules, leaving a (relatively) clear path for state legislatures and city governments to take up the slack.[137] Despite the unprecedented size and scope of the Equifax data breach, Congress seems unable to agree on a data security breach notification bill, even though several bills have been introduced and the patchwork of 48 existing state bills cry out for federal consolidation.[138] About the only likely candidate for successful privacy legislation in the near term is renewal and possible reform of Section 702 of the FAA, which is otherwise scheduled to expire on December 31, 2017.[139] Apart from possible action on Section 702, however, the prospects for new federal privacy legislation seem very dim indeed. In short, Congress has ample power and some interest in enacting new privacy laws but has not done so except in the national security arena, which has no overlap with local privacy regulation.

II. EMPOWERMENT AND IMMUNITY IN LOCAL GOVERNMENT

---

[133] *See supra* text accompanying notes __ to __. *See also* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions* 111 MICH. L. REV. 485, __ (2013) (describing the twenty-odd federal privacy statutes as representing "a relatively recent phenomenon" and as "sectoral rather than universal in character").

[134] [cite] A sixth bill was bandied about when President Obama floated a "Discussion Draft" of a comprehensive consumer privacy bill, but this proposal received no support from Members of either party in the House or the Senate.; *see* [cite]

[135] Schwartz, *Preemption and Privacy, supra* note , at 916. *See also* http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html.

[136] [cite] And the Republicans suffered a major defeat in failing to repeal Obamacare; *see* https://www.bostonglobe.com/news/politics/2017/07/28/republicans-congress-promised-action-numbers-they-have-not-delivered/rTn3iaqg9yPDAMwSJQwqXI/story.html.

[137] http://www.govtech.com/policy/10-States-Take-Internet-Privacy-Matters-Into-Their-Own-Hands.html

[138] *See* Schwartz, *supra* note at 917.

[139] https://www.lawfareblog.com/predicting-support-section-702-senate. A Section 702 reform bill would continue the trend of Congress enacting privacy reforms in the national security area; *see* note __. There has also been strong support in recent years for ECPA reform; *see* https://cdt.org/press/privacy-wins-in-a-landslide-as-house-passes-email-privacy-act/

Do cities have sufficient power to regulate privacy at the local level? At first glance, we might not think so. Of the three levels of government in the U.S. (federal, state, and city), cities are certainly the weakest in terms of political power, fiscal resources, and constitutional standing.[140] 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.[141] Nor is the exercise of state powers over cities subject to federal constitutional constraints or injunctive relief. Thus, states can and do block or control urban initiatives even when they have the strong backing of powerful mayors.[142]

Local government autonomy has two aspects, which Nestor Davidson refers to as "*empowerment*—"the ability to initiate policy—and *immunity*—the ability to resist encroachment from another governmental entity or from a private party."[143] Both aspects of local autonomy rest on what is known as "home rule."[144] 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 as "Dillon's Rule."[145] 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 40 states delegate this authority to local governments.[146] Home rule may be constitutional or statutory or a mixture of the two. Whatever the structure a state may adopt, home rule empowers local governments by delegating broad—but by no means unlimited—regulatory and spending authority. As noted in a recent "Issue Brief" co-authored by five leading local government scholars, the National League of Cities has usefully identified four categories of delegated power: structural (the power to design one's own government); personnel (the power to manage city employees); regulatory (the functional authority that includes the "police power" authority to regulate the health, safety, welfare and morals of the community); and fiscal (the authority to raise revenue, borrow money, and spend it).[147] These categories will prove helpful in assessing both the power and the immunity that state laws confer on local government.

A. City Power to Regulate Privacy

It is beyond doubt that cities have sufficient power to make policy decisions about (1) local policing including surveillance activities and (2) local services including any privacy safeguards applicable to the collection, use and disclosure of personal data by government agencies. Local policing is the paradigm case of regulatory power or what is more commonly referred to as "police power." Police power encompasses standing up and managing a local police force. Arguably, this is true in every

---

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

141 Barron, *supra* note , at 390.

142 *See* FRUG & BARRON, *supra* note , 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 charging).

143 Nestor M. Davidson, *Cooperative Localism: Federal-Local Collaboration in an Era of State Sovereignty,* 93 Va. L. Rev. 959, 967 (2007). *See also* RICHARD BRIFFAULT & LAURIE REYNOLDS, CASES AND MATERIALS ON STATE AND LOCAL GOVERNMENT LAW 346 (8th ed. 2016) (describing two aspects of home rule, which they refer to as "initiative" and "immunity").

144 FRUG & BARRON, *id.* at 31-43.

145 *See* Paul A. Diller, *Intrastate Preemption*, 87 BOSTON UNIV. L. REV. 1113, 1140 (2007); Hugh D. Spitzer, *'Home Rule' vs. 'Dillon's Rule' for Washington Cities*, SEATTLE UNIV. L. REV. 809, 813-24 (2015).

146

147 *See* Richard Briffault, Nestor Davidson, Paul A. Diller, Olatunde Johnson, & Richard C. Schragger, The Troubling Turn in State Preemption: The Assault on Progressive Cities and How Cities Can Respond, Amer. Const. Soc. (ACS) For Law & Policy 3-4 (September 2017)[hereinafter "ACS Issue Briefing"].

state, and every city, and every town in the United States. It is certainly true in both Seattle and New York City.

Washington is a "home rule" state in and the Washington State Constitution gives cities both "strong substantive police powers" and "significant flexibility in how cities structure their governments."[148] Art. XI, Sec. 11 explicitly allows cities to exercise all the "local police, sanitary and other" powers possessed by the state government, so long as local regulations do not conflict with general state laws. Spitzer describes this as a "strong home rule provision" and the exercise of police power as "the earliest and strongest of municipal powers."[149] Similarly, Art. XI, Sec. 10 allows cities with a population of over ten thousand people to frame their own charter and thereby control their form of government.[150] As a charter city, Seattle enjoys structural authority,[151] personnel authority,[152] regulatory authority,[153] and fiscal authority.[154] In short, it has more than enough delegated authority to oversee the surveillance activity of the local police department and to establish the conditions under which city department may process personal data.[155]

New York is also a home rule state but case law interpreting the relevant constitutional and statutory provisions makes the analysis more complex. The relevant portions of Art. IX, Sec. 1(a) of the New York State constitution empower local governments to "(1) adopt or amend local laws relating to its 'property, affairs or government' which are not inconsistent with the provisions of the constitution or of any general law; and (2) adopt or amend local laws, not inconsistent with the constitution or any general law, relating to ten enumerated subjects."[156] These ten subjects relate, inter alia, to "[t]he government, protection, order, conduct, safety, health and well-being of persons or property therein"[157] and controlling their form of government,[158] and transacting their business.[159] Like Seattle, NYC is a charter city and enjoys all four categories of delegated power. Thus, NYC also seems to enjoy sufficient power to oversee the surveillance activity of the NYPD and to establish city wide privacy policies.[160]

In 1989, NYC voters approved amendments to the city charter that made the city council "a more representative body and a co-equal partner in governing the city."[161] According to Caras and Fine, these charter amendments led to "separation of power" disputes between the Mayor and City Council, including disagreements (and law suits) over "how far the Council's legislative powers

---

148 *See* Spitzer, *supra* note , at 824-30 (discussing WASH. CONST., art. XI, § 11 and § 10, respectively).
149 *Id.* at 825.
150 *Id.* at 828.
151
152
153
154
155 *See infra* Part IV.A.
156 Elizabeth Fine & James Caras*, Twenty-Five Years of the Council-Mayor. Governance of New York City: A History of the Council's Powers, the Separation of. Powers, and Issues for Future Resolution*, 58 N.Y.L. SCH L. REV. 119 (2013-14). James D. Cole, *Constitutional Home Rule in New York: "The Ghost of Home Rule",* 59 ST. JOHN'S LAW REVIEW ((2012) 713 (same).
157 *Id.,* NY CONST., Art IX, § IX, 2(c)(10). *See also* N.Y. Mun. Home Rule Law § 10, which also authorizes local government to engage in these activities.
158 NY CONST., Art IX, § 2(c)(1) and (2)
159 *Id.,* NY CONST., Art IX, § IX, 2(c)(3).
160 *See infra* Part IV.B.
161 Fine & Caras, *supra* note , at 124.

extend or where the Mayor's executive authority begins and ends."[162] But none of the leading cases seem relevant to the powers under discussion in this section.[163]

Of course, the fact that Seattle and NYC enjoy—and exercise—their powers to regulate local police surveillance and local government collection, use, and disclosure of personal information does not imply that all U.S. cities do so as well. City power is cyclical in nature and right now, many U.S. cities are on the upswing, not only in terms of population growth but also in terms of economic, cultural, and political clout.[164] But not all cities are prospering as much as Seattle and NYC have in recent years.[165] There are also what Michelle Anderson calls "minimal" or failed cities, which are "beset by rising crime and police layoffs" but lack the ability to respond because of they are insolvent, bankrupt, or subject to state receivership.[166] And there also are what she calls "dissolving" cities, which are closing down their municipal governments and returning to dependence on counties often in response to economic crisis, tax pressure, and population loss.[167] These less fortunate cities must be acknowledged but the constraints on their policy making efforts are beyond the scope of this study.

B. *State Preemption of City Privacy Laws*

State preemption of local laws generally follows the same analytic model as federal preemption, with a few distinctions that are not relevant here.[168] There are over 700 hundred state privacy statues,[169] which makes for a crowded regulatory arena with a seemingly endless capacity to override local privacy law. Thus, state privacy law presents a much greater challenge to privacy localism than federal privacy law because of the sheer plenitude of state laws and the fact that many states regulate in areas that cities wish to address.

Unlike federal privacy law, it is therefore difficult if not impossible to parse every state privacy law, categorically eliminating most of them and focusing on just a few that matter. Accordingly, this Part makes a simplifying assumption by limiting the analysis of state-city preemption to the small number of state laws (i) in Washington and New York, that (ii) based on subject matter, overlap with local surveillance ordinances and local privacy principles, (iii) in Seattle and New York City, respectively.[170]

1. State Preemption of City Regulation of Public Surveillance Technologies

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

---

[162] *Id.* at 126.

[163] Describe cases

[164] *See, e.g.,* EDWARD GLAESER, TRIUMPH OF THE CITY: HOW OUR GREATEST INVENTION MAKES US RICHER, SMARTER, GREENER, HEALTHIER, AND HAPPIER (2012); BENJAMIN R. BARBER, IF MAYORS RULED THE WORLD: DYSFUNCTIONAL NATIONS, RISING CITIES (2013); BRUCE KATZ & JENNIFER BRADLEY, THE METROPOLITAN REVOLUTION: HOW CITIES AND METROS ARE FIXING OUR BROKEN POLITICS AND FRAGILE ECONOMY (2013).

[165] *See infra* text accompanying notes (Seattle) and notes (NYC).

[166] Michelle Wilde Anderson, *The New Minimal Cities*, 123 YALE L. J. 1118, 1120 (2014).

[167] Michelle Wilde Anderson*, Dissolving Cities*, 121 YALE. L. J. 1364 (2012).

[168] *See* Diller, *supra* note , at 1140 (noting differences in a few states including Georgia, Kansas and Oregon).

[169] *See* Robert Ellis Smith, *Compilation of State and Federal Privacy Laws* (2015)(how calculated).

[170] A fifty-state analysis of privacy laws is impractical given limitations of time, space, and interest, so a two-state analysis, with some mention of the trends in other states as appropriate, will have to suffice.

materially conflict.[171] Additionally, courts may limit preemptive effect where state law inadequately protects a right as recognized in a State constitution.[172]

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, then, the task is to identify and review laws in Washington and New York that regulate (1) specific surveillance technologies insofar as they overlap with Seattle and New York City's local surveillance ordinances (this would include Washington and New York state laws regulating video cameras and/or facial recognition, ALPRs, and drones); and (2) 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.

This task is large but manageable. Still, a few caveats are necessary. To begin with, the preemption analysis in the next section omits two surveillance technologies that the SPD or NYPD probably utilize: StingRay tracking devices[173] and electronic toll collection (ETC) systems. The analysis omits StingRays because their use does not raise localism issues. This is because they are regulated by a 2015 DOJ policy requiring federal law enforcement agencies (and state and local agencies working with them) to obtain a search warrant supported by probable cause before using the device.[174] Furthermore, both the Maryland Supreme Court[175] and the District of Columbia Court of Appeals[176] have held that the Fourth Amendment precludes the use of StingRays without a warrant and that federal and state surveillance laws apply to them. Thus, StingRays neither fall within the surveillance gap described in Part IV.B nor are they singled out for privacy regulation by local government. The analysis omits ETC systems (like Seattle's ORCA pass or NYC's MetroCard) because these fare cards are not issued by the city but rather by regional transportation authorities (Sound Transit and the Metropolitan Transit Authority, respectively). And the rules governing department acquisition of data from other government agencies is beyond the scope of this paper, indeed, the topic of a separate paper.[177]

In addition, the preemption analysis omits body cameras, mainly because local police use them as tools for monitoring police behavior and for reconstructing events for evidentiary purposes, rather than as surveillance devices. Nevertheless, body cameras are so prominent in recent discussions of police governance that they can't be omitted. They are discussed below in the context of state open records laws and in both the Seattle and New York case studies.

---

[171] State courts decide when a conflict arises under state law and this is often a question of legislative intent; *see*

[172] In theory, this would include the right of privacy, which ten states have recognized in express constitutional provisions protecting personal privacy; *see* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS: 2017 33 (2017) (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).

[173] StingRays are a type of cell site simulator, i.e., the device simulates a cell tower, thereby detecting cell phone signals in their vicinity. Thus, StingRays allow law enforcement to identify the location of a target with a known phone number.

[174] *See* U.S. Dep't of Justice, Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (2015), http://www.justice.gov/opa/file/767321/download.

[175] State of Maryland v. Andrews, 73 Md. App. 80, 533 A.2d 282 (1987). Washington State also requires a warrant for the use of StingRays. https://arstechnica.com/tech-policy/2015/05/cops-must-now-get-a-warrant-to-use-stingrays-in-washington-state/

[176] Jones v Unites States, (2017)

[177] This author plans to expand his work on privacy localism by conducting research on police department data sharing with other city agencies, with regional, state, or federal agencies, and with private sector firms.

a. Video Cameras/Facial Recognition Technology

Technology, Use and Privacy Concerns. – 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.[178] 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 have the capacity for video content analysis, which detects movement and even anomalous patterns of movement and facial recognition applications, which automatically match a face in a digital image or a video frame to a person in a facial database.[179]

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.[180] 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,[181] and the evidence supporting these claims is mixed at best,[182] which only serves to heighten privacy-related concerns.

One of these concern 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).[183] Additionally, video surveillance can have a chilling effect on political and religious expression. As Justice Sotomayor observed in a related context: "Awareness that the Government may be watching chills associational and expressive freedoms."[184]

---

[178] THE CONSTITUTION PROJECT, GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE: A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES (2007), http://constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf.

[179] *See generally* NY ACLU, *Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight* (2009) [*Who's Watching?*].

[180] http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html. http://fortune.com/2013/04/26/the-great-surveillance-boom/ NYC's Domain Awareness System has [x] video surveillance cameras linked together in a sophisticated network that also permits video content analysis; *see infra* text accompanying notes __.

[181] *Compare* U.S. General Accounting Office, "Report to the Chairman, Committee on Government Reform, House of Representatives: Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, D.C.," GAO-03-748, June 2001, at 29 ("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...") cited in *Who's Watching? supra* note , at 19, n. 1.

[182] An exhaustive study of the effect San Francisco's video surveillance program on crime deterrence found no evidence of an impact on violent crime, 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.

[183] https://www.aclu.org/other/whats-wrong-public-video-surveillance. *Who's Watching?, supra* note , at 7-10.

[184] United States v. Jones, 132 S.Ct. 945, 955-56 (2012) (analyzing GPS tracking)..

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,[185] this is starting to change and local police departments are renewing their interest in adopting FRT.[186] 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.[187] Moreover, facial databases are expanding: they 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."[188] 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 from "Immediate Biometric Identification (IBI)"[189] to "Remote Biometric Identification (RBI)."[190] RBI's intrusiveness presents a unique challenge to liberty because it allows for prolonged surveillance that will also occur more frequently and require significantly fewer resources than existing IBI systems.[191]

Regulation of Video Surveillance. – Congress and state legislatures have done little to address the privacy and free speech risks inherent in law enforcement use of video surveillance. As discussed below, surveillance in public spaces is not covered by ECPA.[192] Although the Fourth Amendment governs video surveillance, the reasonable expectation of privacy test has little application to silent video surveillance in public spaces.[193]

State laws mainly prohibit silent video surveillance when it occurs in "private places,"[194] or anywhere an individual enjoys a reasonable expectation privacy,[195] or when the camera is hidden unless the subject grants consent.[196] But these laws sound in tort, not criminal procedure, and thus have limited relevance to the present topic.

---

[185] [Tampa, London]

[186] http://www.nydailynews.com/opinion/smile-identified-face-recognition-article-1.3008512 (noting that the NYPD has been using FRT 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 FRT in the future).

[187] Donohue at 554

[188] Clare Garvie, et al., Geo. Law Center on Privacy & Tech, The Perpetual Line-Up, Unregulated Police Face Recognition in America 1 (2016), https://www.perpetuallineup.org/background ["The Perpetual Lineup"]. *See also* Government Accountability Office, "Facial Recognition Technology: FBI Should Better Ensure Privacy and Accuracy," May, 2016, http://www.gao.gov/assets/680/677098.pdf (stating that the FBI has access to more than 411 million facial images, including driver's license photos from 16 states as well as visa application and passport photos from the State Department).

[189] Laura Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 415-16 (2012) (describing IBI as "focused (1) on a single individual; (2) close-up; (3) in relation either to custodial detention or in the context of a specific physical area related to government activity; (4) in a manner often involving notice and often consent; and (5) in a one-time limited occurrence").

[190] *Id.* (describing RBI as giving 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").

[191] *Id.* at 529.

[192] *See infra* Part IV.B.3. Unlike ECPA, and its state counterparts, FISA explicitly regulates video surveillance. *See* 50 U.S.C. § 1804 (a).

[193] *See infra* Part IV.B.2.

[194] Alabama, Arkansas, Minnesota

[195] New York, Rhode Island, California

[196] Delaware, Georgia, Hawaii, Kansas, Michigan, New Hampshire

The Ninth Circuit requires heightened specificity for video surveillance warrants in non-public settings.[197] This requirement flows from finding that while the Wiretap Act does not govern silent video surveillance, courts should look to its provisions for "guidance."[198] Washington State's electronic communications privacy statute criminalizes eavesdropping and makes Washington a two-party consent state, but does not cover silent video recording.[199] Washington criminal procedure is non-specific regarding video surveillance warrants, which may fall within general warrant procedures requiring probable cause.[200] In addition, Washington criminalizes voyeurism by hidden camera, but this statute covers only surveillance "for the purpose of arousing or gratifying the sexual desire of any person."[201]

New York criminal procedure requires detailed warrants for individualized video surveillance.[202] 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.[203] But these procedures are limited to situations where warrantless surveillance would infringe on "reasonable expectations of privacy."[204] And the courts do not recognize reasonable expectations of privacy in public places, rendering New York procedural requirements inapplicable to video surveillance of streets and sidewalks.[205] To date, courts have not responded to calls to impose limits on surveillance of public spaces, although the "mosaic" capabilities of new technologies may well prove a catalyst for future change.[206]

Regulation of FRT. – There are no federal laws that specifically govern the use of facial recognition technology.[207] On the other hand, a few states have been active in regulating *commercial* uses of biometrics. For example, the 2008 Illinois Biometric Information Privacy Act (BIPA) was the first state law imposing privacy obligations on the collection and use of biometric information.[208] BIPA requires that before collecting and storing any biometric identifier (defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"), 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.[209] However,

---

[197] *See* United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992) (citing 18 U.S.C. § 2516 et seq.). *See generally* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 10 (2007) (identifying cases establishing Fourth Amendment protection from video surveillance of private places).

[198] *Id.*

[199] *See* Haymond v. State, 872 P.2d 61 (1994) (holding that Wash. Rev. Code Ann. 9.73.030 "does not apply to the operation of a video camera without an audible sound recording").

[200] Wash. Rev. Code Ann. § 10.79.035.

[201] Wash. Rev. Code Ann. § 9A.44.115.

[202] N.Y. Crim. P. Law §§ 700.10-70 (Consol. 2017); *see* 7-28 BENDER'S NEW YORK EVIDENCE § 28.30(2). Warrants are valid only as long as necessary to achieve the object of authorization, up to 30 days. § 700.10. Applications must demonstrate probable cause, show surveillance will yield information about the offense, aver alternatives would not be successful, and list specific locations to be surveilled. § 700.15-20. Warrants must be executed such that collection of unrelated information is minimized. § 700.30.

[203] *See* United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986).

[204] N.Y. Crim. P. Law § 700.05(9).

[205] *See, e.g.*, Rodriguez v. United States, 878 F. Supp. 20, 25 (S.D.N.Y. 1995) (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).

[206] *See* Rachel Levison-Waldman, *Hiding in Plain Sight: a Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 539-42 (2017).

[207] Donohue, *supra* note __, at 414.

[208] Illinois Biometric Privacy Act, 740 ILCS 14/1 et seq.

[209] 740 ICLS 14/15(b)

these restrictions only apply to a "private entity" and this term "does not include a State or local government agency."[210] Texas passed a similar law governing biometric identifiers collected for commercial purposes.[211] Other states have introduced laws modeled on BIPA but with mixed success.[212]

In June 2017, Washington become the third state (after Illinois and Texas) to enact a law regulating businesses that collect and use biometric identifiers for commercial purposes.[213] Moreover, the Washington law is doubly irrelevant for present purposes because it applies solely to biometric identifiers in commercial databases and excludes facial recognition data from the definition of "biometric identifiers."[214] Interestingly, the Washington legislature enacted a second bill regulating *state agency* collection, use, and retention of biometric identifiers, defined more broadly in this bill to include facial recognition data.[215] But this law is also doubly irrelevant for present purposes because it both limits the definition of "agency" to state (and not local) agencies[216] and exempts all "general authority Washington law enforcement agencies" (which covers local police departments in any case).[217]

However, Seattle has stepped up to this regulatory task by developing strict controls restricting the departments use of facial recognition software to comparisons of unidentified images and jail mug shots only.[218] The SPD policy also requires reasonable suspicion that the person in the image has committed a crime and prohibits use of the software to connect with live camera systems.[219] Moreover, SPD developed this policy with input from the ACLU of Washington, secured approval of the policy by an independent body (the Seattle City Council), and published the policy online, all of which makes the policy unique among U.S. cities that regulate FRT.[220]

As for New York, it is another state in which the legislature introduced a bill like BIPA but it never advanced out of committee.[221] The NYPD, which has been using FRT since 2011, has been much less transparent than Seattle regarding its policies and procedures. In response to a request for documents filed by a privacy research center, the department sent the researchers a single memo that indirectly confirmed the existence of a NYPD unit, staffed with analysts, and actively conducting facial recognition searches.[222] While acknowledging that it located records relating to the purchase of

---

[210] 740 ICLS 14/10

[211] Tex. Bus. & Com. Code Ann. § 503.001(b).

[212] *See* Justin Kay & Brendan McHugh, The Next Steps For Biometrics Legislation Across The U.S., May 25, 2017, https://www.law360.com/articles/928056/the-next-steps-for-biometrics-legislation-across-the-us (noting that as of May 25, 2017 similar bills were pending in Alaska, Connecticut, Massachusetts, and New Hampshire and that several additional states proposed bills that did not advance).

[213] H.B. 1493, 65th. Leg., Reg. Sess. (Wash. 2017).

[214] WASH. REV. CODE ANN. 19.375.010.

[215] H.B. 1717, 65th. Leg., Reg. Sess. (Wash. 2017); WASH. REV. CODE ANN. 40.26.020

[216] WASH. REV. CODE ANN. 40.26.020(7)(a).

[217] WASH. REV. CODE ANN. 40.26.020(8).

[218] *See* https://www.seattletimes.com/seattle-news/crime/seattle-police-wins-praise-for-safeguards-with-facial-recognition-software/.

[219] *Id.*

[220] *Id.* (discussing The Perpetual Lineup, *supra* note __). The SPD policy is published in the Seattle Police Department Manual, Section 12.045 (2017), https://www.seattle.gov/police-manual/title-12---department-information-systems/12045---booking-photo-comparison-software.

[221] *See* S.B. 4887, 238th Leg. Sess. (N.Y. 2015), https://www.nysenate.gov/legislation/bills/2015/S4887.

[222] https://theintercept.com/2017/05/02/nypd-refuses-to-disclose-information-about-its-face-recognition-program-so-privacy-researchers-are-suing/

facial recognition technology, the department denied access to those records in their entirety, prompting the center to file a lawsuit seeking disclosure of all relevant records.[223]

b. Automatic License Plate Readers

Technology, Use and Privacy Concerns. – 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.[224] Many police departments now use them mounted on patrol cars or fixed objects (e.g. light poles, bridges, overpasses).[225] There are also applications that allow police officers to scan license plates with their smartphones. 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 plates numbers of stolen cars, AMBER alerts, felony arrest warrants, registered sex offenders or people who are on supervised release.[226] 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.[227] It is also possible to aggregate ALPR data in centralized databases and trace a person's past movements by plotting all of the license plate reads associated with a vehicle's owner or passenger. Additionally, ALPRs allow geofencing, that is, identifying each vehicle seeking to enter a specific geographical area to 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, 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.[228] 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 *Jones* if the extended use of ALPRs is of sufficient duration and pervasiveness to constitute "long-term monitoring."[229] 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."[230]

Regulation. – According to the National Conference of State Legislatures, as of May 2017 at least fourteen states have statutes relating to the use of, or the retention of data collected by, ALPRs.[231] These statutes include some combination of provisions prohibiting the use of ALPRs except for

---

[223] *Id.*
[224] https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf
[225] DHS and DOJ are key sources of funding for the acquisition of license plate readers by local police departments. *Id.*
[226] *Id. See also* https://www.eff.org/sls/tech/automated-license-plate-readers
[227] *Id.*
[228] *See generally* Electronic Frontier Foundation, Automated License Plate Readers Threaten Our Privacy, https://www.eff.org/deeplinks/2013/05/alpr?from=sls.
[229] *See supra* text accompanying note __ to __; *see also* RAND Corporation, Keith Gierlack et al., *License Plate Readers for Law Enforcement: Opportunities and Obstacles*, https://www.ncjrs.gov/pdffiles1/nij/grants/247283.pdf
[230] http://www.criminaljustice.ny.gov/crimnet/ojsa/motor-vehicle/LPR-Operation-Suggested-Guidelines-2011.pdf
[231] http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx

enumerated lawful purposes; setting retention periods—which range from no more than three minutes in New Hampshire[232] to up to three years in Colorado;[233] requiring access controls and/or audits; restricting sales of ALPR data to third parties; and exempting ALPR data from public disclosure under state public record laws.[234] There are no federal laws or proposed bills pertaining to ALPRs.

Washington has not regulated ALPRs nor is there any pending legislation at the state level. However, the Seattle Police Department has independently developed a policy regarding ALPRs that, inter alia, requires operators to be certified and trained in the proper use of this technology, limits the use of ALPRs to routine patrol and criminal investigations, and restricts access to ALPR data.[235] On the other hand, Seattle's surveillance ordinance seems not to apply to ALPRs because it specifically excludes both cameras installed in or on a police vehicles and certain stationary cameras.[236]

In contrast, the New York State Senate is considering legislation (S23) prohibiting businesses and individuals from using ALPRs and imposing requirements on their use by law enforcement agencies.[237] Allowable uses under S23 would include identifying vehicles with parking and traffic violations, stolen vehicles, vehicles registered to a person associated with an outstanding arrest warrant for felony charges or to missing persons, electronic toll collection, and limiting access to secured areas, while prohibiting all other purposes. Additionally, the bill would limit the retention of captured plate data to no more than 180 days (except pursuant to a preservation or disclosure or a warrant) or for longer periods if part of an ongoing investigation, although the data must be destroyed at the end of the investigation. Finally, the bill would mandate 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" or after 14 days if their application is denied.[238] Both the Senate bill and (weaker) Assembly bill are currently in committee.

c. Drones

Technology, Use and Privacy Concerns. – "Unmanned aerial vehicles" (UAVs) or 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

---

[232] *See* N.H. Rev. Stat. Ann. §§ 261.75-b, 236.130 (providing that plate number shall be purged from the system within 3 minutes of their capture, unless the number resulted in an arrest, a citation or protective custody or identified a vehicle that was the subject of a missing or wanted person broadcast).

[233] *See* Colo. Rev. Stat. § 24-72-113 (requiring that video or still images obtained by passive surveillance by governmental entities, such as images from monitoring cameras, must be destroyed within three years after the recording of the images).

[234] *See generally supra* note .

[235] http://www.seattle.gov/police-manual/title-16---patrol-operations/16170---automatic-license-plate-readers

[236] *See infra* Part III.A.1.

[237] https://www.nysenate.gov/legislation/bills/2017/S23. The amended version of a companion bill in the New York State Assembly all but eliminates these requirements on law enforcement. *See* http://blog.tenthamendmentcenter.com/2016/06/fail-new-york-assembly-committee-guts-bill-to-limit-automatic-license-plate-readers/.

[238] *See infra* Part II.B. Additionally, in 2011 the New York State Division of Criminal Justice Services 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* http://www.criminaljustice.ny.gov/crimnet/ojsa/motor-vehicle/LPR-Operation-Suggested-Guidelines-2011.pdf.

extremely powerful cameras. Many cities in the U.S. have acquired the smaller UAVs for non-controversial purposes such as handling bomb threats, search and rescue missions, and crime-scene photography. This includes Seattle—in 2012 the city purchased for about $90,000 two Dragonflyer X6 model remote-controlled drones with grant money from DHS.[239] The drones in question weighed a little more than two pounds, reached a maximum height of 8,000 feet and a top speed of 20 miles per hour, and carried high-quality video equipment with low-light and thermal vison.[240] The mayor of Seattle eventually prohibited their use due to protests from privacy advocates and the general public.[241]

In short, UAVs can facilitate ubiquitous government surveillance by combining cost-effectiveness with high levels of technical capability.[242] Commentators suggest that U.S. law enforcement is expanding its use of drones for surveillance purposes,[243] while drone use by hobbyists and commercial firms raises separate but related privacy concerns ranging from voyeurism to corporate espionage. Indeed, if the past is any guide to the future, only our collective imagination restrains the level of intrusion that a silent, low-cost, low-profile, highly maneuverable device, outfitted with digital recorders and other sensors, might accomplish.[244]

Regulation. – The Federal Aviation Administration (FAA) regulates UAVs with respect to commercial use, safety and licensing, but not privacy.[245] Although the National Telecommunications and Information Administration (NTIA) worked with a multistakeholder group to develop drone privacy guidelines, these are voluntary best practices with little regulatory impact.[246] There are several drone privacy bills before Congress including the Drone Aircraft Privacy and Transparency Act (S. 631), a bill that would amend the FAA rulemaking process to obligate the Secretary of Transportation to "establish procedures to ensure that the integration of unmanned aircraft systems into the national airspace system is done in compliance with [] privacy principles." It also would prohibit government entities from using drones for law enforcement or intelligence purposes except pursuant to a warrant.[247] S. 631 has yet to receive serious consideration by Congress.[248]

On the other hand, almost two dozen states have passed drone-related privacy legislation requiring law enforcement agencies to obtain a search warrant before using drones for surveillance (subject to

---

[239] http://www.thestranger.com/seattle/heres-looking-at-you-kid/Content?oid=15148324

[240] https://en.wikipedia.org/wiki/Draganflyer_X6

[241] *See infra* Part III.A.

[242] *See* Marc Jonathan Blitz et al., *Regulating Drones Under the First and Fourth Amendments*, 57 WILLIAM & MARY L. REV. 49, 56-59 (2015).

[243] *See* American Civil Liberties Union, Domestic Drones, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones (stating "U.S. law enforcement is greatly expanding its use of surveillance drones").

[244] *See generally,* M. Ryan Calo, *The Drone as Privacy Catalyst,* 64 STANFORD L. REV. ONLINE 29 (2011) (observing that in *1984*, "George Orwell specifically describes small flying devices that roam neighborhoods and peer into windows").

[245] http://www.zdnet.com/article/faa-sued-for-lack-of-drone-privacy-rules/

[246] *See Multistakeholder Process: Unmanned Aircraft Systems*, Nat'l Telecomm. & Info. Admin (June 21, 2016), http://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.

[247] The Drone Aircraft Privacy and Transparency Act of 2013, S. 1639, 113th Cong. § 3 (2013). https://www.congress.gov/bill/115th-congress/senate-bill/631/text.

[248] S. 631 is the most recent version of a bill first developed by Senator Ed Markey in 2012, *see* http://thehill.com/policy/technology/273519-markey-introduces-drone-privacy-bill and it currently has no co-sponsors, *see* https://www.congress.gov/bill/115th-congress/senate-bill/631/cosponsors.

an exigent circumstance exception) or providing privacy protections against non-governmental actors that are specific to drones or that adopt existing state privacy laws to cover drones.[249]

In Washington, the legislature enacted a bill that would have placed limits on the use of drones for law enforcement purposes.[250] However, the governor vetoed the bill citing concerns about conflicting provisions on public disclosure and the definition of public information. He also announced creation of a task force to study surveillance technology and imposed a moratorium on purchasing unmanned aircraft for state agencies and asked local law enforcement agencies to do the same pending completion of the study.[251] In 2016, Washington'. 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, including data minimization, and respect civil rights.[252]

In New York, several bills have been introduced to regulate the use of drones by law enforcement. The strictest legislation, S.B. 1174, completely bans the use of drones by any person or entity "to conduct surveillance of or to monitor any individual" inside "locations where a person would have an expectation of privacy."[253] The bill allows some exceptions, including the use of drones under narrowly defined "exigent circumstances" or pursuant to a search warrant in investigations of serious felonies and makes any information obtained or derived in violation of the provisions of the bill inadmissible as evidence in any New York court or in an administrative hearing.[254] The bill also provides for civil remedies, allowing anyone to bring a civil suit against a law enforcement agency.[255] A.B. 3396 imposes similar restrictions on law enforcement use but also contains data minimization, data retention, disciplinary consequences for misuse, and reporting provisions for all state agencies.[256] A third bill, S.B. 2913, bans warrantless use of UAVs (with a few exceptions) and voids the use of such evidence in criminal proceedings.[257] All three bills were introduced in earlier sessions but did not advance.

2. State Preemption of City Regulation of Data Governance Practices

---

[249] http://www.ncsl.org/Portals/1/Documents/transportation/TAKING_OFF-STATE_%20UNMANNED_%20AIRCRAFT_SYSTEMS_%20POLICIES_%20%28004%29.pdf. This level of state activity is not surprising given the FAA's readiness to concede that "Laws traditionally related to state and local police power – including … privacy, trespass, and law enforcement operations – generally are not subject to federal regulation." *See* https://www.faa.gov/uas/resources/uas_regulations_policy/media/uas_fact_sheet_final.pdf (noting that examples of such laws include "requirements for police to obtain a warrant prior to using a UAS for surveillance" and "specifying that UAS may not be used for voyeurism"). *See also* Margot Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry,* 4 CAL. L. REV. CIR 57, 67 (2014) (arguing that "Congress should defer to states on privacy regulations governing civilian drone use for video and audio surveillance").

[250] *See* H.B. 2789, 63rd Leg. Reg. Sess. (Wash. 2014).

[251] http://www.govtech.com/state/Washington-Gov-Jay-Inslee-Vetoes-Drone-Bill.html 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).

[252] Wash. Office of Privacy and Data Protection, Wash. State Policy Guidelines for Unmanned Aircraft Systems (2016), http://www.wsdot.wa.gov/NR/rdonlyres/AC738BE5-FDCE-4FD9-A173-6C913FDABE24/0/DronePolicyGuidelines.pdf.

[253] S.B. 1174, 2017 N.Y. Sen., Reg. Sess. (NY 2017), http://assembly.state.ny.us/leg/?default_fld=&bn=SB1174&term=2017&Summary=Y&Actions=Y&Text=Y

[254] *Id.*

[255]

[256] A.B. 3396, 2017 N.Y. Assemb., Reg. Sess. (NY 2017), https://www.nysenate.gov/legislation/bills/2017/A3396.

[257] S.B. 2913, 2017 N.Y. Sen., Reg. Sess. (NY 2017) https://www.nysenate.gov/legislation/bills/2017/S2913.

The federal Privacy Act regulates the way federal agencies collect, maintain, use or disseminate the personal information of individuals. Although the Act generally does not apply to state and local agencies, [258] it is worth examining for several reasons. First—despite several significant shortcomings—the Privacy Act embodies the Fair Information Practice Principles (FIPPs) by limiting disclosure, data collection and retention, requiring various notices, granting a right of access and correction, imposing data security requirements, and providing enforcement rights.[259] Second, the Privacy Act and the related E-Government Act require federal agencies to prepare both System of Records Notices (SORNs) and Privacy Impact Assessments (PIAs). 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. [260] Thus, SORNs serve two salutary purposes: first, they provide (i) notice to the public about their rights under the Privacy Act and (ii) useful information for privacy advocates, alerting them to new government databases and thereby enabling them to analyze whether these databases comply with federal law; [261] and, second, they force agencies to continually examine and rationalize their own policies and practices (as a prelude to issuing new SORNs).

In keeping with latter purpose of SORNs, agencies also must 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.[262] More precisely, the purpose of a PIA is to demonstrate that program managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or program. Further, PIAs must be approved by a "reviewing official" who is someone other than the official procuring the system or the official who conducts the PIA (e.g., the reviewing official could be the agency's chief information officer). Then, in general, 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.[263]

Unfortunately, few states have statutes comparable to the federal Privacy Act, and the ten or so states that do are all over the map. New York's Personal Privacy Protection Act, for example, requires that each state agency "that maintains systems of records" must comply with FIPPs.[264] But

---

[258] The one exception is the act's rules for social security numbers, which apply more broadly. *See* 5 USC § 552a.

[259] Describe shortcomings; exemptions; challenges in proving damages

[260] 5 U.S.C. § 552a(e)(4)

[261] *See, e.g.,* http://epic.org/blog/2015/02/dod-claim-nsa-in-compliance-with-the-privacy-act-when-it-clearly-is-n.html.

[262] *See* Section 208 of the E-Government Act of 2002, 44 USC 3501(b), which requires agencies to perform a PIA before (i) developing or procuring new technology that collects, maintains, or disseminates personally identifiable information (PII), or (ii) initiating new collections of PII. The Office of Management and Budget (OMB) has authority to provide guidance and oversee the implementation of PIAs across federal agencies. The PIA process requires agencies to review the following: (1) what information is collected; (2) why the information is collected; (3) how the information will be used by the agency; (4) with whom the information will be shared; and (5) how the information is handled and secured when using IT to collect new information or when developing new IT systems to handle collections of PII. When agencies conduct PIAs for "major information systems," as defined in OMB Circular A-130 (Section 6.u.) and OMB Circular A-11 (section 300-4 (2003)), they must provide a more extensive analysis of the consequences of collection and flow of information, the alternatives to the collection and handling as designed, the appropriate measures to reduce risks identified for each alternative, and the rationale for the final design choice.

[263] A program or system may be exempted from the publication requirement if it would raise security concerns or reveal classified information, or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest). *But see* Donohue, at 484 (stating with regard to federal biometric programs that "a strong argument could be made that PIAs provide little by way of limits on the federal development" such programs).

[264] Pub. Off. Law § 94 (1983). A few other states have similar laws, for example, California, Massachusetts, Minnesota, *see* SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS, *supra* note , at 125-26. Additionally, Hawaii has a Uniform

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,[265] Washington does not have a state privacy act.

In any case, none of these state laws discussed or mentioned above have anything resembling the Privacy Act's requirement for publishing SORNs or PIAs and, even more importantly, none of them apply to local governments. There is an exception to this broad generalization, however. All fifty states have a public records or freedom of information law requiring government agencies to disclose certain information to people upon request.[266] 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.[267] These laws generally include some form of privacy exemption, which may be similar (or more restrictive) than the two privacy exemptions in FOIA.[268]

The Washington Public Records Act (PRA) is unusual in that it combines a very broad public disclosure requirement[269] with a very narrowly construed privacy exemption.[270] Thus, an agency exempting information from a record must do so based upon an independent statute that creates a right to privacy and that outweigh the PRA's broad policy in favor of disclosing records.[271] In *Does v. King County*, the Washington Supreme Court found that individuals did not have a right to privacy when they were captured on surveillance video of a public area. As discussed below, the PRA's

---

Information Practices Act, Haw. Rev. Stat. 92F, Indiana has a Fair Info Practices Act, Ind. Code 4-1-6, and Utah has a Government Records Access and Management Act, Utah Code Ann. Sec. 63G-2-101. States with much narrower laws include Alaska, Connecticut, and Wisconsin.

[265] *See* Executive Order 16-01 and SHB 2875.

[266] For a list of all fifty laws, *see* SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS, *supra* note , at 119-21.

[267] *See, e.g.,* Washington Public Records Act, WASH. REV. CODE ANN. 42.56.010(1) (defining "agency to include "all state agencies and all local agencies" and noting further "local agency" includes every county, city, town, municipal corporation, quasi-municipal corporation, or special purpose district, or any office, department, division, bureau, board, commission, or agency thereof, or other local public agency"); New York Freedom of Information Law, New York Pub. Off. Law 86(3) (defining "agency" to mean "any state or municipal department, board, bureau, division, commission, committee, public authority, public corporation, council, office or other governmental entity performing a governmental or proprietary function for the state or any one or more municipalities thereof, except the judiciary or the state legislature").

[268] § 552(b) of FOIA includes two privacy exemptions: Subsection (6), which exempts from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." *See* § 552(b)(6); and subsection 7(C), which exempts from disclosure "records of information compiled for law enforcement purposes … which could reasonably be expected to constitute an unwarranted invasion of personal privacy." *See* § 552(b)(7)(C).

[269] *See, e.g.,* WASH. REV. CODE (WASH. REV. CODE ANN. § 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, 314 P.3d 1093, 1097 (Wash. 2013) (discussing how the PRA mandates "broad public disclosure").

[270] Indeed, the PRA lacks a stand-alone privacy exemption. Rather, it provides several exemptions that address privacy concerns while furnishing a restrictive definition of privacy for the purpose of these exemptions. *See* WASH. REV. CODE ANN. § 42.56.050 (defining privacy in language that parallels the elements of the tort of public disclosure of privacy facts, namely, whether the disclosure of information about the person "(1) Would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public." This same provision also expressly states that it does not "create any right of privacy beyond those rights that are specified in this chapter as express exemptions from the public's right to inspect, examine, or copy public records." *Id.*

[271] For example, personal information in agency employee files is exempt if disclosure would violate the employee's right to "privacy." *See* WASH. REV. CODE ANN. § 42.56.230(3)("Personal information in files maintained for employees, appointees, or elected officials of any public agency to the extent that disclosure would violate their right to privacy").

highly restrictive privacy exemption has had a very direct impact on the Seattle Police Department's recently released body camera policy.[272]

New York's Freedom of Information Law (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."[273] The law goes on to partially define an "unwarranted invasion of personal privacy" by enumerating six categories of information that would qualify, although the exemption is not limited to the examples set forth in the statute.[274] In the non-enumerated cases, the court "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."[275] As discussed below, New York law includes a provision that broadly exempts police and other uniformed officers from the reach of the FOIL,[276] which arguably blocks the public disclosure of footage from body cameras.[277]

Finally, Washington and New York both have several narrower state privacy laws that may affect how cities treat specific records including school records,[278] medical records concerning HIV/AIDS status,[279] and library records.[280]

*****

In sum, most states (including Washington and New York) do not regulate video surveillance of public spaces and while a few states (including Washington) regulate commercial uses of FRT (bills are pending in New York)), none of these laws regulate use of FRT by law enforcement. As for ALPRs, over a dozen states permit their use by law enforcement but limit retention periods and sale to third parties, while exempting ALPR data from disclosure under state public record laws. Washington has not regulated ALPRs, although the SPD has developed its own policy guidelines. There are two proposed bills in New York that regulate permissible uses of ALPRs by law enforcement impose limits on data retention and data destruction obligations. As for drones, almost two-dozen states regulate drone privacy and thereby require law enforcement agencies to obtain a warrant prior to any surveillance use of drones. Washington passed such a drone law but the governor vetoed it, while several such bills are pending in New York. Finally, 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. These results are displayed in Table 1 below.

---

[272] *See infra* Part III.A.

[273] N.Y. Pub. Off. Law § 87(2)(b).

[274] N.Y. Pub. Off. Law § 89(b)(2)(b) states that "An unwarranted invasion of personal privacy includes, but shall not be limited to" various employment and medical records; credit histories; information of a personal nature "when disclosure would result in economic or personal hardship to the subject party and such information is not relevant to the work of the agency requesting or maintaining it" or when "reported in confidence to an agency and not relevant to the ordinary work of such agency"; personal information contained in a workers' compensation record, except as provided by statute; and e-mail addresses or a social network usernames if collected from a taxpayer under provisions of the real property tax law. For a comprehensive discussion of the relevant cases interpreting this provision, *see* https://www.rcfp.org/new-york-open-government-guide/ii-exemptions-and-other-legal-limitations/exemptions-open-records-s-4.

[275] Matter of New York Times Co. v. City of N.Y. Fire Dept., 4 N.Y.3d 477, 485 (N.Y. Ct. App. 2005).

[276] Civil Rights Law §50-a

[277] *See* Cynthia Conti-Cook, *Open Data Policing*, 106 GEORGETOWN L. J. __(2017).

[278] WASH. REV. CODE ANN. § 28A.605.030 and N.Y. Educ. Law § 3222.

[279] WASH. REV. CODE ANN. § 70.02.220 and N.Y. Pub. Health Law § 2782.

[280] WASH. REV. CODE ANN. § 42.56.310 and N.Y.C.P.L.R. § 4509.

	RELEVANT LEGISLATION			
TECHNOLOGIES	**Federal**	**Washington**	**New York**	**Other States**
Video	N	N	N	N
FRT	N	N	N	N
ALPR	N	N	Pending	13
Drones	N	N	Pending	14
LOCAL GOVERNMENT RECORDS	N	N	N	N

In short, 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, in all likelihood they would set state floors on local activity without preventing Seattle or NYC from strengthening these privacy protections 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 III and render them superfluous? In fact, we need look no 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 (proposed), Berkeley, and Palo Alto. California is on the verge of passing Senate Bill 21 (SB 21), a law that requires transparency and accountability in decisions about the use of surveillance technology.[281] Interestingly, SB 21 is not only highly consistent with local surveillance ordinances already in effect California cities, it keeps intact their underlying structure by requiring all local law enforcement agencies to develop surveillance use polices for surveillance technologies and seek approval from governing bodies before deployment. Indeed, Ed Chau, Chair of the Assembly Committee on Privacy and Consumer Protection stated in the committee's bill analysis that SB 21 "is inspired in part by a Santa Clara County ordinance … passed in 2016."[282] Thus, in California, at least, the state legislature responded to innovative city regulations by emulating them, not supplanting them.

III. CASE STUDIES: PRIVACY IN THE CITY

A. *Seattle*

Seattle is Washington State's largest and fastest-growing city with an estimated 2016 population of 704,000.[283] It has a vibrant local economy,[284] a lower crime rate than most medium size U.S. cities,[285] and a crime rate has been falling.[286] The city has not experienced a large-scale terrorist act involving

[281] Senate Bill 21, https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201720180SB21.
[282] https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB21# ("
[283] Based on the 2010 census Seattle ranks as the 22nd largest city in the U.S. It has a metropolitan area population of 4,500,000 (13th in the U.S.).
[284] The city/region is home to a 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.
[285]
[286]

major loss of life or serious property damage, although several smaller terrorist incidents have occurred.[287] Thus, life in Seattle is not colored by a fear of crime or terrorist attacks nor are there 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. In the 2016 elections, 80% of Seattle voters supported the Democratic Party, although the state is more evenly divided between Democrats and Republicans and the former control the governor's office and the state House of Representatives, while the latter control the state Senate.[288] A recent study calculating the level of conservatism of all U.S. cities with a population above 20,000 people ranked Seattle as the third most liberal city in America.[289]

In Seattle, the mayor appoints the chief of police, who serves at the mayor's pleasure.[290] The Seattle Police Department (SPD) is not a very large police force, with approximately 1,400 sworn officers (about 20 officers per 10,000 residents) and a 2016 budget of about $ 320 million out of a total citywide budget of $ 5.1 billion.[291] A closer look at the Seattle Police Department (SPD) reveals a few significant events relevant to this case study. 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.[292] On the other, 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;[293] inadequate preparation for the 1999 World Trade Organization meeting in Seattle, where 100,000 protestors disrupted the conference and engaged in minor rioting;[294] applying a Taser to an African-American woman who was seven months pregnant 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;[295] and two racially charged use of force incidents in 2010, one involving a fatal police shooting of a handicapped Native American, the other abuse of two Latino suspects.[296]

In 2011, the DOJ announced an investigation of the SPD based on these and other widely publicized incidents. The investigation found that the SPD routinely used excessive force and followed policing practices that could lead to discriminatory or biased policing.[297] Although Seattle initially objected to these findings, in 2102 it entered into a consent decree that required the city to

---

[287] https://www.seattle.gov/Documents/Departments/Emergency/PlansOEM/SHIVA/2014-04-23_Terrorism.pdf (discussing, inter alia, a bin-Laden affiliated terrorist group unsuccessful attempt in 1999 to blow up the Seattle Space Needle on New Year's Eve; the Earth Liberation Front 2001 firebombing of a University of Washing facility, costing $7 million in damage but no injuries or loss of life; an American citizen of Pakistani descent 2006 killing of one woman and wounding of five others at the Seattle Jewish Federation; and, the arrest of two Muslim men in a 2006 plot to attack a Seattle military processing facility)

[288] By one seat. *See*

[289] *See* Chris Tausanovitch & Christopher Warshaw, *Representation in Municipal Government*, 108 AMER. POL. SCI. REV. 605 (2014) (the rankings are based on recent large-scale population surveys regarding public policy).

[290] https://www.seattle.gov/financedepartment/17proposedbudget/documents/SPD.pdf

[291] http://www.seattle.gov/financedepartment/16proposedbudget/documents/16proposedbudgetexecsummary.pdf

[292] https://www.seattle.gov/police-manual *See* Friedman, at 17, identifying Chicago and Seattle as among the few cities with publicly available police manuals.

[293]

[294] Although there were no serious injuries of deaths, accusations of police misconduct forced the then chief of police, Norm Stamper, to resign.

[295] http://www.nytimes.com/2012/05/15/us/police-taser-use-on-pregnant-woman-goes-before-supreme-court.html

[296] This latter incident was captured on a bystander's cell phone video, sparking protests over racial tensions and a police department internal investigation.

[297] [cite investigation--https://www.justice.gov/sites/default/files/crt/legacy/2011/12/16/spd_findletter_12-16-11.pdf

adopt new policies and training to address excessive force.[298] The federal monitor overseeing court-ordered police reforms recently stated that the SPD had achieved a dramatic turnaround, and that Seattle now represents "a model of policing for the 21st century."[299] Nevertheless, he concluded that the SPD was not yet fully compliant with the consent decree due in large part to the June 2017 fatal shooting by two white officers of Charleena Lyles, a 30-year-old African-American mother of four.[300] The SPD dispute this conclusion, insisting that the department has met its federally mandated obligations to address excessive force and biased policing.[301]

1. Seattle's Surveillance Ordinance

In 2013, the Seattle City Council City approved a bill and ordinance requiring city departments to obtain council approval prior to acquiring and using certain surveillance equipment.[302] 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 presence in public life."[303] But this was not the first time Seattle enacted a local ordinance regulating police surveillance. In 1979, in response to disclosures that the Seattle police had spied on, photographed and compiled extensive files on hundreds of political activists as well as community and church leaders during the 1960s and 1970s,[304] the city council adopted a police intelligence ordinance.[305] This ordinance (which remains in effect and again was the first of its kind in the country) restricts the SPD from collecting political, religious, and private sexual orientation information unless it is relevant to a crime or the investigation of a criminal act, requires authorization from a lieutenant or above before engaging in such collection, contains specific requirements for auditing police compliance with these and other provisions, and creates a private right of action against the city "for injuries proximately caused by departmental personnel willfully in the scope and course of their duties" and in violation of its restrictions.[306] Using a

---

[298] http://www.seattlemonitor.com/overview/ The Seattle 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." *Id.*

[299] http://www.seattletimes.com/seattle-news/crime/in-major-step-federal-monitor-finds-seattle-police-use-of-force-reforms-are-working/

[300] http://www.seattletimes.com/seattle-news/crime/despite-progress-seattle-police-not-yet-in-compliance-with-reforms-federal-monitor-says/ *But see* http://www.seattletimes.com/seattle-news/crime/seattle-police-dispute-monitors-report-say-theyve-met-federal-reform-standards/. OR https://www.seattletimes.com/seattle-news/in-watershed-moment-seattle-asks-federal-judge-to-find-it-in-compliance-with-court-ordered-reforms/

[301] https://www.seattletimes.com/seattle-news/crime/seattle-police-dispute-monitors-report-say-theyve-met-federal-reform-standards/

[302] *See* Seattle City Council Bill No. 117730, Ordinance No. 124142, (March 26, 2013), establishing a new Chapter 14.18 in the Seattle Municipal Code (SMC), 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 (the "*Seattle Surveillance Ordinance*").

[303] Seattle Surveillance Ordinance*, id.*

[304] Michael Sweeney, *Seattle Law Limits Police In Intelligence Gathering*, WA. 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

[305] [full cite] Few cities other than Seattle have relied on legislation to address the free speech issues associated with police spying. *see* FRIEDMAN, 69-72 (describing District of Columbia's police intelligence law). Most other cities that have restricted police spying on political protests have done so only as a result of protracted litigation. *See* Allan Adler & Jay Peterzelli, *Courts Curtail Political Surveillance by Police Intelligence Units,* Center for National Security Studies (March/April 1981) and *infra* note (discussing the Handschu case).

[306] SMC 14.12.__(allowing liquidated damages of up to $1,000 depending on the nature of the violation).

consensus approach known as the "Seattle Way,"[307] 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.[308]

In 2013, the city council adopted the surveillance equipment ordinance, spurred to action by negative media reports and a public outcry in response to two incidents: the city's acquisition of two small drones,[309] and its installation of surveillance cameras (along with a "mesh network") at Seattle's waterfront, both of which were funded by a $5 million DHS grant.[310] In both cases, the SPD behaved secretively, failing to consult with or notify the city council or the public prior to acquiring or installing the equipment.[311]

The surveillance ordinance required SPD and other city agencies to obtain council approval before deploying "surveillance equipment."[312] More specifically, it obligated the SPD to develop operational and data management protocols for all such equipment. The operational protocols addressed the proper deployment, acquirement, and use of the equipment including information on its purpose,

---

[307] *See* MARK HAMILTON PURCELL, RECAPTURING DEMOCRACY: NEOLIBERALIZATION AND THE STRUGGLE FOR ALTERNATIVE URBAN FUTURES 111, 119 (2008) (describing the Seattle Way as a political procedure with both positive connotation ("the Seattle Way values popular participation, transparent process and meaningful debate") and negative connotations ("it has been decried as a culture that values process and debate over results, that bogs down and can't get important things done").

[308] Sweeney, *supra* . *See infra* notes __ and __.

[309] The drones were never used because the mayor responded to the public controversy by terminating the program. Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES (Feb. 7, 2013), http://seattletimes.com/html/localnews/2020312864_spddronesxml.html ("The announcement [to end the drone program] came one day after the city held a public hearing on a proposed ordinance outlining restrictions for the . . . program, which drew vocal opposition from numerous citizens concerned with intrusions into their privacy").
A year later, Seattle donated the drones to Los Angeles, where they provoked a similar controversy and were never flown. Shawn Musgrave, *LAPD *Still* Doesn't Know What to Do With Its Drones*, MUCKROCK (Oct. 1, 2015), https://www.muckrock.com/news/archives/2015/oct/01/lapd-drones-still-shelf-year-later/. For a more detailed account fo the drone controversy in Seattle and its connection to the surveillance equipment ordinance, *see* Crump, *supra* note , at 1605-11.

[310] Christine Claridge, *Waterfront Surveillance Cameras Stir Privacy Fears*, SEATTLE TIMES (Jan. 31, 2013) http://seattletimes.com/html/latestnews/2020260670_waterfrontcamerasxml.html. Although the city council and the mayor pushed through the authorizing ordinance for the surveillance cameras without significant public input, *see* Matt A. Fiske, *Seattle's new waterfront cameras: The beginning of city-wide surveillance?*, CROSSCUT (Mar. 13, 2013), http://crosscut.com/2013/03/crosscut-investigates-questions-spd-surveillance/, the city soon shelved that program until sufficient protections were put in place following a public outcry, *see* Jillblocker, *City Council looks to limit SPD after public outcry ends another spy cam program*, CAPITAL HILL SEATTLE BLOG (Mar. 6, 2013), http://www.capitolhillseattle.com/2013/03/city-council-looking-to-limit-spd-after-public-outcry-ends-another-spy-cam-program/. A few months later, a similar public response led the city to back down after announcing it would use federal funds for a WiFi network in the port area that residents feared could track cell phones and devices; *see* Christine Clarridge & Jennifer Sullivan, *Seattle Police to Shut Off Wi-Fi After Privacy Backlash*, THE SEATTLE TIMES (Nov. 18, 2013), http://www.govtech.com/public-safety/Seattle-Police-to-Shut-Off-Wi-Fi-After-Privacy-Backlash.html. For a more detailed account of all three controversies and their connection to the Seattle surveillance equipment ordinance, *see* Catherine Crump, *Surveillance Policy Making By Procurement,* 90 WASH. L. REV. 1595, 1605-16 (2016).

[311] Crump, *supra,* note .

[312] The ordinance defines this term as "equipment capable of capturing or recording data, including images, videos, photographs or audio operated by or at the direction of a City department that may deliberately or inadvertently capture activities of individuals on public or private property, regardless of whether "masking" or other technology might be used to obscure or prevent the equipment from capturing certain views." It includes "drones or unmanned aircraft and any attached equipment used to collect data" but excludes "a handheld or body-worn device, a camera installed in or on a police vehicle, a camera installed in or on any vehicle or along a public right-of-way intended to record traffic patterns and/or traffic violations, a camera intended to record activity inside or at the entrances to City buildings for security purposes, or a camera installed to monitor and protect the physical integrity of City infrastructure."

type, specific location, and use (whether continuous or limited to specific circumstances); 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.[313] 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.[314]

The 2013 surveillance ordinance represented a big step forward in bringing transparency and accountability to public surveillance by the SPD. But it suffered from three main shortcomings. First, it defined "surveillance equipment" very narrowly, covering "drones and unmanned aircraft and any attached equipment used to collect data" but excluding many other types of equipment such as body cameras, traffic cameras, and security cameras.[315] 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 so that it covered investigations supported by reasonable suspicion.[316] Third, and most importantly, the Seattle 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.[317] Apparently, this is exactly what happened.

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. In particular, the SPD had purchased and begun using a social media tracking tool, Geofeedia, without seeking approval by the city council or submitting the required protocols.[318] This incident not only generated public controversy but also illustrated the lack of clarity over the scope of the ordinance and whether it applied to equipment (hardware) only or software as well.[319] In any case, the SPD

---

[313] *Id.*, SMC 14.18.20.

[314] *Id.*, SMC 14.18.30.

[315] SMC 14.18.10. The Seattle Police Department Manual addresses a few of these scenarios but mainly from an operational standpoint; *see* Seattle Police Department Manual, Chap. 16.090 (in car video system); Chap. 16.091 (body worn video pilot program); Chap. 16.170 (automatic license plate readers), https://www.seattle.gov/police-manual.

[316] *Id.*, SMC 14.18.40. For a detailed account of how this came to pass, *see* Phil Mocek, Updates to Seattle Surveillance Equipment Bill, MOCEK.ORG (March 15, 2013), https://mocek.org/blog/2013/03/15/updates-to-seattle-surveillance-equipment-bill/; Phil Mocek, Seattle City Council pass ordinance restricting surveillance equipment after Councilmember Harrell slips in a gift for police, MOCEK.ORG (March 15, 2013), https://mocek.org/blog/2013/03/19/seattle-passes-ordinance-restricting-surveillance-after-harrell-slips-in-gift-for-police/.

[317] https://www.aclu-wa.org/news/aclu-urges-city-council-put-teeth-surveillance-law-delay-vote-add-auditing-process (calling for the ordinance to include an auditing process in which the city auditor would "examine relevant documentation and produce a report on how police have carried out the ordinance").

[318] Ansel Herz, *How the Seattle Police Secretly—and Illegally—Purchased a Tool for Tracking Your Social Media Posts*, THE STRANGER (Sept. 28, 2016)

[319] An SPD spokesperson told a local newspaper that the Geofeedia purchase "should have been cleared … in accordance with the Seattle Municipal Code" (i.e., the surveillance equipment ordinance), *id.,* while a local TV station reported that according to sources inside the police department, "the law applies only to hardware like cameras, not software like Geofeedia. http://www.kiro7.com/news/local/opa-investigates-reported-spd-acquisition-of-tool-that-tracks-social-media-posts/451898379 (also stating that according to a different SPD official, the department had started using new software from a firm called Babel Street). A few weeks later, the ACLU of 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; *see* https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-

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.

The revised ordinance began with a draft text developed by the ACLU of Washington State (ACLU-WA).[320] The city council then 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, and advocacy groups like the ACLU-WA. This group met over the course of several months to discuss and revise the ACLU-WA draft.[321] The revised ordinance, which the mayor signed into law on August 2, 2017,[322] repealed and replaced the 2013 ordinance, changing it in six fundamental ways. First, it re-conceptualizes the scope of the ordinance by jettisoning "surveillance equipment" in favor of two newly defined terms: "surveillance technology" (broadly defined as "any electronic device, software program, or hosted software 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) 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").[323] Second, it renames the operating and data management protocols "Surveillance Impact Reports" (SIRs) and required that all SIRs must be posted to the city's web site. Third, it provides that departments filing SIRs must conduct community outreach prior to council approval,[324] and that a newly formed community advisory group would assist the council in its surveillance technology decision-making.[325] Fourth, 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

---

target. Twitter soon followed, *see* , http://www.chicagotribune.com/bluesky/originals/ct-twitter-suspends-geofeedia-access-bsi-20161011-story.html.

[320] The revised Seattle ordinance closely resembles a model ordinance developed (or at least distributed) in 2013 by the Washington State ACLU; *see* This model local ordinance was a precursor to a national campaign that the ACLU e launched in 2016 under the name of the Community Control Over Police Surveillance (CCOPS), with the goal of introducing surveillance ordinances in cities across the country. *See* https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf According to the ACLU: "Local city councils alone, not the police, should be empowered to decide if and how surveillance technologies are used, through a process that maximizes the public's influence over those decisions." *See* https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.

[321] Email from Mary F. Perry, Director of Transparency and Privacy, Seattle Police Department to Ira Rubinstein, (September 11, 2017) (on file with author); Email from Amy Tsai, Seattle City Council Legislative Analyst & Capital Coordinator to Ira Rubinstein (October 9, 2017) (on file with author). Nor is the first time that the ACLU-WA and SPD collaborated on privacy guidelines; *see* http://www.seattletimes.com/seattle-news/crime/seattle-police-wins-praise-for-safeguards-with-facial-recognition-software/

[322]

[323] SMC Section 14.18.010 (2017). 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. *See infra* Part IV.2 for further discussion. The ACLU-WA worried that a narrow definition would undermine transparency and accountability. 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." 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 city 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. https://www.aclu-wa.org/news/seattle-adopts-nation%E2%80%99s-strongest-regulations-surveillance-technology.

[324] SMC Section 14.18.020(C) (2017).

[325] SMC Section 14.18.070(4) (2017).

suspicion, but now requires a showing of imminent risk of death or serious injury.[326] Fifth, it requires all city departments to create an inventory of existing surveillance technologies and process them for council approval at a rate of at least one per month.[327] Last, it adds several new provisions related to oversight and enforcement including (a) annual compliance reviews by the city auditor and inspector general; (b) annual equity impact assessments conducted by the chief technology officer (who also has the authority to order any department that is out of compliance to cease acquisition or use of the surveillance technology); and (c) a private right of action against the city for injunctive or declaratory relief for a material violation of the new bill, after a 90-day opportunity for the city department to address the concern. [328] The ACLU-WA praised the replacement ordinance as "the strongest measure adopted by an American city to regulate the acquisition of surveillance technology."[329] In fact, the new Seattle ordinance compares very favorably with strong measures recently adopted in Santa Clara County,[330] and still under consideration in Oakland.[331]

[add paragraph on body cameras]

2. Seattle's Privacy Principles and Processes

In 2014, Seattle launched a Privacy Initiative aimed at providing greater transparency into the city's data collection and use practices.[332] Moving beyond the narrow focus of the surveillance ordinance, this new initiative seeks to ensure that the city takes "appropriate steps to facilitate the collection, use, and disposal of data [that is, any sort of personal 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."[333] As part of the Privacy Initiative, the Mayor convened a group of stakeholders from across city departments (including the SPD) to carry out three tasks: establishing a set of governing principles; devising an approach to educating city departments on privacy practices; and determining how to assess compliance.[334] They were assisted by a Privacy Advisory Committee comprised of privacy researchers, practitioners, and community representatives, including noted privacy experts from the University of Washington and Microsoft.[335]

In 2015, the city released Privacy Principles governing its data collection and use practices.[336] This set of six principles provides an ethical framework for developing appropriate policies, standards

---

[326] SMC Section 14.18.030(C)(1) (2017).
[327] SMC Section 14.18.070(3) (2017).
[328] SMC Section 14.18.060-.070 (2017).
[329] https://www.aclu-wa.org/news/seattle-adopts-nation%E2%80%99s-strongest-regulations-surveillance-technology.
[330] SANTA CLARA CTY., CAL., ORDINANCE NS-300.897 (June 21, 2016). *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), https://www.paloaltoonline.com/news/2016/06/18/county-cracks-down-on-police-surveillance-technology.
[331] Darwin Bond Graham, *Oakland Privacy Commission Approves Surveillance Transparency and Oversight Law,* EAST BAY EXPRESS, https://www.eastbayexpress.com/SevenDays/archives/2017/01/06/oakland-privacy-commission-approves-surveillance-transparency-and-oversight-law.
[332] http://murray.seattle.gov/city-of-seattle-launches-digital-privacy-initiative/ *See also* City Council Resolution #31570 (Feb. 23, 2015), http://www.seattle.gov/Documents/Departments/InformationTechnology/City-of-Seattle-Privacy-Principles-FINAL.pdf.
[333] http://murray.seattle.gov/city-of-seattle-launches-digital-privacy-initiative/ *See also* Angelique Carson, *Seattle Launches Sweeping, Ethics-Based Privacy Overhaul*, THE PRIVACY ADVISOR (Nov. 7, 2014), https://iapp.org/news/a/seattle-launches-citywide-privacy-initiative/ (lauding the Seattle privacy initiative as one of the most progressive in the country).
[334] http://murray.seattle.gov/city-of-seattle-launches-digital-privacy-initiative/
[335] https://www.seattle.gov/tech/initiatives/privacy/privacy-advisory-committee
[336] City of Seattle Resolution 31570 (Feb. 23, 2015). Five months later, the city also adopted a citywide privacy statement providing direction to all city departments about their obligations to follow the new principles, the privacy statement and

and practices regarding the public's personal information.[337] The city also outlined a three-part process for privacy reviews, consisting in (1) a self-service assessment using a standardized questionnaire; then (2) a privacy threshold analysis to be reviewed with a privacy "champion" appointed by each city department; followed by (3) a full-scale privacy impact assessment.[338] Additionally, the city allocated resources in its 2016 budget to launch an online training and awareness program, required of anyone who touches the public's personal data, and the hiring of a full-time Chief Privacy Officer,[339] and adopted 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.[340]

While the Privacy Program Brochure lists surveillance technology prominently as a motivating factor for the new program,[341] the Program's privacy policy specifically excludes surveillance technologies from its purview as the city's surveillance ordinance already covers them.[342] 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 "establishing consistent standards and priorities for IT investments" and protecting city resources against threats, "especially related to security and privacy risks."[343] This consolidation covers the IT activities of the SPD as well as civilian departments.[344] 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.

B. *New York City*

New York City is the wealthy, thriving financial and cultural capital of the U.S. It is America's most populous city with an estimated 2016 population of over 8.5 million people.[345] On par with London and Tokyo, New York is a truly "global city."[346] Like Seattle, NYC has a lower crime rate than similarly sized cities.[347] Indeed, the city now enjoys historically low crime rates.[348] In stark contrast

---

a privacy review process. In 2015, the University of Washington and City of Seattle 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, City of Seattle Blog, available at, https://www.seattle.gov/tech/initiatives/smart-cities. For a case study of open data in Seattle, *see* Whittington, *supra* note __.

[337] City of Seattle Department of Information Technology, "City of Seattle Privacy Program" (Oct. 2015), http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf (the Privacy Program Brochure). The six principles constitute a local statement of the Fair Information Practices Principles, *see* , and include (1) a statement valuing privacy; (2) collection limitations; (3) use limitations; (4) accountability; (5) disclosure limitations; and (6) accuracy.

[338] *Id.* at 8.

[339] In May 2016, the city appointed its first Chief Privacy Officer, who has since been replaced. *See* http://techtalk.seattle.gov/2017/07/11/city-of-seattle-hires-ginger-armbruster-as-chief-privacy-officer/.

[340] To date, Seattle has posted only one PIA, which assesses a smart metering pilot project referred to as the Seattle City Light Advanced Metering Initiative (AMI; *see* http://www.seattle.gov/tech/initiatives/privacy.

[341] Privacy Program Brochure, p. 4 ("Technology's impact on privacy […] Technologies including unmanned aircraft (drones), wireless communications networks and various forms or image capture such as surveillance and body-worn cameras while useful to aspects of our mission to protect people and property can conflict with privacy.)

[342] Privacy Program Brochure at 35 (data not falling under the Program's protections included "[d] ata collection or use of technologies governed by the City's Surveillance Ordinance (SMC 14.18)").

[343] https://www.seattle.gov/tech/initiatives/it-consolidation

[344]

[345] Cite. NYC is thus twelve times the size of Seattle. The metropolitan area population of NYC is 20.2 million, which is also the most populous in the U.S.. Cite. The NY metro area is thus 4.5 times the size of the Seattle metro area.

[346]

[347]

with Seattle's lack of major terrorist incidents, however, the September 11, 2001 attacks on NYC's World Trade Center by the Islamist terrorist group al-Qaeda killed almost 3,000 people (including 343 firefighters, and 71 police officers), injured over 6,000 people, and caused at least $10 billion in damage to property and infrastructure.[349] The attacks changed many things in NYC including how the NYPD understood its mission.[350] Following 9/11, then Police Commissioner Raymond A. Kelly quickly shifted NYPD resources from crime fighting to counter-terrorism.[351] He created the first local Counter-Terrorism Bureau and expanded the existing Intelligence Bureau (and he recruited a Marine Corps general to run the former and a senior CIA official to take charge of the latter).[352] In addition, Kelly created a controversial Demographics Unit[353] In his book, *Vigilance,* Kelly argues that these and related decisions helped to avert sixteen "active terrorist plots" during his almost twelve year (second) term as police commissioner.[354]

In NYC, the mayor appoints the chief of police, who serves at the mayor's pleasure.[355] The NYPD is the largest police force in the country, with over 36,000 sworn officers (about 42 officers per 10,000 residents) and a 2016 budget of over $5 billion[356] out of a total city budget in 2016 of more than $80 billion.[357] Like Seattle, NYC is very liberal,[358] with a heavy Democratic presence. As of April 2016, 69% of registered voters in the city were Democrats and only 10% were Republicans; this drops to 49% and 23% respectively at the state level.[359] Elected officials in NYC 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,[360] he and Democratic Governor (Andrew Cuomo) have a long running personal feud that undermines city initiatives requiring collaboration between the city and state governments.[361]

The NYPD has had 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.[362] The settlement decree outlined a series of intelligence reforms known as the Handschu Guidelines, which imposed restrictions on political investigations and provided for

---

[348] The seven major felony offenses fell by over 45% in the sixteen-year period from 2000 to 2016 and has since hekd steady at the lower level. *See* http://www1.nyc.gov/assets/nypd/downloads/pdf/analysis_and_planning/seven-major-felony-offenses-2000-2016.pdf. *See also* http://nypost.com/2017/03/01/nycs-low-crime-rate-just-got-even-lower/

[349]

[350] KELLY at 176.

[351] The 9/11 attacks radically altered federal counter-terrorism activity as well. Some of the more prominent changes included the creation of DHS; enactment of the USA Patriot Act; the use of mass surveillance programs against American citizens.

[352] KELLY, 166, 171.

[353] "The idea was a simple one: we should know who lives where." *Id.* at 205. The unit was disbanded in 2014 after being accused of spying on Muslim communities in NYC; its tactics were also the subject of two law suits. *See* https://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html

[354] *Id.* at 208-56 (2002-2013)..

[355] City Charter

[356] http://council.nyc.gov/budget/wp-content/uploads/sites/54/2016/06/nypd.pdf

[357]

[358] (8th in the country)

[359] *NYS Voter Enrollment by County, Party Affiliation and Status*

[360] Michael Barbaro & David W. Chen, *De Blasio Is Elected New York City Mayor,* NEW YORK TIMES (Nov. 5, 2013).

[361] 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.

[362] Handschu v. Special Services Divison, 605 F. Supp. 1384 (S.D.N.Y. 1985), *aff'd* 787 F.2d 828 (2d Cir. 1986).

civilian oversight of the NYPD's compliance with the guidelines. The settlement also created the Handschu Authority, a three-member panel consisting of one civilian and two deputy commissioners, whose approval was required for investigations longer than 30 days.[363]

In 2003, the court agreed to modify the guidelines in the wake of the 9/11 terrorist attacks.[364] The 2003 Modified Handschu Guidelines, inter alia, abolished the Authority's approval role and reduced its function to reviewing records and investigating complaints from the public.[365] But this did not end the long running controversy over NYPD spying on political (and religious) activity. In 2011, the Associate Press ran a series of articles demonstrating extensive NYPD surveillance and attempted infiltration of local Muslim communities and mosques,[366] which resulted in a new law suit and still further revisions to the modified guidelines.[367]

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.[368] 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 mechanisms 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 cameras.[369]

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 putg him in a chokehold. The incident was captured on a cell phone video that went viral, showing Garner yelling "I can't breathe."[370] Three weeks later, a police officer in Ferguson, Missouri shot an unarmed black teenager named Michael Brown, leading to violent protests and the birth of the Black Lives Matter movement.[371]

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

The DAS Guidelines. – One of the steps taken by Commissioner Kelly to help protect New Yorkers against future terrorist attacks was the creation of the DAS, which was described above. The New York City Charter grants the NYPD plenary power to preserve order and enforce criminal law, and the NYPD exercised this power in creating the DAS, without the need for any additional authority or direction by the city council.[372] However, the team responsible for developing and implementing the DAS anticipated that wide-scale police surveillance of public spaces would raise significant

[363] Handschu, 605 F. Supp. at 1420-24.
[364] Handschu v. Special Services Divison, 273 F.Supp. 2d 327 S.D.N.Y. 2003).
[365] *Id.*
[366] For a list of relevant references, *see* Friedman at 377, n. 4.
[367] https://www.lawfareblog.com/settling-more-nypds-new-oversight-deal
[368] http://www.nytimes.com/2013/08/13/nyregion/stop-and-frisk-practice-violated-rights-judge-rules.html
[369] https://www.nytimes.com/2017/04/21/nyregion/judge-police-body-cameras-new-york.html?_r=0. For a discussion of the NYOPD's body camera policy, *see infra* text accompanying notes __.
[370] https://www.nytimes.com/2015/06/14/nyregion/eric-garner-police-chokehold-staten-island.html
[371] https://www.usatoday.com/story/news/nation-now/2016/08/08/how-michael-browns-death-two-years-ago-pushed-blacklivesmatter-into-movement/88424366/
[372] New York City Charter, §435(a).

privacy concerns.[373] Accordingly, they released draft privacy guidelines for a 30-day comment period in 2009 and later that spring published revised guidelines in final form.[374]

The DAS guidelines established policies and procedures serving two main goals: "to limit the authorized use of counterterrorism technologies and to provide for limited access to and proper disposition of data."[375] In keeping with the former, the guidelines prohibit targeting or monitoring by the DAS solely based on actual or perceived membership in protected categories, which are very broadly understood. 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.[376] Additionally, secondary uses beyond counterterrorism purposes and data sharing with a third party both require approval at the deputy commissioner level.

The 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 imposing sanctions if data is used for unauthorized purposes (these rules also apply to "stakeholder" representatives from partner companies, who are also denied access to personally identifiable information captured by the system); and requiring the creation of an immutable data logs, which are subject to periodic compliance reviews by a NYPD integrity control officer.[377] 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 (for example, 30 days for video; five years for metadata related to the DAS; and five years for ALPR data).

The NYPD developed the DAS guidelines voluntarily using an informal version of notice-and-comment rulemaking. This "rulemaking" procedure is hard to assess, however, since 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.[378]

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, their informal approach to rulemaking hardly satisfies core requirements of the Administrative Procedure Act (APA), which requires an agency engaged in notice-and-comment rulemaking to provide an opportunity for public comment but also to respond to each substantive comment it receives,

---

[373] *Supra* note

[374] NYPD, Public Security Privacy Guidelines (April 2, 2009), http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf (the "Privacy Guidelines").

[375] *Privacy Guidelines, supra* at 1.

[376] *Id.* at 2-3.

[377] *Id.* at 6-7.

[378] *See* Constitution Project, Comments Regarding the New York City Security Privacy Guidelines for the New York City Police Department's (NYPD) "Domain Awareness System," Apr 6, 2009, http://www.constitutionproject.org/wp-content/uploads/2012/09/137.pdf. After noting several positive features in the document, the Constitution project identified three needed improvements: First, shortening the retention period for ALPR data and metadata; second, adopting more stringent rules for private "stakeholder" access to the system and its data (including explicit limits on allowable purposes for such access and on the number and identity of stakeholder representatives who will be granted such access); and, third improved audit requirements such as biannual reviews to assess not just compliance with internal rules but also the *effectiveness* of the system in serving its intended purpose. It does not appear that the NYPD modified the guidelines in response to any of these comments.

explaining why it chose either to adopt or disregard it.[379] This did not happen. Furthermore, the NYPD 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.[380] 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. 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 any 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.[381] The bill, called the Public Oversight of Police Technology (POST) Act, requires the reporting and evaluation of surveillance technologies used by the NYPD (broadly defining such technologies as "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"). More specifically, the POST Act requires the NYPD to issue a surveillance impact and use policy (the "SIU Policy") about covered surveillance technologies, including a detailed description of their capabilities, the rules, processes and guidelines regulating access or use (including "whether the department obtains a court authorization for each use" and, if so, the specific type of authorization that is sought); any safeguards and security measures designed to protect the information collected; policies relating to the retention, access, and use of data collected by such technology; policies regarding data sharing with local, state, federal, or private entities; a description of internal audit and oversight mechanisms; and any reports on the health and safety effects of the surveillance technology.[382] 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 and the mayor, and posts it to the department's website.[383] Finally, the bill requires the inspector general for the NYPD to audit the SIU Policy to ensure compliance with its terms, describe any violations, and publish recommendations, if any, relating to revisions of the policy.[384]

The POST Act is not the product of any public outcry over newly installed surveillance systems and in this way clearly differ from the surveillance ordinances adopted in Seattle and other cities. As noted above, the NYPD imposed the DAS guidelines from the outset in a largely successful effort to head off privacy concerns. So perhaps the POST Act reflects some combination of political

---

379

380 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 the LMSI. The request included documents transmitted between the NYPD and DHS including, inter alia, "the extent to which the information will be shared with other law enforcement agencies or other entities." The NYPD denied the FOIL request, and the denial was upheld despite a legal challenge; *see* Matter of New York Civil Liberties v. N.Y.C. Police Department, N.Y. Misc. LEXIS 2542 *; 242 N.Y.L.J. 3 (2009).

381 http://www.nydailynews.com/news/politics/pol-pushes-bill-nypd-unveil-high-tech-surveillance-tools-article-1.2985193

382 New York City Council, Interim Bill No. 1482 (March 1, 2017), § 14-167.

383 *Id.*

384 *Id.* § 809.

ambitions on the part of its sponsors and some hesitation by the City Council to tie the hands of a police department that has foiled several terrorist attacks in the years following 9/11.[385] 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 a final report (the SIU Policy) after public comment, and provide it to the City Council and Mayor, but does not require their approval prior to any use of the technology in question.[386] While the POST Act forces greater transparency upon the NYPD, it dispenses with enforcement mechanisms or penalties for non-compliance.[387] Moreover, and this too differs from the SPD response to 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."[388] The bill's sponsors and supporters rejected this criticism as wildly overblown, noting that "the NYPD always resists transparency measures" and that it unhelpful to mischaracterize the bill as requiring the NYPD to disclose "operational details" on its technology.[389] As the Brennan Center pointed out, "the federal government routinely discloses its ground rules for using new technologies and strongly encouraged local agencies to be open to the public about the surveillance technologies they use."[390]

[add paragraph on body cameras]

2. NYC Privacy Principles

NYC does not have citywide privacy principles or any privacy initiative of comparable breadth to that of Seattle. The closest it comes is a set of guiding principles for smart cities announced in 2016.[391] These guidelines originated with the Mayor's Office of Technology and Innovation, which conducted research identifying 450 best practices regarding the use of sensor technologies and other Internet of Things (IoT) deployments.[392] NYC's IoT guidelines consolidate these best practices under five headings: privacy and transparency, data management, infrastructure, security, and operations and sustainability.[393] Although the privacy and transparency principles match up reasonably well with the FIPPs, it is not clear if the IoT Guidelines impose binding obligations on city agencies.[394] Indeed, the guidelines may be nothing more than recommendations, rather than

---

[385] Cite Kelly

[386] Compare Seattle law

[387] same

[388] Ben Kochman & Erin Durkin, *NYPD officials argue 'very bad' City Council bill would aid terrorists in working around high-tech surveillance tools*, NEW YORK DAILY NEWS (March 1, 2017), http://www.nydailynews.com/new-york/nypd-officials-bill-terrorists-dodge-surveillance-article-1.2986286

[389] *Id.*

[390] https://www.brennancenter.org/blog/new-york-city-making-its-citizens-safer-overseeing-police-technology (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). [cite June testimony]

[391] *See* New York City Mayor's Office of Technology and Innovation's, NYC Guidelines for the Internet of Things, https://iot.cityofnewyork.us/privacy-and-transparency/ ("IoT Guidelines").

[392] https://iot.cityofnewyork.us/about/

[393] NYC took the lead in developing the IoT Guidelines bit more than twenty other cities (including Seattle) have agreed to adopt them as well. *Id.*

[394] The IoT Guidelines cross-reference a number of 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 (Local Law 11 of 2012 (previously Introduction 0029A-2010)), but do not refe to any citywide privacy policies or laws. 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 by adopting

legally enforceable requirements.[395] Nor does NYC have a Chief Privacy Officer with citywide responsibility for ensuring that all city agencies abide by published privacy principles or follow a process for privacy reviews.[396] Moreover, the IoT Guidelines seems to exempt law enforcement projects. As the FAQ notes, "If you are looking to deploy an IoT solution in a public space (e.g. parks, public buildings, et.) or using City assets (e.g. City government funding, light poles, etc), these guidelines apply to you. Special circumstances and concerns may exist for IoT systems and/or data related to public safety, security and law enforcement."[397] This carve out is consistent with the Mayor's 2010 Executive Order authorizing the Department of Information Technology and Telecommunications (DoITT) to consolidate and manage IT infrastructure and establish and enforce coordinated citywide IT policies, which allows a group consisting of the DoITT, Police, and Fire Commissioners to determine that certain technology initiatives and systems "fall outside the purview of this Executive Order."[398]

IV. THE CASE FOR PRIVACY LOCALISM

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 play this role: Paul Schwartz observes that states act as first movers in identifying and regulating emerging privacy concerns, provide innovative approaches, and enable simultaneous experimentation with different policy solutions.[399] Based on the Seattle and NYC case studies, the time is ripe to expand this characterization to cities as well. This Part argues that the Seattle and NYC experiments in local privacy regulation are likely to succeed. It assesses the anticipated benefits of the two city's surveillance ordinances and privacy principles, identifies several policy concerns, and finds that the balance lends support to privacy localism.

---

appropriate administrative, technical and physical safeguards to ensure the confidentiality of personal records and destroying those records once the purpose of collecting that information was achieved. *See* Committee on Technology, Hearings on Int. 0627-2015 (Feb. 1, 2015). The bill did not advance, however, in part due to objections voiced by the Mayor's office 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." *See* Testimony of Mindy Harlow, Director, Mayor's Office of Operations, http://legistar.council.nyc.gov/View.ashx?M=F&ID=4233458&GUID=87B6F563-96A0-433A-ACD8-B36BC7371D67..

[395] On the one hand, the FAQ accompanying the guidelines state "These guidelines do not replace existing City policies and laws – they are intended to supplement and support them, and in many cases may reference these related policies and laws (e.g. open data laws) directly." On the other, the FAQ also states "The New York City Mayor's Office of Technology and Innovation, in coordination with the City of New York Technology Steering Committee, oversees the citywide implementation and broad enforcement of the IoT Guidelines. City agencies are responsible for implementing and enforcing the guidelines when deploying and managing IoT projects." *See* NYC Guidelines for the Internet of Things, FAQ, https://iot.cityofnewyork.us/faq/.

[396] This contrasts with the extensive published policies regarding IT security; *see* http://www1.nyc.gov/site/doitt/business/it-security-requirements-vendors-contractors.page. Laura Negron is the Chief Privacy Officer of the Department of Operations but the author has been unable to find any publicly available description of her role in city government. And the annual report from the Mayor's Office of Operations makes no mention of privacy; *see* Mayor's Management Report, http://www1.nyc.gov/assets/operations/downloads/pdf/mmr2017/2017_mmr.pdf.

[397] Thus, it would appear that the DAS is not covered by the IoT Guidelines, even though a smart city brochure from the Mayor's Office of Technology and Innovation lists one of its components—the gun shot detection system—as one of ten case studies. *See* https://www1.nyc.gov/site/forward/innovations/smartnyc.page.

[398] New York City, Executive Order No. 140, § 5 (Oct. 20, 2010), nyc.gov/html/records/pdf/executive_orders/2010EO140.pdf.

[399] Schwartz, *supra* note

Next, it argues that there are two additional reasons in favor of privacy localism as carried out in Seattle and NYC. The first relates to what I call the public surveillance gap, that is, the failure of both Fourth Amendment doctrine and federal (and hence state) electronic surveillance law to offer much protection against government surveillance of public roads, streets, sidewalks, parks, plazas, and other urban gathering places. Both in their structure and content, the local surveillance ordinances help fill this gap. And they do so in an innovative manner that also respects the political and cultural differences between Seattle and NYC (including differences in their level of concern over terrorist attacks). The second reason relates to a new emphasis on governance rules and agency design as solutions to Fourth Amendment doctrinal deficiencies and lack of transparency and accountability in modern policing. Chris Slobogin,[400] Barry Friedman and Maria Ponomarenko,[401] and Daphna Renan[402] have all turned to administrative law as a new source of insight into these longstanding problems.[403] And privacy localism perfectly exemplifies this administrative turn.

A. Assessing Local Privacy Regulation in Seattle and New York

Seattle and New York have taken important first steps to define transparency and accountability obligations for police departments in their use of surveillance technologies and for city departments more generally concerning their collection, use, and disclosure of personal data. Neither city has engaged in these regulatory activities long enough to provide much data on how well things are working in practice. (This is especially true in NYC, where the POST Act is still pending.) Despite this lack of data, it is still possible to examine the rulemaking process and substantive outcomes in both Seattle and New York and evaluate the likelihood of the new regulations achieving their stated goals and fostering the values of local autonomy such as innovation, diversity, and participation, and to addresses potential obstacles and policy concerns.

1. Anticipated Benefits

The primary goals of the surveillance ordinances and data governance principles adopted (or under consideration) in Seattle and NYC are transparency and accountability, which are also the primary mechanism for achieving secondary goals such as adopting to changes in technology, restoring and maintaining public trust, and balancing (1) public safety and civil liberties (the surveillance ordinance and (2) city operations and privacy (the privacy principles). To begin with the surveillance ordinances: Overall, they 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 data governance practices. Such transparency allows privacy advocates (lawyers, activists, journalists, technologists, citizens) to generate politically relevant information about privacy protection, which in turn fosters research and analysis, working behind the scenes to assist organizations in improving their practices,

---

[400] Slobogin, *supra* note

[401] Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 101 (2015).

[402] Renan, *supra* note

[403] *See also* Kami Chavis Simmons, *New Governance and the "New Paradigm" of Police Accountability: A Democratic Approach to Police Reform*, 59 CATH. U. L. REV. 373, 408–09 (2010); David Sklansky, *Police and Democracy*, 103 MICH. L. REV. 1699, 1706 (2005); Jonathan M. Smith*, Closing the Gap Between What Is Lawful and What Is Right in Police Use of Force Jurisprudence by Making Police Departments More Democratic Institutions,* 21 Mich. J. Race & L. 315, 340–41 (2016).

commenting on proposed uses, and where necessary exerting leverage through the threat of bad publicity.[404]

The Seattle and NYC 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 when they are publicized. It is too soon to say which approach will prove more effective. The Seattle process gives elected representatives the final word but (as discussed in the next section) imposes significant costs and potential backlogs and delays in securing approvals. The New York 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 any political oversight. Moreover, since the proposed bill includes audits but no penalties for non-compliance, how much does the NYPD risk if its internal cost-benefit calculations favors pushing the envelope to the outer boundaries of what the POST Act allows?

As for data governance, the two cities rely on similar privacy principles but Seattle has a far more extensive program than NYC in terms of both breadth (all departments and not just IoT projects) and depth (including a greater emphasis on PIAs). It is also worth emphasizing that the Seattle PIA process fills a gap in federal and state law. Recall that the Privacy Act and the related E-Government Act require federal agencies to prepare both SORNs and PIAs. These laws do not apply to state agencies and Washington State lacks a mini-Privacy Act. Thus it falls to the Seattle Privacy Initiative to ensure that the city takes advantages of these processes at the local level.

Again, it is too soon to say if the Seattle program will yield superior results. To date, Seattle has published only one PIA, covering the deployment of smart meters by Seattle City Light (the city-owned electric utility). Although some privacy activists initially objected to the program,[405] it is now offered with an opt-out option that covers most circumstances.[406] In addition, City Light designed the program so the data collection and transmission remains limited[407] and the Seattle CPO not only prepared a PIA,[408] but it also hired an outside law firm to suggest actions to mitigate potential privacy risks.[409] Nevertheless, in May 2017 the ACLU voiced significant concerns about the smart meter program, criticizing the smart meter PIA as unclear, inadequate and incomplete.[410] More PIAs

---

[404] *See* COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 95-132 (2008)(describing these and other modes of advocacy).

[405] *See, e.g.,* Molly Connelly and Jan Bultmann, Seattle City Light: Seattlites Need an Opt-In Policy for Smart Meters, SEATTLE PRIVACY COALITION BLOG (Mar. 3, 2014), available at https://www.seattleprivacy.org/advanced-metering-devices-and-customer-choice/.

[406] Seattle City Light, Advanced Metering: Opt-Out Policy, http://www.seattle.gov/light/ami/opt-out.asp.

[407] The program's website explains, "personally identifying information (such as name, address, or account number) is not stored in the meter nor is it sent through the wireless network. Only the meter number and the amount of energy a customer uses will be relayed through the wireless network."

[408]

[409]

[410]

are needed to determine if the problems identified by the ACLU reflects flaws in this PIA or indicates a systematic weakness in the PIA process itself.

Even though there is insufficient data to determine if the Seattle and NYC privacy ordinances and data governance principles will achieve their stated goals in practice, it is already clear that both cities, in their own ways, are trying out innovative privacy protections. This embrace of local autonomy in the privacy sphere demonstrates policy leadership in three ways. First, Seattle and NYC (indeed, all of the cities that have enacted or are now considering surveillance ordinances) recognize that public surveillance, if pervasive, erodes civil liberties and engenders mistrust of government, including local police forces. And they implicitly understand that the time for action is now, especially in view of the uncertain path of Fourth Amendment doctrine (discussed below) and the absence of federal or (in many cases) state legislation. Second, they are experimenting with a novel approach: instead of enacting one-off laws that address a specific technology (ALPRs, FRT, drones), they have devised a comprehensive, iterative method for reviewing *all* surveillance technologies, using a procedure that not only captures emerging technologies but allows for the city to reassess prior decisions in light of new threat assessments and other changes in local conditions. Third, the cities are proceeding in the best tradition of local autonomy, experimenting with diverse solutions that reflect key differences in how political leaders in Seattle and NYC weigh the social costs of surveillance against the risk of catastrophic losses of a potential terrorist attack. In light of NYC's sheer size, the number and importance of its landmark buildings and public and private spaces, its losses in the 9/11 attack, and the human and symbolic importance of keeping it safe from future attacks, it is not surprising that the review process under consideration in NYC is less onerous for the police than the more burdensome process now in place in Seattle.

2. Policy Concerns

At least three policy concerns require brief discussion in this section. These policy concerns may be expressed in the form of three questions: (1) Do cities like Seattle and NYC have sufficient expertise and resources to maintain their innovative roles and follow through on robust privacy management programs involving both law enforcement and civilian agencies? (2) Is the Seattle model unduly burdensome, given the very large number of surveillance impact reports and PIAs potentially required under local law and policy? And (3) Are these cities relying too heavily on legal instruments as opposed to technology instruments to achieve their stated policy goals?

Expertise and resources. – Federal and state privacy regulators have years of experience and considerable resources to draw on as they go about their tasks. For example, Congress has been writing federal privacy legislation for almost fifty years and draws on ample staff through its committee structure. Many states have taken the lead in regulating privacy and California has amassed a remarkable record of innovation and success in enacting privacy legislation. The "California effect" alone suggests that the state devotes sufficient resource to protecting privacy.[411] The FTC's Division of Privacy and Identity Protection has a staff of 54 lawyers, paralegals, investigators, and technologists and a budget of $10.1 million.[412] State AGs have smaller privacy

411

412 FED. TRADE COMM., FISCAL YEAR 2018 CONGRESSIONAL BUDGET JUSTIFICATION 141 (2017), https://www.ftc.gov/system/files/documents/reports/fy-2018-congressional-budget-justification/2018-cbj.pdf.

staffs and budgets but often join together in multi-state investigations, allowing them "to share expertise and conserve resources."[413]

In contrast, when Seattle launched its 2015 privacy initiative, it hired a new CPO who had one staff member and a budget of $ x.[414] Privacy resources in the NYC government are not much larger. However, that does not make them insufficient. After all, neither Seattle nor NYC engage in any enforcement activity. Seattle draws on the expertise of a Privacy Advisory Committee, just as the city council turns to the ACLU and others advocacy groups for model legislation. The "Seattle Way" seeks consensus and thereby encourages the city to convene stakeholder groups from city departments and external experts and advocates to help draft major bills such as 2017 surveillance ordinance. These internal dynamics and external resources may be enough for now. Still, it seems unlikely that existing resources will be adequate to handle the onslaught of incoming SIRs under the Seattle surveillance ordinance or the number of PIAs the CPO needs to perform.

During the public hearings on revising the Seattle surveillance ordinance, the SPD did not oppose the bill but it did argue that if the revised ordinance covered "surveillance data," it would become unworkable for two reasons. First, a broad understanding of "surveillance data" would force city staff and council members alike to review hundreds if not thousands of city IT systems, thereby creating a bottleneck for approving surveillance technologies under the ordinance.[415] This is a serious concern, especially in the absence of any administrative infrastructure of the kind we take for granted when Congress delegates rulemaking, programmatic design, and ongoing supervisory duties to federal agencies. Federal agencies rely on institutional, organizational, and doctrinal mechanisms to produce, review, and approve a high volume of rules, licenses, permits, and so on. Without these mechanisms, the SPD, the Seattle IT department and CPOs office, and the Seattle City Council and its staff may be overwhelmed by the amount of work required to review and approve a high volume of SIRs and PIAs. If the burden of surveillance approvals turns out to be too great, one obvious solution for the city council is to establish an ongoing and well-funded surveillance advisory board. This board would evaluate SIRs and issue non-binding recommendations to the city council, which would retain its role as final approver.[416] Similarly, the mayor's office might benefit from standing up an ongoing multi-stakeholder process to develop best practice guidelines governing city use of non-surveillance technologies, thereby reducing the burden on the CPO to conduct one-off PIAs.[417]

Undue burden. – Second, during the hearings on the revised surveillance ordinance, the SPD raised concerns that by extending the ordinance beyond surveillance technology to encompass surveillance data as well, the city might jeopardize regional partnerships for combatting gang activity and gun violence programs. According to Brian Maxie, the Chief Technology Officer of the SPD, these regional programs depend on data sharing arrangements with other local governments. However, the new ordinance requires that SIRs address "what restrictions, if any, the department will place upon the receiving non-City entity's use of [approved] surveillance technologies" and that "[w]hen providing access to the City's surveillance technology by contract with a non-City entity, the City shall require that such entity be bound by any restrictions specified in the Surveillance Impact Report … with regard to such surveillance technology. The City department providing such access shall have written procedures in place for determining how the department will ensure the receiving

[413] Citron

[414]

[415] [Cite videotape of hearings on June 28 and July 26]

[416] *See* Renan, *supra* note , at discussing the role of the PCLOB.

[417] *Id.* discussing the role of the NTIA

non-City entity's compliance with any restrictions identified in the SIR."[418] As Maxie pointed out, this might be fine for Seattle but other Washington cities are likely to object to any required limitations on how they use surveillance technology or data acquired from Seattle and he worried that these provisions might turn Seattle into a "data island."[419] On the other hand, exempting these data sharing arrangements from transparency and accountability carries its own dangers.

Legal vs. technological instruments. –As Colin Bennett and Charles Raab have observed, there are various policy instruments available to organizations for governing privacy.[420] These include both legal instruments (ranging from self-regulatory principles to laws imposing specific obligations and prohibitions) and technological instruments including "privacy by design" (i.e., cities imposing design requirements on vendors or only purchasing technology with certain privacy protective features).[421] Seattle and NYC have relied almost exclusively on legal instruments to regulate technology deployments and data collection, use and disclosure within their local government and have largely done without technological instruments. Arguably, technological instruments, when designed to ensure required privacy outcomes, have an inherent efficiency that helps lighten the burden of detailed SIRs or PIAs. For example, suppose that Seattle or NYC decides to reduce and control downtown traffic through congestion pricing, using an electronic toll collection (ETC) systems. There are two ways to think about ETCs. The first is to design an ETC that relies solely on collection, use, and retention policies to minimize privacy risks. This approach places a lot of burden on the city on the CPO to carry out an extensive PIA and provide ongoing oversight of the ETC to ensure that it complies with all applicable restrictions. The second is to design a privacy-preserving pay-as-you drive system that uses so called "zero knowledge" techniques to take private user information as input (e.g., the driver's identity and payment credentials) without revealing such information to the city.[422] The point is that technological instruments that guarantee certain privacy-preserving outcomes may obviate the need for SIRs or PIAs or at least make the less burdensome.

Chicago's "Array of Things" (AoT) project illustrates how the privacy by design approach achieves regulatory goals using technological instruments. The Chicago AoT is an urban sensing project consisting in "a network of interactive, modular sensor boxes that will be installed around Chicago to collect real-time data on the city's environment, infrastructure, and activity for research and public use." The goal of the project is to measure factors that impact livability in Chicago such as climate, air quality and noise. While the project relies to a certain extent on legal instruments such as a privacy policy and an oversight board, it also relies on technological instruments "to specifically avoid any potential collection of data about individuals," thereby building privacy protection into "the design of the sensors and into the operating policies."[423] By designing the AoT so that it limits or avoids the collection of personal data and deletes data that may raise privacy concerns, this project ensures privacy-protective outcomes in a highly efficient and effective manner.[424] Seattle and

[418] SMC Section 14.18.040(B)(3)(f)
[419] Cite July 26 hearing
[420] COLIN BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY 117-204 (2006).
[421] For an overview of privacy by design, *see* Ira Rubinstein, *Regulating Privacy by Design*, 26 BERK. TECH. L. J.1409 (2012).
[422] For a discussion of a privacy-preserving pay-as-you drive systems, *see* Claudia Diaz, Omer Tene, & Seda Gurses, *Hero or villain: The data controller in privacy law and technologies*, 74 OHIO ST. L. J. 923, 944-46 (2013).

[423] https://arrayofthings.github.io/
[424] "To that end, each sensor that has a potential impact on privacy is operated with specific safeguards in place. The sound sensor will only collect data on ambient volume (the level of noise at the node) and will neither record nor transmit the raw microphone data. A low-resolution infrared camera will be included in each node, pointed at the road surface and sidewalk, with the sole purpose of measuring surface temperature. An imaging camera will be included in each node to detect features such as standing water, weather conditions, and sky color (an indicator of pollution), or to

NYC might achieve similar efficiencies by adopting a privacy by design approach in addition to their use of standard legal instruments.

B. The Public Surveillance Gap

1. Privacy in Public

Privacy theory has long recognized the tension between the surveillance of pedestrians on public streets and the anonymity of public places as symbolized by city streets. In his early and influential analysis of the function of privacy in a democratic society, Alan Westin identified anonymity as "a state of individual privacy" that "occurs when the individual is in public places or performing public acts, but still seeks, and finds, freedom from identification and surveillance."[425] Westin continued:

He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but … he does not expect to be identified and held to the full rules of behavior and role that would operate if he were known to those observing him … . Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.[426]

In his book on government surveillance, *Privacy at Risk,* Christopher Slobogin offers perhaps the most detailed analysis to date of what he calls "a right to public anonymity."[427] Slobogin defines this right as an assurance that when in public, one is "presumptively nameless …as far as the government is concerned." His primary concern is to establish a Fourth Amendment basis for "privacy in public."[428] More specifically, he seeks to build a case for applying the reasonable expectation of privacy test to closed-circuit television ("CCTV") operated by the government in public spaces, notwithstanding the Supreme Court's holding in the so-called flyover and beeper cases (discussed below). Slobogin's analysis draws on Michel Foucault's study of the role of prisons in establishing modern techniques of social discipline. Foucault famously reinterpreted Bentham's Panopticon (a prison facility designed to allow a single watchman to observe all inmates without their knowing whether they are under observation) as a metaphor for self-imposed discipline or normalization. More precisely, Foucault argues that ordinary individuals in modern society know they are subject to constant observation and therefore internalize the norms of their observers and conform their behavior without any need for threats of punishment. Surveillance in this panoptic sense has a stultifying effect on the freedom of activity we associate with public anonymity, leading to "conformity and an oppressive society." And panoptic surveillance is clearly inconsistent with cherished American values of individualism, independence, and self-confidence. In short, the

---

count the number of pedestrians and various types of vehicles on public streets. All images will be processed into numerical data within the node, after which image data will be immediately deleted. After initial calibration, no images or video will be stored within or transmitted from the nodes". *Id.*

[425] ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967) (identifying four states of privacy: solitude, intimacy, anonymity, and reserve).

[426] *Id.*

[427] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 79-117 (2007).

[428] Other scholars contributing to this analysis include HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010); Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643 (2013) (arguing that Nissenbaum's theory of contextual integrity should be applied to Fourth Amendment analysis); Joel R. Reidenberg, *Privacy in Public*, 69 UNIV. MIAMI L. REV. 141 (2014).

panoptic analogy supports a generalized argument in favor of revising Fourth Amendment doctrine so that it supports a right to public anonymity. But as Slobogin rightly concludes, the Supreme Court's case law construing "privacy in public" leaves little room for the necessary revisions.[429]

2. The Fourth Amendment

The Fourth Amendment governs the protection of people against searches and seizures by government officials.[430] In analyzing the Fourth Amendment, the Supreme Court typically applies a two-part test: Is the Fourth Amendment applicable (was there a "search" or "seizure") and if so was the search or seizure "reasonable."[431] Over the years, the test for the threshold question has evolved from one based on physical trespass to the "reasonable expectation of privacy" test first introduced in Justice Harlan's famous concurrence in *Katz v. Unites States.*[432] While *Katz* is best known for Justice Harlan's new test, Justice Stewart's majority opinion includes some much-cited language that bears directly on the Court's later analysis of public surveillance. Recognizing the "vital role" of public telephones in modern communications, Justice Stewart asserts that the Fourth Amendment "protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[433]

In later cases, neither the reasonable expectation of privacy test nor the "knowing exposure" language in the majority opinion have proven very helpful in protecting citizens against government surveillance in public settings. The black letter law makes this abundantly clear. Over the years, the Court has consistently held that there is no reasonable expectation of privacy in anything seen or heard from a public vantage point.[434] In several cases involving marijuana plants, the Court extended this doctrine to open fields, even if they are secluded and the owner takes steps to shield them from public view,[435] and to naked-eye aerial observation of a person's backyard[436] or a greenhouse with partially open sides and roof.[437] 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 publics" might require a warrant.[438] It is hardly surprising that commentators have

---

[429] Slobogin also offers constitutional arguments based on the First Amendment, due process rights to movement and repose, and decisional privacy, SLOBOGIN, *supra* note at 98-106, although he ultimately hangs his hat on revising Fourth Amendment doctrine based on his empirical findings about public attitudes towards CCTV cameras, *id.* at 108-16.

[430] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" U.S. Constitution amend. IV.

[431] Generally speaking, a search supported by probable cause is considered reasonable.

[432] 389 U.S. 347 (1967)(the two-part test asks whether (1) a person has "exhibited an actual (subjective) expectation of privacy and, (2) whether the expectation is "one that society is prepared to recognize as 'reasonable'").

[433] *Id.* at 351.

[434] Harris v United States, 390 U.S. 234, 236 (1968) (announcing the "plain view" doctrine).

[435] Olivier v United States, 466 U.S. 170 (1984) ((announcing the "open fields" doctrine).

[436] California v Ciralo, 476 U.S. 207 (1986) (police flew over defendant's house at an altitude of 1,000 feet, and readily identified marijuana plants growing in the yard and on this basis obtained a search warrant).

[437] Florida v Riley, 488 U.S. 445.

[438] Dow Chemical Co. v United States, 476 U.S. 227, __ (declining to apply this exception a high precision mapping camera costing $22,000 that successfully captured not just the basic sizes, shapes, outlines, and colors of the objects observable from altitudes of 1,200 feet and above but "vivid images of Dow's plant which EPA could later analyze under enlarged and magnified conditions").

ridiculed this exception as unworkable given the rapid pace at which even the most sophisticated technology becomes readily available.[439] A final set of "beeper" cases involved the police using a radio transmitter to follow a car holding chemicals used in drug manufacturing. In *United States v. Knotts*, the Court held that the Fourth Amendment did not apply to a beeper placed in a container of such chemicals because a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[440] A year later, the Court distinguished *Knotts* in a similar case involving the installation of a beeper in a can of ether and the monitoring of its location as it moved back and forth among private dwellings and storage lockers.[441] The use of a device that reveals a "critical fact about the interior of the premises" constitutes a search and therefore requires a warrant.[442]

These cases amount to little or no Fourth Amendment protection when the police use surveillance technology to monitor public spaces. Thus, police use of video cameras, ALPRs, shot detectors, drones, and facial recognition software—in other words, all the components of NYPD's DAS—do not constitute a search under the plain view or open fields doctrines and the beeper cases. Public surveillance receives somewhat more protective treatment under *United States v Jones*, a 2012 case in which the police, acting without a valid warrant, attached a Global Position System (GPS) tracking device to the underside of a drug suspect's car and tracked his movement over a period of 28 days.[443] In a majority opinion authored by Justice Scalia, the Court applied a trespass theory in finding that the government's physical installation of the device constituted a "search" under the Fourth Amendment.[444] However, five Justices in two separate concurrences rejected the 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 expectations of privacy under the *Katz* test. Justice Alito (joined by Justices Ginsburg, Breyer and Kagan) made this point rather bluntly, contending that the majority's reasoning "largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking)."[445] Similarly, Justice Sotomayor in her separate concurrence, noted 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."[446]

Jones signals that five Justices of the Supreme Court now believe that new surveillance technologies must be confronted head on if the Fourth Amendment is to maintain its vitality in the contemporary

---

[439] *See* Slobogin, *supra* at 54-62.
[440] United States v. Knotts, 460 U.S. 276, 281(1983) (emphasizing that travel over public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.".
[441] United States v. Karo, 468 U.S. 705, 715 (1984).
[442] Karo, 468 U.S. at 715. Similarly, in Kyllo v. Unites States, 533 U.S. 27 (2001), the Court reached a similar conclusion about the use of a thermal imaging device to explore details of the home that previously would have been inaccessible without physical invasion and concluded that the device was not in general public use).
[443] 565 U.S. 400.
[444] United States v. Jones, 565 U.S. 400, 409 (2012) (as Justice Scalia noted in defending his approach, "The *Katz* reasonable-expectation-of-privacy test has been *added* to, but *not substituted for*, the common-law trespassory test" (emphasis in the original).
[445] Jones, 565 U.S. at 424.
[446] Jones, 565 U.S. 415.

setting,[447] and that pervasive surveillance may violate society's reasonable expectations of privacy, even in cases where the surveillance occurs in public places.[448] And yet, it is not at all clear that *Jones, Riley*, or *Carpenter* will alter the Court's treatment of video cameras and the related public surveillance technologies associated with the DAS. The GPS tracking at issue in *Jones* consisted in long-term monitoring of a single known target. In sharp contrast, 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 office reviews and evaluates it in the larger context of the DAS including other sensor feeds and all records geocoded in the vicinity of the alarming sensor. This step prevents the police from deploying resources if the alarm is a false-positive.[449] Finally, if the officer judges the alarm to be legitimate, a police response follows. Thus, the DAS bears little resemblance to GPS tracking, at least in terms of extended monitoring.

Of course, one can imagine scenarios in which the universal monitoring of the DAS begins to look like the extended monitoring of a particular suspect using GPS tracking. But important differences remain. Imagine a scenario where the DAS issues an alert for a suspicious package left behind at Grand Central Terminal. It is not a false positive. Officers respond and discover a bomb, which the bomb squad disarms. Meanwhile, a NYPD analyst reviews the surveillance feeds, identities the person who left the package behind, captures his facial image, matches it to video footage from other cameras in the vicinity, searches a national database of driver license photos for a matching facial image, searches a watch list for suspected terrorists and their known aliases, finds useful matches, identifies vehicles owned or rented by the bomb suspect under different aliases, and issues a tri-state alert for these vehicles. Two hours after the DAS generated the alert, an ALPR mounted on the Henry Hudson Bridge in northern Manhattan records a hit, which ultimately leads to the suspect's arrest.[450] In short, the DAS enabled the analyst to reconstruct the suspect's movements across the city by foot and by car over a short period of time. Thus, the DAS' monitoring capabilities are wide, but not very deep.[451] And unlike the 24x7x4 GPS monitoring at issue in *Jones,* the DAS does not generate "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual

---

[447] *See also* Riley v. California, 134 S. Ct. 2473 (2014) (holding 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 due in part to their immense storage capacity).

[448] In a new case that the Court will hear during the current term, the Court must decide whether the Fourth Amendment permits the government, acting without a warrant, to obtain access to historical cell phone data to determine the location of a suspect over a four-month period. *See* Carpenter v. United States*,* 819 F.3d 880, 885-86 (2016), *cert granted*, U.S. LEXIS 3686 (U.S., June 5, 2017. *Carpenter* may be the "test case" that forces the Court to modify or abandon the third-party doctrine in light of the difference between the status of dialed phone numbers at issue in Smith v. Maryland, 442 U.S. 735 (1979) and the near constant exchange of location information that occurs with the use of digital cellphones. *See* Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward* WILLIAM & MARY BILL OF RIGHTS, (forthcoming, 2018) (arguing that *Carpenter* is a test case because it squarely presents how the twentieth-century third party doctrine will fare in contemporary times).

[449] Levine, at 75.

[450] *Id*

[451] Kiel Brennan-Marquez helped me formulate this distinction. Renan, *supra* note at 1058, makes a similar point, noting that "the context of *Jones*—a particular search against a specific suspect—obscures additional aggregation problems that programmatic surveillance poses."

associations." The absence of long-term monitoring seems like enough of a distinguishing factor for the Court to adhere to its reasoning in *Katz, Ciralo, Dow Chemical, and Knotts*, rather than apply *Jones* to the DAS or its component parts.[452]

3. ECPA

Federal privacy laws generally do not cover video surveillance in public spaces by federal or state law enforcement officers. Congress deliberately omitted video surveillance from the scope of the Wiretap Act, which otherwise covers government interception of "wire" and "oral" communications.[453] And this omission was not reversed when Congress enacted ECPA, which extended the Wiretap Act to "electronic communications."[454]

The Wiretap Act defines a "wire communication" in terms of "aural transfers" (i.e., a communication containing the human voice) that travels through a wire, a cable, or a similar medium.[455] "Oral communications" differ from "aural transfers" because they are intercepted through bugs and other recording or transmitting devices that capture words uttered by a person exhibiting an expectation of privacy.[456] "Electronic communications" is a catch-all term for everything other than wire or oral communications (such as email).[457] But none of these definitions cover video surveillance (with two minor exception discussed below). 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.[458]

The two exceptions are (1) if the video surveillance includes sound, which brings it within the definition of "oral communications" under the Wiretap Act; and (2) "if the government intercepts a communication consisting of video images (such as a transmission of a webcam image or an e-mail containing a video clip), then the Wiretap Act applies."[459] Neither exception applies to a system like the DAS. The norm for CCTV cameras and ALPRs is silent video surveillance 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).[460] As to the second scenario, case law establishes that an "interception" under the Wiretap Act must be contemporaneous with the

---

[452] For an alternative view of the Fourth Amendment implications of surveillance in the public space, *see* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public,* 66 EMORY L. J. 527 (2017) (explaining a six-factor test based on *Jones* and concluding that while public video surveillance does not constitute a search, a networked tracking of individuals would be a search due to its duration and potential for combination with other technologies).

[453] *See* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE, 2nd ed., § 6.2.1.A.2 (20156-17) (citing S. REP. NO. 99-541, at 16-17 *reprinted in* U.S.C.C.A.N. 3555, 3570-71); *see also* United States v. Koyomejian, 970 F.2d 536, 539-40 (9th Cir. 1992).

[454] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW, 5th ed., 383 (2015).

[455] 18 U.S.C. § 2510(1).

[456] 18 U.S.C. § 2510(2).

[457] 18 U.S.C. § 2510(12).

[458] 18 U.S.C. § 2510(4).

[459] SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note __, at 383.

[460] 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 (2016) ().

communication.[461] But the NYPD does not intercept or capture communications consisting of video images in real-time—rather, it operates a data center that stores these images on its own servers and allows authorized personnel to process and access them as appropriate. Nor do the SCA or PRA apply to the second scenario. The SCA has no application because it authorizes access "by the person or entity providing a wire or electronic communications service" (in this case, the NYPD).[462] Furthermore, the operative provisions of the SCA only apply to services provided to the public.[463] But police networks like the DAS offer no services to the public. They are private networks and restricted exclusively to NYPD personnel. The PRA does not apply because it covers "dialing, routing, addressing, or signaling" information, none of which is at issue with video surveillance.[464] And much the same analysis would apply to the other components of the DAS. In short, ECPA does not apply to public surveillance systems like the DAS or to its main components.

4. Closing the Gap

The dozen or so local surveillance ordinances adopted or proposed in Seattle, New York, and other cities across the country have begun to close the public surveillance gap by developing a transparency and accountability mechanism for surveillance technology free of Fourth Amendment doctrinal constraints. These mechanisms apply even when the government uses these technologies in scenarios involving plain view, open fields, or beepers or other devices for tracking suspects on public roads. 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, allowing elected officials or the public to determine whether it is appropriate for a city to acquire and use such technology based on a range of operational and data management factors as detailed above.[465] 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 camera policy. It also excludes cameras installed for a single purpose—such as solely to record traffic violations, solely for security purposes, or solely to protect the physical integrity of city infrastructure.[466] The POST Act in NYC similarly excludes "cameras installed to monitor and protect the physical integrity of city infrastructure."[467] These exceptions will have to be interpreted and applied, although they seem narrow enough to avoid a blanket exemption for something like the DAS. On the other hand, the Santa Clara County ordinance defines "surveillance technology in

[461] *See, e.g.,* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002).
[462] 18 U.S.C. § 2701(c).
[463] 18 U.S.C. § 2702 and 18 U.S.C. § 2711(2).
[464] 18 U.S.C. § 3127(3).
[465] *See supra* Parts II.A.1 and II.B.1.
[466] *See supra* text accompanying note __.
[467]

extremely broad terms and by the examples it provides, leaves no doubt that it would apply to a system like the DAS:

> Examples of surveillance technology include, but are not limited to, drones with cameras or monitoring capabilities, automated license plate readers, closed-circuit cameras/televisions, cell-site simulators, International Mobile Subscriber Identity (IMSD trackers, Global Positioning System (GPS) technology, radio-frequency identification (RFID) technology, biometrics-identification technology, and facial-recognition technology.[468]

C. *Policing and Democratic Governance*

Much commentary on urban policing and related privacy issues is tale of two competing narratives. One narrative centers on race and crime and the fight for social justice. Thus, it tends to focus on controversial or abusive policing practice.[469] 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, and Paris (to name a few), which have caused tens of thousands of deaths and many billions of dollars of economic losses.[470] This terrorism narrative also involves controversial policing practices ranging 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 JTTFs.[471]

In his recent work on democratic policing, Barry 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.[472] Friedman's argument proceeds in three steps. First, he observes that the broad enabling statutes under which most policing agencies operate authorize them to enforce the substantive criminal law without providing much detail about permissible methods or procedures.[473] As a result, when it comes to policing agencies, the usual administrative governance schemes that apply to most other agencies are almost entirely lacking. To the contrary, most policing occurs without any clear rules or policies in place or, when such rules and policies exist, they are often kept hidden from public view.

---

[468] Santa Clara County Ordinance No. NS-300.897, Section A-40-7(C) (May 24, 2016), http://sccgov.iqm2.com/Citizens/FileOpen.aspx?Type=4&ID=149330&MeetingID=7193.

[469] *See supra* text accompanying note _.

[470] 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) that wreak havoc in their own devastating way.

[471] *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); Robert Muggah, *Is urban terrorism the new normal? Probably*, World Economic Forum, https://www.weforum.org/agenda/2016/01/is-urban-terrorism-is-the-new-normal-probably/.

[472] FRIEDMAN, *supra* note , AT 6-14; *see also* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 101 (2015).

[473] Friedman & Ponomarenko, 118.

Second, as public choice theory predicts, legislative bodies lack incentives to regulate policing.[474] Not only are there powerful special interest groups (e.g., police unions) with a stake in opposing such regulation but the victims of out-of-control policing (typically minorities and the poor) are not usually as well-organized in support of politicians who would stand up to the police. Even when a rash of terrible incidents occurs that energizes this constituency—such as the police shooting of Michael Brown in Ferguson, Missouri and Erle Garner in Staten Island, New York, which led directly to the creation of the Black Lives Matter movement—regulating the police remains a heavy lift.

Finally, Friedman contends that courts have failed to properly supervise policing procedures, mainly because judicial remedies such as the exclusionary rule and damage actions are ineffective.[475] Moreover, judicial review is ill-equipped to deal with the recent shift from reactive and investigative policing, which allowed courts to supervise whether police investigations were justified on the basis of particularized suspicion, to proactive and programmatic policing, which targets larger populations and entire neighborhoods or ethnic groups and subjects them to dragnet forms of surveillance, which has so far resisted effective judicial oversight.[476] Friedman sums up these governance failures as constituting a kind "police exceptionalism" within the Administrative state.[477] He contends that what is urgently needed to overcome police exceptionalism is not more oversight in the form of Inspector Generals, civilian complaint boards, or special monitors resulting from consent decrees but rather "rules: rules that are written *before* officials act, rules that are *public,* rules that are written with *public participation."*[478] "We," says Friedman (and he truly means "we the people" in the sense of our democratic polity) must insist on "transparent democratic processes such as legislative authorization and public rulemaking"[479] as applied to policing.

Friedman's call for democratic policing may strike some as unduly optimistic, but there is little question that recent events have forced police to become more adept at 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 far more common 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,[480] drones,[481] and body cameras.[482] As Friedman concedes, there will be difficult questions around how to scale public rulemaking to communities and police forces of various sizes;[483] however, the availability of model rules from the American Bar Association (ABA), the American

---

474

475 FRIEDMAN, at

476 Friedman & Ponomarenko, 146-49. Slobogin refers to this as panvasive surveillance, *see supra* note , ; Renan refers to it as programmatic surveillance, *see supra* note .

477 Friedman & Ponomarenko, 117.

478 FRIEDMAN, at 20.

479 Friedman & Ponomarenko, 106.

480

481 FRIEDMAN, at 98.

482

483 Friedman & Ponomarenko, 161-62 (noting that there are more than 13,000 U.S. police departments serving both large cities and smaller communities (more than half of these departments serve communities with fewer than 10,000 residents) and a high degree of variance in their size. For example, the median local department has only eight full-time officers, while the New York Police Department (NYPD) has 36,000.

Law Institute (ALI), and the International Association of Chiefs of Police (IACP) should help ease the burden of smaller communities having to draft rules from the ground up.[484] Lastly, Friedman notes that "By virtue of their *closeness* to the citizenry, local government is already adept at fielding input from the community, be it through school boards, zoning boards, arts commissions, or neighborhood councils."[485] 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."[486]

The local surveillance ordinances described in this Article are a nice example of what Friedman has in mind by democratic policing. [why] More broadly, privacy localism perfectly exemplifies the administrative turn in police governance. [expand]

CONCLUSION

[484] Friedman also directs the Policing Project at NYU School of Law, whose activities include "writing model rules and policies for policing, promoting community engagement around policing policies at all levels of government, and helping to develop sound metrics of policing success"). *See* https://policingproject.org/.
[485] Friedman & Ponomarenko, 163 (emphasis added).
[486] FRIEDMAN, at 96.