12-2016

Surveillance Policy Making By Procurement

Catherine Crump
Berkeley Law

SURVEILLANCE POLICY MAKING BY PROCUREMENT

Catherine Crump*

Abstract: In Seattle, the police obtained a surveillance drone with the approval of a city council that did not realize what it was doing. In Oakland, following a council review that lasted literally two minutes, the city created a data integration center that networked together all of its existing surveillance infrastructure. In San Diego, elected representatives were only dimly aware that the law enforcement agency they supervised had built and deployed innovative facial recognition technology.

In an age of heightened concern about the militarization of local police and surveillance technology, how do local law enforcement agencies obtain cutting edge and potentially intrusive surveillance equipment without elected leaders and the general public realizing it? The answer lies in the process of federal procurement, through which the federal government, often in the name of combatting terrorism, funnels billions of dollars to local law enforcement agencies that can then be used to purchase surveillance equipment. But the federal government does not take steps to ensure that local elected representatives and members of the public are involved in decisions about what technologies to acquire, or that anyone develops a protocol to constrain how the technologies are used. Surveillance policy making by procurement thus raises a host of questions about accountability for policy choices when the federal government influences local policing through grants, but does not address all relevant concerns and how to deal with the inevitable spillover effects of the federal government's national security initiatives on the ways local law enforcement agents carry out their more routine policing functions.

This Article is the first to comprehensively consider the intersection of procurement and local surveillance policy making. Using case studies from Seattle, Oakland, and San Diego, it exposes the practice of surveillance policy making by procurement. The case studies highlight the structural and institutional factors that lead to surveillance policy making by procurement, and elected representatives' responses to it point the way towards policy solutions that would bring a greater measure of transparency and accountability to local surveillance policy making. The case studies also provide fodder for thinking through the way federal spending programs can generate confusion over who is responsible for policy

---

*Assistant Clinical Professor of Law, University of California, Berkeley, School of Law. Thanks to Ty Alper, Derek E. Bambauer, Jane Bambauer, Eric Biber, Allie Bohm, Matthew Cagle, Donna Crump, Frank Crump, James X. Dempsey, Malcolm M. Feeley, Susan Freiwald, Barry Friedman, Jared Friend, Mark P. Gergen, Naomi Gilens, Katie Haas, Brian Hofer, Sonia Katyal, Christina Koningisor, Deirdre K. Mulligan, Anne Joseph O'Connell, Pamela Samuelson, Jonathan Simon, Jay Stanley, Kerry Tremain, Molly Shaffer Van Houweling, Charles D. Weisselberg, John Yoo, and Franklin E. Zimring for helpful comments. For excellent research assistance, thanks especially to Max de la Cal, as well as Waqas Akmal, Olivia Layug Balbarin, J. William Binkley, Caleb Braley, Raphaella Friedman, Vanessa Ing, David Schlussel, Monsura Sirajee, and Haejin Song. Thanks also to participants of the Internet Law Works in Progress conference, Berkeley Law Faculty Workshop and Junior Working Ideas Group, and the Clinical Law Review Writers' Workshop for their suggestions. Finally, thanks to the Berkeley Law librarians, and to the staff of the *Washington Law Review* for excellent editorial assistance.

choices and how the federal government's national security policies have spillover effects on the conduct of routine policing.

Local communities vary greatly in their crime rates, the competence and trustworthiness of their police departments, and their political convictions. This Article draws on the case studies to suggest that local governments have a valuable role to play in tailoring surveillance policy to local conditions. It concludes by proposing politically feasible steps to strengthen local democratic input regarding what surveillance technology should be adopted and the conditions under which it should be deployed.

INTRODUCTION

> One day some of us showed up [to] committee and there were some objects on [the] table. It turns out they were drones. We didn't even know we owned drones. We looked at each other [and asked], where did these come from? And then someone said, oh, you approved it two years ago.[1]
>
> —Seattle City Council Member Nick Licata

The heavily militarized response to those protesting the police shooting of Michael Brown in Ferguson, Missouri generated real shock among members of the public, who did not realize that the federal government provided military-grade weapons and equipment to local law enforcement agencies. In the aftermath, the White House conducted a top-to-bottom review of federal support for local law enforcement equipment acquisition.[2] It concluded that "training has not been institutionalized, specifically with respect to civil rights and civil liberties protections[.]"[3] It also found that "[l]ocal elected officials are frequently not involved in the decision-making" about what technology their police forces acquire, and the general public is "unaware of what their [law enforcement agencies] possess."[4]

---

1. Seattle City Council, *Full Council*, SEATTLE CHANNEL, at 1:07:25 (Mar. 18, 2013), http://www.seattlechannel.org/mayor-and-council/city-council/full-council?videoid=x22150 (last visited Dec. 17, 2016) (statement of councilmember Nick Licata).

2. EXEC. OFFICE OF THE PRESIDENT, REVIEW: FEDERAL SUPPORT FOR LOCAL LAW ENFORCEMENT EQUIPMENT ACQUISITION (2014), https://www.whitehouse.gov/sites/default/files/docs/federal_support_for_local_law_enforcement_equipment_acquisition.pdf [http://perma.cc/YCV2-TXN7] (reviewing federal funding and programs that provide equipment to state and local law enforcement agencies); Mark Landler, *Obama Offers New Standards on Police Gear in Wake of Ferguson Protests*, N.Y. TIMES (Dec. 1, 2014), http://www.nytimes.com/2014/12/02/us/politics/obama-to-toughen-standards-on-police-use-of-military-gear.html [https://perma.cc/6HXL-QL7A] (describing administration response to public disapproval of federal programs viewed as promoting militarization of police).

3. EXEC. OFFICE OF THE PRESIDENT, *supra* note 2, at 2.

4. *Id.* at 4.

These statements are equally true of federal programs promoting the acquisition of surveillance equipment. The primary difference is that while the public does eventually witness the use of force, surveillance, by its nature, remains largely invisible. Yet surveillance equipment is also susceptible to abuse. The federal government's role in promoting its use merits close attention. This Article begins that work.

Federal agencies make considerable funds available to local law enforcement agencies, in the form of grants, to acquire surveillance technologies. Congress substantially increased the amount of funding available in response to the 9/11 terrorist attacks, reflecting the view that local cooperation was essential to prevent future incidents of terrorism.[5] Its interest in enhancing the capabilities of local law enforcement agencies is likely to increase because anti-terrorism experts are convinced that Orlando and San Bernardino-style "home-grown" terrorist incidents are now a substantial threat to our security and safety.[6]

By influencing the process of procurement, the federal government can entice local police departments—over which it has no formal control—to enhance their surveillance capabilities in line with federal priorities. But this approach, which this Article refers to as surveillance policy making by procurement, has a variety of additional consequences. For the most part, local law enforcement agencies are directed and controlled by locally elected government officials, who are in turn subject to the pressures of local public opinion. Surveillance policy making by procurement can short-circuit this process when elected officials and the public are left without a meaningful understanding of what technologies their law enforcement agency is acquiring. This can create a governance void, in which law enforcement agencies deploy powerful surveillance technologies in ways that may conflict with local political preferences. Moreover, because the same surveillance technologies that are useful in investigating terrorism are also useful in investigating more routine forms of criminal conduct, federal programs created with the War on Terror in mind can have significant effects on standard law enforcement work.

---

5. *See infra* Part II.

6. According to Matthew G. Olsen, former Director of the National Counterterrorism Center, the Boston Marathon bombing highlighted the "danger posed by lone actors and insular groups not directly tied to terrorist organizations, as well as the difficulty of identifying these types of plots before they take place." *Hearing Before the S. Comm. on Homeland Sec. and Governmental Aff., The Homeland Threat Landscape and U.S. Response*, 113th Cong. 1 (2013) (statement of Matthew G. Olsen, Director, National Counterterrorism Center).

To better understand surveillance policy making by procurement, this Article develops three case studies: Seattle's acquisition of a drone and deployment of a "mesh network"; Oakland's construction of a "domain awareness center"; and San Diego's rollout of facial recognition technology. The technologies that Seattle, Oakland, and San Diego acquired are not marginal improvements on existing tools.[7] All substantially increase the capacity of a law enforcement agency to collect, store, analyze, and share information about individuals, with a potentially significant, negative impact on privacy. Using a drone, a law enforcement agent can conduct aerial surveillance of an area as soon as it becomes of interest. A mesh network—a wireless infrastructure that connects cameras and other devices—has the potential to significantly increase video surveillance of public places and to track anyone carrying a wi-fi-enabled device. Integrating sensor data into a domain awareness center—a hub that integrates surveillance data from cameras and other networked sensors—raises the prospect of substantially expanding the analysis and sharing of data initially collected for different purposes. Facial recognition technology has the potential to allow any officer with a smartphone to snap a photo of another person and ascertain that person's identity, which is key to accessing a wealth of other information, such as criminal history and threat assessment score.

This Article draws on available public information to demonstrate that the phenomenon of surveillance policy making by procurement is widespread and merits attention. It is the first piece of legal scholarship to focus on the impact of federal procurement programs on local surveillance policy making.[8] The Article focuses on salient examples, but the quantity of federal funding available suggests its broader importance.

Part I explains the scope of the federal government's involvement in local law enforcement agencies' procurement of surveillance technology. The Part both documents the billions of dollars of federal funding available to local law enforcement agencies to purchase surveillance technologies and builds on the scholarship of others to demonstrate the already substantial, and likely expanding, interest of the

7. There is wide recognition that digital technology has vastly expanded the capacity for the collection, retention, analysis, and sharing of data. *See, e.g.*, Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1042 ("Technology has made it easier than ever to collect, combine, share, and retain massive amounts of data and to search the resulting datasets.").

8. Taking a broader view, Rachel A. Harmon has addressed the distortions federal funding programs can create in conducting cost-benefit analyses of local policing programs. *See* Rachel A. Harmon, *Federal Programs and the Real Costs of Policing*, 90 N.Y.U. L. REV. 870 (2015).

federal government in enhancing the capabilities of local law enforcement agencies. Part II introduces the three case studies—Seattle, Oakland, and San Diego—that provide more detailed accounts of surveillance policy making by procurement. These case studies demonstrate the structural and institutional factors that contribute to surveillance policy making by procurement as well as its consequences for local governance of police surveillance. The policy changes local elected officials implemented in the three case studies point the way toward reforms that bring local surveillance policy in line with local crime conditions, the competence and trustworthiness of the police department, and local political preferences.

Part III takes a theoretical turn. It identifies factors that should be considered when optimizing surveillance policy. While there is no one-size-fits-all solution to how a surveillance technology should be utilized, every surveillance scheme raises the same basic questions about how data is collected, retained, used, and shared. The absence of a technology use policy that hits these basic points—and especially the failure to draft *any* policy at all—should be cause for concern.

The Part then draws on two bodies of scholarship to explore aspects of accountability for local surveillance policy choices. In the case studies, federal involvement weakened local democratic control over local surveillance policy without offering any replacement. The Supreme Court has privileged federal interventions in the form of conditional grants-in-aid, such as those in the case studies, over federal interventions that commandeer state and local officials precisely because of its view that spending programs do a better job of preserving clear lines of accountability. But the case studies show that federal spending programs can generate considerable confusion over who is responsible for policy choices and provide reason to question the factual basis of the distinction the Court has drawn. Next, the Part situates the case studies within the federal government's broader efforts to work more closely with local law enforcement agencies to prevent, investigate, and respond to acts of terror. Particularly, given the dual-purpose nature of much surveillance technology, these initiatives have significant impacts not just on combatting terrorism but also on how local officers conduct routine policing. This suggests that any cost-benefit analysis of the federal government's national security programs should consider not only their impact on national security, but also their impact on law enforcement, including on transparency and accountability.

Finally, Part IV makes the case that local elected officials' familiarity with local circumstances positions them particularly well to set local surveillance policy. It sets out some policy proposals for enhancing local

input over surveillance choices and ensuring that the use of surveillance technology is governed by policies that take into account bedrock data management principles. This menu of reform options includes actions at the federal, state, and local levels. These actions would bring an increased measure of local democratic decision making to local surveillance policy.

I. FEDERAL FUNDING OF LOCAL SURVEILLANCE

In her scholarship on policing and its regulation, Rachel Harmon has observed that federal support for local law enforcement in the form of money, equipment, personnel, and power "is far more extensive than its civil rights enforcement and has an enormous and understudied impact on policing."[9] The response to the events of 9/11 extended this support even further. As national security scholar Matthew Waxman explained, "[o]nce a major component of the national security threat was seen as residing or operating within U.S. borders, local police agencies were an obvious resource for the federal government to turn to given the vastness of the intelligence challenge."[10]

After 9/11, the federal government established or expanded a number of programs to provide equipment and training to help state and local law enforcement agencies.[11] A quick tally of just the most major federal programs indicates that they have made tens of billions of dollars

9. *Id.* at 872.

10. Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289, 305 (2012); *see also* JEROME P. BJELOPERA & KRISTIN FINKLEA, CONG. RESEARCH SERV., DOMESTIC FEDERAL LAW ENFORCEMENT COOPERATION: THROUGH THE LENS OF THE SOUTHWEST BORDER 16 (2014), https://www.fas.org/sgp/crs/homesec/R43583.pdf [http://perma.cc/G5QU-WVM2] (identifying "a broad recognition that state and local law enforcement and public safety agencies play significant roles in homeland security—especially stopping terrorist plots."). For example, the federal government significantly expanded the number of joint terrorism taskforces around the country. Of the 104 such taskforces that bring together federal and local law enforcement personnel to investigate terrorism, 71 were created after September 11, 2001. *See Joint Terrorism Task Forces*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/terrorism [https://perma.cc/5MGD-NUZS]. Also, the federal government has funded the establishment of a network of information fusion centers to serve as "focal points for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial [] and private sector partners." *State and Major Urban Area Fusion Centers*, DEP'T OF HOMELAND SEC. (June 16, 2016), http://www.dhs.gov/state-and-major-urban-area-fusion-centers [https://perma.cc/J6TV-2FHL].

11. EXEC. OFFICE OF THE PRESIDENT, *supra* note 2, at 2 ("Particularly in the years since September 11, 2001, Congress and the Executive Branch have steadily increased spending and support for [equipment for state and local law enforcement agencies], in light of legitimate concerns about the growing threat of terrorism, shrinking local budgets, and the relative ease with which some criminals are able to obtain high-powered weapons.").

available for this purpose. It is challenging to understand the impact of this funding on local surveillance practices because few programs collect statistics on how funding is distributed across categories of equipment (e.g., surveillance, weaponry) and training. However, the sheer quantity of money suggests these programs' importance.

The United States Department of Homeland Security (DHS) administers a substantial number of programs that give grants to law enforcement agencies:

The State Homeland Security Program (SHSP) provides support to state governments and agencies for planning, organizing, equipping, training, and exercising capabilities and procedures to "prevent, protect against, mitigate, respond to, and recover from" terrorist and other threats.[12] Between fiscal years 2003 and 2014, the program awarded $9.9 billion in grant funds.[13]

The Urban Areas Security Initiative has similar goals to the SHSP, but focuses on the needs of "high-threat, high-density Urban Areas[.]"[14] Between fiscal years 2003 and 2014, the program awarded $8.4 billion in grant funds.[15]

The Port Security Grant Program, available to 360 ports, has distributed nearly $2.9 billion since its inception in January 2002.[16]

Operation Stonegarden, dedicated to border security,[17] has disbursed $361 million between 2008 and 2014.[18]

In addition to DHS programs, the Department of Justice (DOJ) also administers grants to state and local governments. For example, its Justice Assistance Grant (JAG) program is the biggest source of federal

12. U.S. DEP'T OF HOMELAND SEC.: FED. EMERGENCY MGMT. AGENCY, HOMELAND SECURITY GRANT PROGRAM 4 (2014), http://www.fema.gov/media-library-data/1395161200285-5b07ed0456056217175fbdee28d2b06e/FY_2014_HSGP_FOA_Final.pdf [https://perma.cc/G6FL-MYM8] [hereinafter HSGP FOA].

13. Catherine Crump, *Statistical Compendium*, http://scholarship.law.berkeley.edu/facpubs/2633/ [perma.cc/AE42-HXYK].

14. HSGP FOA, *supra* note 12, at 4.

15. Crump, *supra* note 13.

16. *See id.* (outlining calculations and sources underlying figure).

17. HSGP FOA, *supra* note 12, at 4.

18. Crump, *supra* note 13.

justice funding to state and local jurisdictions.[19] The program granted a total of nearly $3.8 billion between 2003 and 2014.[20]

How are state and local law enforcement agencies using these funds for surveillance? Again, information is incomplete, but accounts of the JAG program, one of the few that releases information on equipment purchased with its grants, indicated that in the 2012 program year, 113 state and local governments used JAG funds to purchase license plate readers, 371 purchased video observation equipment, 284 purchased undercover surveillance equipment, and 619 purchased on-car or body-worn cameras.[21]

Lists of equipment eligible for purchase under various grants offer additional clues about how federal money is spent. The DHS federally authorized equipment list, which sets out what local law enforcement agencies are authorized to purchase under a broad range of grant programs, includes a wide array of "[s]urveillance equipment and related accessories," including audio, data, and visual equipment.[22] It specifically mentions: (1) equipment for surveillance of telephone communications; (2) devices to extract data from cell phones; (3) cameras; and (4) infrared illumination equipment.[23]

As mentioned previously, although the federal government has provided incentives for the expanded use of surveillance equipment by local law enforcement agencies, it has not offered any systematic guidance on the appropriate uses of this technology, and federal programs generally have not required that local elected officials decide on surveillance technology acquisitions.[24] For example, in the case studies that follow, localities obtained funds from two DHS programs, the Urban Areas Security Initiative and the Port Security Grant Program,

---

19. U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE ASSISTANCE, EDWARD BYRNE JUSTICE ASSISTANCE GRANT (JAG) PROGRAM FACT SHEET (2016),

https://www.bja.gov/Publications/JAG_Fact_Sheet.pdf [https://perma.cc/L3RJ-BYH7].

20. Crump, *supra* note 13. In addition to the DHS and DOJ, the U.S. Department of Defense also works to disseminate surveillance equipment to state and local law enforcement agencies. For example, as of December 2014 there were 44,275 of its night vision goggles in the possession of local law enforcement agencies. *See* EXEC. OFFICE OF THE PRESIDENT, *supra* note 2, at 8.

21. U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE ASSISTANCE, GRANT ACTIVITY REPORT, JUSTICE ASSISTANCE GRANT (JAG) PROGRAM (APRIL 2012 – MARCH 2013) 4 (2013), https://www.bja.gov/Publications/JAG_LE_Grant_Activity_03-13.pdf [https://perma.cc/ZM4E-BS2B].

22. U.S. DEP'T OF HOMELAND SEC.: FED. EMERGENCY MGMT. AGENCY, DHS AUTHORIZED EQUIPMENT LIST 121 (2012), http://www.fema.gov/media-library-data/20130726-1825-25045-7138/fema_preparedness_grants_authorized_equipment_list.pdf [https://perma.cc/JT27-FFF5].

23. *Id.*

24. *See supra* Introduction.

and one DOJ grant program, designed to facilitate information-led policing.[25] None of the statutes or regulations governing these programs require the involvement of local elected officials.[26]

II. MUNICIPAL SURVEILLANCE TECHNOLOGY ACQUISITION: THREE CASE STUDIES

This Part develops a detailed account of surveillance policy making by procurement through the examination of three case studies: Seattle's acquisition of a drone and construction of a mesh network, Oakland's construction of a domain awareness center, and San Diego's development of facial recognition technology. The case studies suggest some of the structural and institutional factors that lead local police departments to acquire surveillance technologies without participation by elected representatives or the general public. The policy solutions local elected representatives have devised also serve as a starting point for consideration of how to bring a greater measure of local control, transparency, and accountability to local surveillance policy. Moreover, the case studies provide concrete illustrations of how federal spending programs can generate considerable confusion over who is responsible for policy choices and how federal programs with the purpose of enhancing national security can have their biggest impact on more routine policing practices.

A word about case selection is advisable. The case studies of Seattle, Oakland, and San Diego were chosen because a substantial amount of information is available about them, which is not often true when the topic under consideration is surveillance technology acquisition. In each case, a media entity or a non-profit organization uncovered an instance

---

25. *See infra* section II.A (describing Seattle's receipt of funding from the Urban Areas Security Initiative and Port Security Grant Program); section II.B (describing Oakland's receipt of funding from the Port Security Grant Program); section II.C (describing San Diego's receipt of funding from an information-led policing grant).

26. Urban Areas Security Initiative, 6 U.S.C. § 604 (2012); 46 U.S.C. § 70107 (2012) (statute governing port security grants); 2 C.F.R. §§ 200.318–200.326 (regulations applicable to procurement by non-federal entities that are not states). *See also* Memorandum from Bryan E. Kamoie, Assistant Adm'r for Grant Programs, Fed. Emergency Mgmt. Agency, to All State Administrative Agency Head et al. (Dec. 23, 2014), https://www.fema.gov/media-library-data/1419366341862-296dd0cc30bbf64a6b45581afe9d8b17/InformationBulletin400 2CFRPart200 _FINAL.pdf [http://perma.cc/SJS2-ZAAX] (stating that the Urban Areas Security Initiative and Port Security Grant Program are governed by the regulations contained at 2 C.F.R. § 200); Letter from Michael L. Alston, Dir., Office for Civil Rights, to Pamela Scanlon, Doctor, Automated Reg'l Justice Info. Sys., 1 (Sept. 13, 2007), https://www.eff.org/files/2013/11/07/01_-_tacids_award Z_letter_2.pdf [http://perma.cc/9PVX-DUSL] (describing the sources of authority supporting the grant funds).

where a law enforcement agency acquired a surveillance technology without consulting members of the public or elected representatives. And in each case, consistent media coverage, the availability of public records, or a combination of the two meant there was adequate information to examine how members of the public and elected representatives responded.

Given this selection methodology, the case studies cannot be used to draw causal inferences regarding surveillance policy making by procurement.[27] They are nonetheless adequate to the task of this Article, which is to identify structural and institutional features that characterize policy making by procurement. To the extent that other municipalities have similar features, the case studies suggest that an examination of whether surveillance policy making by procurement is occurring may be warranted.

A. Seattle Acquires a Drone and a Mesh Network

In 2013, the Seattle City Council passed an ordinance, the first of its kind, requiring city agencies to obtain council approval prior to deploying surveillance technology and to accompany such requests for approval with a specific proposal for how data would be collected, retained, used, and shared. This was prompted by a strong, negative public reaction to the police department's secret acquisition of two federally funded surveillance technologies: a surveillance drone[28] and a mesh network.[29] The public response to both technologies was so negative, strongly felt, and sustained that the mayor at the time acceded to the opposition and terminated the programs.[30] This was not the first

---

27. *See generally* GARY KING, ROBERT O. KEOHANE, & SIDNEY VERBA, DESIGNING SOCIAL INQUIRY 56 (1994) (describing as a fundamental goal of descriptive inference "to distinguish the systematic component from the nonsystematic component of the phenomena we study"); *id.* at 75–76 (distinguishing descriptive inference from causal inference).

28. Christine Clarridge, *Waterfront Surveillance Cameras Stir Privacy Fears*, SEATTLE TIMES (Jan. 31, 2013, 8:45 PM) http://seattletimes.com/html/latestnews/2020260670_waterfrontcameras xml.html [https://perma.cc/ZV47-LBML].

29. A wireless mesh network is a wireless network consisting of multiple nodes that relay data. *See, e.g.*, *Mesh Networking*, WIKIPEDIA, https://en.wikipedia.org/wiki/Mesh_networking [https://perma.cc/H2KP-7N5G]. The network was to be spread throughout downtown Seattle, and was to have a variety of functions, including facilitating data transmission from thirty new surveillance cameras. *See* Christine Clarridge, *Protesters Steal the Show at Seattle Police Gathering to Explain Intended Use of Drones*, SEATTLE TIMES (Oct 25, 2012, 10:54 PM), http://www.seattletimes.com/seattle-news/protesters-steal-the-show-at-seattle-police-gathering-to-explain-intended-use-of-drones/ [https://perma.cc/LP6N-JS2Z].

30. *See* Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES (Feb. 7, 2013, 9:33 PM), http://seattletimes.com/html/localnews/2020312864_spddronesxml.html [https://

time the Seattle Police Department's surveillance initiatives became embroiled in controversy. Several years earlier, the police department installed surveillance cameras in public parks, without the consent of the council, by finding an alternate source of funding after the council refused to provide funding.[31] The secretive manner in which the police acquired the surveillance technologies contributed to public opposition and may well have undermined some valuable programs that could have been implemented in a less contentious environment.[32]

1. History of Police Surveillance in Seattle

In 2008, the police department activated three cameras in Seattle's Cal Anderson Park, a sizeable urban park in the city's Capitol Hill neighborhood.[33] The city council had prohibited certain funding sources from being used to finance cameras.[34] But because it did not technically prohibit surveillance cameras in parks, the police department found other funding to install the cameras, and did so, ultimately without informing the city council.[35] It did not take long for members of the public to spot the cameras and start asking questions. When council members realized they had been circumvented, they were upset both with the lack of transparency and the department's failure to address basic data management issues, such as how long video footage would be kept and how it would be used.[36]

---

perma.cc/6XV7-RP3A]; Jon Humbert, *City Leaders Raising Questions About Seattle Surveillance Plan*, KOMO NEWS (Feb. 14. 2013), http://www.komonews.com/news/local/City-leaders-raising-questions-about-Seattle-surveillance-plan-191352151.html [https://perma.cc/VW6F-WRGY].

31. *See* Bob Young, *Surveillance Cameras Installed in Seattle's Cal Anderson Park*, SEATTLE TIMES (Apr. 22, 2008) http://www.seattletimes.com/seattle-news/surveillance-cameras-installed-in-seattles-cal-anderson-park/ [https://perma.cc/2H54-CCS6].

32. *See id.* During this time, tensions between the police and residents were already high. In 2011, the DOJ announced an investigation of the Seattle Police Department. Complaint ¶ 19, United States v. City of Seattle, No. 12-cv-01282-JLR (W.D. Wash. July 27, 2012), https://www.justice.gov/sites/default/files/crt/legacy/2012/07/31/spd_complaint_7-27-12.pdf [http://perma.cc/7A4E-UAFY]. It did so after several widely publicized instances of police officers allegedly using excessive force against individuals, especially minorities and persons with disabilities. *Id.* at ¶ 18. The DOJ found that the police department routinely used excessive force and followed policing practices that could lead to discriminatory policing. Letter from Thomas E. Perex, Assistant Attorney Gen., Civil Rights Div., and Jenny A. Durkan, United States Attorney, W. Dist. of Wash., to Michel McGinn, Mayor, City of Seattle 3 (Dec. 16, 2011), https://www.justice.gov/sites/default/files/crt/legacy/2011/12/16/spd_findletter_12-16-11.pdf [http://perma.cc/9GF4-8ASB].

33. Bob Young, *supra* note 31.

34. *Id.*

35. *Id.*

36. *Id.*

Despite this rocky start, the Seattle city council went along with a proposal to install cameras in three additional parks for a twenty-one-month period to test whether the cameras would have a meaningful impact on crime.[37] After a city auditor concluded that there was no evidence that the cameras had reduced crime, the council ordered them removed.[38]

This experience made city council members particularly skeptical when, a few years later, the police department's acquisition of a drone and a mesh camera network came before them for oversight.

2. The Drone and Mesh Network Controversies

In 2010, the Seattle Police Department acquired a surveillance drone.[39] The drone was essentially a remote-controlled, miniature helicopter that weighed just over two pounds and could remain airborne for about ten minutes while live-streaming footage to law enforcement agents.[40] While it could zoom in on a subject, its magnification was about as powerful as that of a standard point-and-click camera.[41] It was also quite loud, precluding the possibility of surreptitious surveillance.[42]

It is hard to see this particular drone as a civil liberties threat or as a significant benefit to law enforcement. Given its limited range and

---

37. Sharon Pian Chan, *3 More Seattle Parks to Get Security Cameras*, SEATTLE TIMES (June 10, 2008) http://www.seattletimes.com/seattle-news/3-more-seattle-parks-to-get-security-cameras/ [https://perma.cc/97CH-KAXP]. The city spent approximately $406,000 installing the cameras. *Id.* Subsequent budget cuts ultimately made it impossible to maintain the cameras in all but Cal Anderson Park. Lauren Padgett, *Seattle to Take New Look at Cal Anderson Surveillance Cameras*, CAPITOL HILL SEATTLE BLOG (Mar. 10, 2010, 11:11 PM), http://www.capitolhillseattle.com/2010/03/seattle-to-take-new-look-at-cal-anderson-surveillance-cameras/ [https://perma.cc/ZY43-VMNX].

38. *Timetable Set for Cal Anderson Cam Removal: Surveillance Tech to be Redeployed*, CAPITOL HILL SEATTLE BLOG (Sept. 27, 2010, 5:02 PM), http://www.capitolhillseattle.com/2010/09/timetable-set-for-cal-anderson-cam-removal-surveillance-tech-to-be-redeployed/ [https://perma.cc/MT62-5ETA].

39. *See* Lynn Thompson, *Police Apologize for Not Keeping Council in Loop on New Drones*, SEATTLE TIMES (May 2, 2012), http://www.seattletimes.com/seattle-news/police-apologize-for-not-keeping-council-in-loop-on-new-drones/ [https://perma.cc/7RVQ-2T8P]; PUB. SAFETY, CIVIL RIGHTS & TECH. COMM., CITY OF SEATTLE, SEATTLE POLICE DEPARTMENT UNMANNED AERIAL SYSTEMS 3 (2012), http://clerk.seattle.gov/~public/meetingrecords/2012/pscrt20120502_1a.pdf [http://perma.cc/J2DA-WYC6]; Memorandum from John Diaz, Chief, Seattle Police Dep't, to Sally Clark, President, Seattle City Council, and Seattle City Council Comm. on Pub. Safety, Civil Rights & Tech. 1 (May 1, 2012) (on file with author).

40. Thompson, *supra* note 39; CITY OF SEATTLE, *supra* note 39, at 4.

41. *See* CITY OF SEATTLE, *supra* note 39, at 4.

42. *See id.*

capabilities, it has more in common with toy drones currently available commercially for a few hundred dollars than with its military brethren.

The department purchased the drone with some $82,500 of federal money, funds that comprised a small sliver of a 2008 grant from the DHS.[43] The grant came from the Urban Areas Security Initiative, which, as discussed earlier, is devoted to helping high-density, high-threat urban areas prevent and recover from acts of terror.[44] The city council had authorized the police chief to accept about $3.6 million to "provide training for Seattle's first responders to further enhance their ability to respond to, and aid in the recovery from, threats or acts of terrorism."[45] It did not mention acquiring a drone.

City council members found out about the drone in the same way as everyone else: from the media. In January 2012, a San Francisco-based advocacy organization, the Electronic Frontier Foundation (EFF), sued the Federal Aviation Administration (FAA) to obtain records regarding drone flights in the United States.[46] When the FAA disclosed a list of authorized drone users a few months later, the Seattle Police Department was on the list.[47] Media outlets covered the department's acquisition of the drone prominently.[48] The American Civil Liberties Union (ACLU)

---

43. Memorandum from John Diaz, *supra* note 39, at 1; Memorandum from Christa Valles, Council Cent. Staff, Seattle City Council, to Councilmembers, Seattle City Council 1 (Feb. 1, 2013), http://clerk.seattle.gov/~public/meetingrecords/2013/pscrt20130206_3a.pdf [http://perma.cc/2Q8B-UHJT].

44. *Id.*

45. SEATTLE, WASH., ORDINANCE 122886 (2008), http://clerk.seattle.gov/~archives/Ordinances/Ord_122886.pdf [http://perma.cc/J3KM-QUM6] (approving receipt of fiscal year 2008 UASI funds); Memorandum from John Diaz, *supra* note 39, at 1 (stating that drones were purchased with funds authorized pursuant to Ordinance 122886).

46. *See* Jennifer Lynch, *Are Drones Watching You?*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you [http://perma.cc/RJP3-MD2F]. Lynch filed many of the public records act requests discussed in this Article, demonstrating the ability of one person making good strategic use of open records laws to bring meaningful increased transparency to a policy arena.

47. *See* Jennifer Lynch, *FAA Releases Lists of Drone Certificates—Many Questions Left Unanswered*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Apr. 19, 2012), https://www.eff.org/deeplinks/2012/04/faa-releases-its-list-drone-certificates-leaves-many-questions-unanswered [http://perma.cc/YVC5-DHUD]; FAA LIST OF CERTIFICATES OF AUTHORIZATIONS (COAS), ELEC. FRONTIER FOUND., https://www.eff.org/files/filenode/20120416_faa_drones_coa_0.pdf [http://perma.cc/8V9S-8P52].

48. *See, e.g.*, Christine Clarridge, *Eye-in-Sky SPD Drones Stir Privacy Concerns*, SEATTLE TIMES (Apr. 20, 2012, 10:05 PM), http://www.seattletimes.com/seattle-news/eye-in-sky-spd-drones-stir-privacy-concerns/ [http://perma.cc/699P-NHNM]; Somini Sengupta, *Lawmakers Set Limits on Police in Using Drones*, N.Y. TIMES, Feb. 16, 2013, at A1. Interestingly, this was not the first time the media had covered acquisition of the drones, but prior stories appear to have gone unnoticed. According to the city council testimony of Assistant Chief Paul McDonagh, the police department

of Washington did not condemn acquisition of the drone, but did call for regulations for its use.[49] Seattle's leading newspaper called for "formal oversight" of the drone to prevent encroachments on civil liberties.[50]

The Seattle Police Department defended its acquisition of the drone.[51] The police chief downplayed any policy implications, describing the drone as "merely an expansion of the daily task of patrol officers to collect all information necessary to safely and effectively respond to calls for service and accomplish law enforcement goals."[52] The police chief agreed to develop a policy for permissible uses for the drone, but made no mention of running the policy by the city council.[53]

Some city council members expressed exasperation that they had not been told about the drone in advance.[54] They were also frustrated by the police department's failure to identify a role for the city council in approving a use policy, which prompted one council member to suggest that police "have more of a dialogue with the council, because we are the ones that . . . approve funding decisions and we want to make sure . . . that you are hearing everything that we hear as well."[55] This was a reminder that the city council controls the police department's overall budget and can choose to approve or disapprove purchases on an item-by-item basis. It was also an implicit suggestion that it would be

---

had done two pieces on the drones about a year prior. Seattle City Council, *Public Safety, Civil Rights and Technology Committee*, SEATTLE CHANNEL, at 38:55 (May 2, 2012) http://www.seattlechannel.org/mayor-and-council/city-council/20122013-public-safety-civil-rights-and-technology-committee/?videoid=x23397 (last visited Dec. 17, 2016) (statement of Assistant Chief Paul McDonagh); *see, e.g.*, Johnathon Fitzpatrick, *Did You Know Seattle Police Have a Flying Surveillance Drone?*, SEATTLE WKLY. (Mar. 6, 2012), http://www.seattleweekly.com/home/936836-129/technology [https://perma.cc/6SQ6-TZ46] (one of the earlier stories on the drones).

49. Clarridge, *supra* note 48.

50. *Aerial Drones Are Law-Enforcement Tools That Need Formal Oversight*, SEATTLE TIMES (May 6, 2012), http://seattletimes.com/html/editorials/2018143433_edit07drone.html [https://perma.cc/95U2-JSJ4].

51. Memorandum from John Diaz, *supra* note 39.

52. *Id.* at 4.

53. *Id.* at 3.

54. Thompson, *supra* note 39. As councilmember Mike O'Brien put it,

> when we have cameras flying around and significant costs and I think to some eyes, is it a toy or is it a useful tool is a question that we're always considering, I think we're in a little bit of a tough place and I think the best thing is to bring us along and to make sure we're working really closely with partners, especially anything with a camera in it to get to a place where we're going to all be comfortable with it.

Seattle City Council, *supra* note 48, at 58:00 (statement of Mike O'Brien, Vice Chair, Public Safety, Civil Rights and Technology Committee).

55. Seattle City Council, *supra* note 48, at 55:00 (statement of Bruce Harrell, Chair, Public Safety, Civil Rights and Technology).

wise for the police department to cooperate with the city council by involving it in key decisions.

The police department mounted a public relations campaign to convince the public of the good the drone would do, but it was too little, too late. The local ACLU affiliate was willing to go along with a regime that involved the regulated use of drones, but others outflanked it by demanding that the police get rid of the drone. When the police hosted an open house to display the drone and answer questions, members of the public hurled insults at them.[56] The police department also invited the public to contribute to a draft policy for the use of drones.[57] After some members of the public asserted that a use policy was inadequate because the police department would be free to amend it at any time,[58] a council member proposed a draft ordinance setting legally binding limits on police use of drones.[59] The city council hearing at which the ordinance was first discussed likewise drew heated public opposition to the idea of using drones at all.[60] In addition, some objected to the process, driven by the availability of federal funds, which led to the drone's acquisition.[61]

---

56. *See* Christine Clarridge, *Police Display Drones They Hope to Deploy*, SEATTLE TIMES (Oct. 24, 2012, 10:29 PM), http://www.seattletimes.com/seattle-news/seattle-police-display-drones-they-hope-to-deploy/ [https://perma.cc/8VS4-SGFX]; Christine Clarridge, *Protesters Steal the Show at Seattle Police Gathering to Explain Intended Use of Drones*, SEATTLE TIMES (Oct 25, 2012, 10:54 PM), http://www.seattletimes.com/seattle-news/protesters-steal-the-show-at-seattle-police-gathering-to-explain-intended-use-of-drones/ [https://perma.cc/LP6N-JS2Z]; Jake Ellison, *Drones Get Really Tiny; New Rules Proposed for Seattle Police*, SEATTLE POST-INTELLIGENCER, (Feb. 6, 2013, 3:48 PM) http://www.seattlepi.com/local/article/Drones-get-really-tiny-Seattle-council-may-make-4250452.php [https://perma.cc/D7HD-C9UW]; Brendan Kiley, *Last Night's Police Drone "Demonstration" Turned into Another Kind of Demonstration*, THE STRANGER: SLOG (Oct. 26, 2012, 10:17 AM), http://slog.thestranger.com/slog/archives/2012/10/26/last-nights-police-drone-demonstration-turned-into-another-kind-of-demonstration [https://perma.cc/A4PC-J5JU].

57. Clarridge, *Protesters Steal the Show at Seattle Police Gathering to Explain Intended Use of Drones*, *supra* note 56.

58. Christine Clarridge, *Use of Police Drones by Seattle Police Strikes a Nerve*, SEATTLE TIMES (Nov. 4, 2012, 6:34 PM), http://www.seattletimes.com/seattle-news/use-of-drones-by-seattle-police-strikes-a-nerve/ [https://perma.cc/8SMN-4DUZ].

59. Jake Ellison, *supra* note 56.

60. Christine Clarridge, *Heated Hearing Airs Distrust over SPD Drones*, SEATTLE TIMES (Feb. 7, 2013, 3:03 PM), http://www.seattletimes.com/seattle-news/heated-hearing-airs-distrust-over-spd-drones/ [https://perma.cc/Z2AW-95EB].

61. As Jennifer Shaw, Deputy Director of the Washington State American Civil Liberties Union (ACLU) put it,

> [w]e really are concerned that our police department has jumped on this bandwagon that other departments across the country have jumped on, which is to follow federal money instead of having the city leaders, the elected officials, and the civilian leaders, be the ones to decide the directions and the use of the technology that comes into the department.

Despite efforts by the police department and some city council members to save the drone, the mayor stepped in and terminated the program. He explained that it had become a distraction from more pressing law enforcement priorities.[62] In 2014, Seattle donated the drone to Los Angeles,[63] where it also provoked such strenuous public opposition that it was never flown.[64]

The drone was one of two surveillance controversies in Seattle that unfolded in quick succession. Around the same time, members of the public began to express dismay over a second issue: the deployment of a mesh network with surveillance cameras in waterfront neighborhoods.[65]

In 2011, the DHS awarded Seattle nearly five million dollars to deploy a mesh network.[66] The funds came from the Port Security Grant Program, which, as the name suggests, works to improve security at vulnerable ports.[67] The network had many potential capabilities. It would allow first responders to communicate even if the cellular telephone network was unavailable or overloaded (a well-known problem that occurred in New York City on 9/11).[68] It would also enable

---

Seattle City Council, *Public Safety, Civil Rights and Technology Committee*, SEATTLE CHANNEL, at 2:20 (Feb. 6, 2012), http://www.seattlechannel.org/mayor-and-council/city-council/20122013-public-safety-civil-rights-and-technology-committee/?videoid=x22317 (last visited Dec. 17, 2016) (statement of Jennifer Shaw, Deputy Director of the Washington state ACLU). The *Seattle Times* editorialized along similar lines, stating that "[i]t was simply bad timing to acquire the drones ahead of having established operating procedures and requirements for rigorous performance reviews." Editorial, *Seattle Mayor McGinn Right to Ground Drones*, SEATTLE TIMES (Feb. 12, 2013), http://www.seattletimes.com/opinion/editorial-seattle-mayor-mcginn-right-to-ground-drones/ [http://perma.cc/KV22-F2NZ]; *see also* Danny Westneat, *Spy Gear Needs Public Scrutiny First*, SEATTLE TIMES (Feb. 9, 2013, 6:00 PM), http://www.seattletimes.com/seattle-news/spy-gear-needs-public-scrutiny-first/ [https://perma.cc/KV22-F2NZ].

62. Clarridge, *supra* note 30 ("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.").

63. Steve Gorman, *Los Angeles Police Try to Reassure Public on Newly Acquired Drones*, REUTERS (Sept. 16, 2014, 6:23 PM), http://www.reuters.com/article/2014/09/16/us-usa-drones-california-idUSKBN0HB2NC20140916 [https://perma.cc/VF7C-69S3].

64. 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/ [https://perma.cc/2X75-RXR2].

65. *See* Clarridge, *supra* note 28; Christine Clarridge, *Police Get the Picture on Seattle's Spy-Camera Qualms*, SEATTLE TIMES (Feb. 20, 2013, 9:01 PM), http://www.seattletimes.com/seattle-news/police-get-the-picture-on-seattlersquos-spy-camera-qualms/ [https://perma.cc/KW9K-9UHL].

66. Clarridge, *Police Get the Picture on Seattle's Spy-Camera Qualms*, *supra* note 65.

67. *See supra* Part I.

68. *See* SEATTLE POLICE DEPARTMENT, CITY OF SEATTLE PORT SECURITY MESH NETWORK 1 (2015), http://clerk.seattle.gov/~public/meetingrecords/2013/pscrt20130220_1b.pdf [http://perma.cc/J87B-8ZSL].

police to stream video back from their patrol cars to a central monitoring station.[69] And, fatefully, it would facilitate the deployment of thirty surveillance cameras in public places.[70]

In May 2012, the police department sought and obtained the unanimous approval of the city council to accept the DHS money and begin construction of the network.[71] Unfortunately, the police department's depiction of the camera network was deeply misleading. The department created the strong impression that the cameras would focus solely on port facilities and the shoreline—in other words, selected, sensitive commercial buildings and the coast—and did not mention that they would also be used for surveillance of people in residential neighborhoods.[72] Written materials described only "strategic placement of video cameras monitoring port facilities, ferry terminals, and coast lines within the City's limits."[73] Chris Steel, the police department's grant manager, testified that the cameras would "basically keep an eye on the port facilities within the Port of Seattle region."[74] Assistant Chief Paul McDonagh added that, "[t]he idea here was to strategically place cameras, video cameras, around the waterfront area that monitor the shoreline and the waterway."[75]

The department's statements turned out to be true but incomplete. The department *also* placed cameras in parts of downtown where a substantial number of people lived, but where there were no port facilities to protect. Even some of the department's strongest supporters on the council felt blindsided by this revelation. One such ally, public safety committee chair Bruce Harrell, said,

> moving forward on any kind of camera surveillance technology . . . , it's not a twenty questions game, did you ask

69. Matt A. Fikse, *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/ [https://perma.cc/LGW7-69YM].

70. *Id.*

71. *Id.*; SEATTLE, WASH., ORDINANCE 123879 (May 7, 2012), http://clerk.ci.seattle.wa.us/~archives/Ordinances/Ord_123879.pdf [http://perma.cc/9JXB-E8M4] (approving receipt of funds from U.S. Department of Homeland Security Port Security Grant Program).

72. Letter from Michael McGinn, Mayor, City of Seattle, to Sally J. Clark, President, Seattle City Council (Mar. 13, 2012), http://clerk.ci.seattle.wa.us/~archives/Ordinances/Ord_123879.pdf [https://perma.cc/KR68-MXUN].

73. *Id.*

74. Seattle City Council, *supra* note 48, at 1:17:00 (statement of Chris Steel, Grant Manager, Seattle Police Department).

75. *Id.* at 1:21:00 (statement of Paul McDonagh, East Precinct Commander, Seattle Police Department).

> the right questions . . . . I just expect the department . . . to have a heightened sensitivity toward camera issues such that I would have liked to have had this conversation when the grants were approved.[76]

In February 2013, the mayor stated that he did not want the not-yet-activated mesh network turned on until there was more public discussion.[77] The coup de grâce for the mesh network came when the media reported on yet another undisclosed capability: it could track the location of anyone carrying a wi-fi-enabled device.[78] This tracking was too much coming on the heels of the camera controversy: the mesh network was dead. In March 2014, the newly elected mayor, Ed Murray, commented that he did not expect the network to be activated for a long time, if ever. He further remarked: "This city, it appears, when opportunities arise to get money from the feds, we go after the money, maybe without thinking through whether we actually want this kind of equipment in our city."[79]

Given the cascade of surveillance controversies, some members of the city council concluded that the police department's lack of transparency was a systemic problem.[80] This led the council to adopt an innovative solution: the nation's first-ever local ordinance requiring city departments to seek approval prior to acquiring any surveillance equipment.

---

76. *Seattle City Council, Public Safety, Civil Rights and Technology Committee*, SEATTLE CHANNEL, at 1:11:00 (Feb. 20, 2013), http://www.seattlechannel.org/mayor-and-council/city-council/20122013-public-safety-civil-rights-and-technology-committee/?videoid=x22257 (last visited Dec. 17, 2016) (statement of Bruce Harrell, Chair, Public Safety, Civil Rights and Technology).

77. Jon Humbert, *City Leaders Raising Questions About Seattle Surveillance Plan*, KOMO NEWS (Feb. 14. 2013), http://www.komonews.com/news/local/City-leaders-raising-questions-about-Seattle-surveillance-plan-191352151.html [https://perma.cc/VW6F-WRGY].

78. *See* David Ham, *Seattle Police Have a Wireless Network That Can Track Your Every Move*, KIROTV (Nov. 7, 2013, 8:09 PM), http://www.kiro7.com/news/seattle-police-have-wireless-network-can-track-you/246051198 [https://perma.cc/ZSB7-72EH]

("Every time a device looks for a Wi-Fi signal and the access point recognizes it, it can store that data.").

79. *Mayor Murray Re: SPD Surveillance Cams*, WEST SEATTLE BLOG, at 01:01 (Mar. 24, 2014), http://westseattleblog.com/2014/03/wsb-qa-with-the-mayor-2-will-spds-surveillance-cameras-ever-be-turned-on/ [https://perma.cc/SD2Q-QFBV].

80. *See, e.g.*, Seattle City Council, *Public Safety, Civil Rights and Technology Committee*, SEATTLE CHANNEL, at 1:48:00 (Mar. 6, 2013), http://www.seattlechannel.org/mayor-and-council/city-council/city-council-all-videos-index?videoid=x22186 (last visited Dec. 17, 2016) (statement of Council President Sally J. Clark); SEATTLE, WASH., ORDINANCE 124142 (2013) ("WHEREAS, recent incidents involving the City's acquisition of drones and the installation of video cameras along Seattle's waterfront and downtown have raised concerns over privacy and the lack of public process leading up to the decisions to use certain surveillance equipment . . . .").

The ordinance, which passed unanimously, provides for democratic oversight and greater transparency. It obligates any department wishing to acquire surveillance equipment to "obtain City Council approval via ordinance prior to acquisition."[81] It also forbids city departments from installing or deploying such equipment until the council approves an operational protocol governing its use.[82] The operational protocol must specify how the equipment will be used and where it will be located. It must provide a description of how the equipment will impact privacy and anonymity and how the department will mitigate any risks to privacy and anonymity. Further, it must specify how and when data will be retained and who will be able to access the data and must contain a plan for reaching out to members of the public in communities where surveillance equipment will be located.[83] In addition to this operational protocol, the ordinance obligates the police to submit for approval a separate data management protocol relating to the surveillance equipment in question, addressing the collection, use, retention, and sharing of data it gathers.[84]

Although comprehensive in its requirements, the ordinance's definition of "surveillance equipment" contains exceptions that limit the scope of its application. The effect of these exceptions is unclear but could be significant. Most notably, the ordinance exempts police from the requirement to obtain council approval before acquiring surveillance equipment that it uses "on a temporary basis for the purpose of a criminal investigation supported by reasonable suspicion[.]"[85] This exemption could cover a vast amount of surveillance activity. If, for example, police temporarily installed an automatic license plate reader to register all cars coming in and out of a particular parking lot because they had reasonable suspicion that prostitution was taking place on the premises, this use would appear to be exempt.

The Seattle surveillance ordinance is now more than two years old, and the police department has not returned to the council regarding any technology acquisition. It is difficult to know what to make of this outcome. Did the negative public and political response, which included the ordinance itself, and the prospect of constraints imposed by the required protocols lead the police department to avoid the acquisition of

81. SEATTLE, WASH., MUNICIPAL CODE § 14.18.20 (2013).

82. *Id.*

83. *Id.*

84. *Id.* § 14.18.30.

85. *Id.* § 14.18.40.

new surveillance technology requiring council approval? If so, does that mean surveillance practices have been effectively constrained by the ordinance? Or have authorities found they could satisfy their wish to obtain additional surveillance using the ordinance's exceptions?

Doug Klunder, Privacy Counsel at the Washington ACLU affiliate, believes that the ordinance has forestalled the deployment of surveillance technology:

> The ordinance has had real value. It is much more likely that the mesh network would be up and running now without the ordinance. Drafting a vague privacy policy after a quiet period of a year or two might well have been enough to overcome public opposition to the mesh network. The ordinance's requirement of development of detailed protocols, along with council approval, is a greater obstacle that the police department seems unwilling to tackle.[86]

Klunder also believes that the ordinance, coupled with the experiences with the drone and the mesh network, achieved something of a cultural shift within the police department. When the Seattle Police Department wanted to roll out limited facial recognition capabilities, it brought local privacy activists into the conversation at the outset and also obtained city council approval, even though facial recognition was not covered by the terms of the ordinance (because it is a piece of software, not "equipment," as the ordinance defines it).[87]

3. Analysis of Surveillance Policy Making in Seattle

The collapse of Seattle's drone and mesh network surveillance initiatives seems to have been the result of the Seattle Police Department's persistent and ultimately self-defeating inability (or unwillingness) to bring councilmembers and the public into the decision-making process at an early stage. Once the technologies (or the full extent of their capabilities) were discovered, the public was so upset by the department's secrecy that it proved impossible to have a reasonable conversation about the underlying merits of the technology. Federal public spending programs contributed to the police department's mishandling of public relations by enabling the department to acquire the technologies without obtaining public support. The programs also enabled the police department to acquire the technologies without

86. Statement of Doug Klunder, Privacy Counsel, ACLU of Washington (June 25, 2015) (on file with author).

87. *Id.*

addressing their impact on civil rights and liberties. When the acquisitions became public, these issues had to be addressed, but it was too late to address them in a reasonable manner.

The Seattle case study also illustrates how the national security objectives that drive the federal programs are largely irrelevant at the local level. The federal government's purpose in expending funds through its Urban Areas Security Initiative and Port Security Grant Program was to combat terrorism. This purpose was lost in the debate in Seattle. Instead, residents and council members focused on the immediate and tangible effects of the surveillance equipment acquired under these programs on day-to-day policing. This outcome is not surprising. Surveillance equipment is inherently dual-purpose equipment, and terrorism is a relatively small proportion of overall crime.

Finally, the Seattle case study offers a partial path forward in the council's surveillance equipment ordinance. The ordinance ensures early public disclosure and an opportunity for public debate. But this solves only the problem of nondisclosure. The city council and the public must be able to grasp the implications of what they are being told. Our next case study, Oakland, shows that this can be a problem.

B. Oakland Acquires a Domain Awareness Center

In 2010, the Oakland City Council granted its police and fire departments approval to build a Domain Awareness Center (DAC), using federal funds from the Port Security Grant Program, to enhance security at Oakland's port. The DAC aggregated surveillance data already being gathered in all corners of the city into a single facility for monitoring and analysis. The theory behind this data aggregation was that it would improve the ability of port officials to anticipate threats to the port while also enhancing the capabilities of Oakland's police and fire departments to detect crime and respond to emergencies.

The council unanimously approved the DAC, and no members of the public objected. It was not to stay that way. In 2013, police and fire representatives (whom I refer to as "city staff") returned to the city council to request approval to accept another infusion of federal funds to increase the DAC's capacity, primarily by integrating additional data sources. This time, the community response was swift and overwhelmingly negative. Given Oakland's decades-long history of poor community-police relations, the DAC's capabilities far outstripped anything the public was willing to entrust to its police department.

The opposition prompted the city council to pass a resolution limiting the geographic scope of the DAC's surveillance to the immediate port

area and then to convene a citizen task force to draft a privacy policy for the DAC. A dedicated collection of residents met dozens of times in meetings open to the public. They worked collaboratively with city staff and crafted a privacy policy acceptable to everyone. The process was so successful that the policy passed the city council unanimously, and the council also created a standing citizen privacy committee to draft a Seattle-style surveillance equipment ordinance to apply to all government surveillance technology citywide.

If Seattle demonstrated how a police department could sabotage its surveillance initiatives by provoking public anger through excessive secrecy, then Oakland illustrates both the limits and promise of greater involvement of local elected officials and members of the public. Oakland city staff did voluntarily what Seattle officials are now compelled by ordinance to do: they came early to the city council and were forthcoming with details about their surveillance initiative. Yet neither council members nor the general public grasped the significance of what they were being told. Once the DAC did become politically salient, however, the process by which Oakland devised a privacy policy was a model of inclusiveness and collaboration. It resulted in a privacy policy that allowed the DAC to go forward and still reflected the community's strongly expressed political preferences.

1. History of Police-Community Relations in Oakland

It is difficult to understand Oakland's reaction to the DAC without at least some understanding of the history of police-community relations in Oakland. It is not possible to more than gesture at this history in the space available in this Article.[88] For present purposes, suffice it to say that the people of Oakland have a long and troubled relationship with their police force. The Black Panthers got their start organizing armed citizens' patrols to monitor police officers in Oakland[89] and became one of the FBI's main targets in its notorious COINTELPRO surveillance investigations. COINTELPRO, or "Counterintelligence Program," was an FBI initiative that surveilled and disrupted domestic political and social groups. Eventually, Congress condemned the program and the

88. There does not appear to be a single, definitive treatment of policing in Oakland. However, for a work that addresses policing in Oakland within the context of broader social and political questions, see ROBERT O. SELF, AMERICAN BABYLON: RACE AND THE STRUGGLE FOR POSTWAR OAKLAND (2003).

89. Steve Wasserman, *Rage and Ruin: On the Black Panthers*, THE NATION (June 5, 2013), http://www.thenation.com/article/rage-and-ruin-black-panthers/ [https://perma.cc/3BKF-CNYP].

FBI repudiated it.[90] Politically involved people in Oakland, particularly older people, still evoke COINTELPRO when arguing for limits on surveillance and on the authority of the police more generally.[91]

If Oakland's status as home of the Panthers provides a historical backdrop, a more recent example of systematic police abuse further shapes citizen-police relationships. In 2000, rookie police officer Keith Batt resigned after just ten days on the force. He did so to blow the whistle on the conduct of four officers, known as the Riders, who were assaulting, planting evidence on, and arresting innocent people in West Oakland—at that time a mostly black community.[92]

Investigations substantiated Batt's allegations. Although criminal prosecutions of the accused officers was unsuccessful, the police department fired the Riders, and a civil suit based on the officers' abuse yielded a $10.9 million settlement for 119 people.[93] More importantly, the settlement compelled the city to agree to implement a list of fifty-one reforms.[94]

Nearly a decade later, the city had failed to implement a substantial number of these mandated reforms.[95] In 2012, U.S. District Court Judge Thelton Henderson, frustrated with the non-compliance, threatened to put the entire department under federal receivership and ultimately

---

90. FED. BUREAU OF INVESTIGATION, *COINTELPRO*, FBI RECORDS: THE VAULT, https://vault.fbi.gov/cointel-pro [https://perma.cc/3MPU-9TDM] ("COINTELPRO was later rightfully criticized by Congress and the American people for abridging first amendment rights and for other reasons.").

91. *See, e.g.*, *Concurrent Meeting of the Oakland Redevelopment Agency & City Council*, CITY OF OAKLAND, CAL., at 03:41 (Mar. 4, 2014), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1462 (last visited Dec. 17, 2016) (public commenter invoking the Panthers and COINTELPRO).

92. Glenn Chapman, *Prosecutor Gives Up 'Riders' Case*, EAST BAY TIMES (June 3, 2005), http://www.insidebayarea.com/dailyreview/localnews/ci_2777760 [https://perma.cc/LW8D-B5MA]; Jim Herron Zamora, *Spotlight on Police as 'Riders' Go on Trial*, S.F. GATE (Apr. 29, 2002), http://www.sfgate.com/bayarea/article/Spotlight-on-police-as-Riders-go-on-trial-2844728.php [https://perma.cc/NES2-LHFD] ("Two years after a band of Oakland police officers known as the 'Riders' allegedly arrested and roughed up innocent citizens in the biggest scandal to hit the department in decades, three of the officers are scheduled to go on trial today as the case ripples through the city.").

93. *D.A. Is Right to Seek Retrial of 'Riders' Case*, THE ARGUS (Nov. 19, 2003); Chip Johnson, *Prosecution Fumbled on Riders' Case / Witnesses Couldn't Win Credibility*, S.F. GATE (Oct. 6, 2003, 4:00 AM), http://www.sfgate.com/bayarea/johnson/article/Prosecution-fumbled-on-Riders-case-Witnesses-2554318.php [https://perma.cc/5H9J-DMCJ].

94. Matthew Artz, *Oakland Makes Case Against OPD Takeover*, EAST BAY TIMES (Nov. 9, 2012), http://www.insidebayarea.com/oakland-tribune/ci_21965506/oakland-makes-case-against-opd-takeover [https://perma.cc/5LYC-SD64].

95. *Id.*

approved the appointment of a court-supervised compliance director to force progress.[96] The compliance director continues his work to this day.

Although shootings of civilians by Oakland police have dropped substantially in recent years, as have civil rights lawsuits against the city, the department is still riven by scandal.[97] Two years before the DAC controversy broke out, Oakland was the home of a major spin-off of the Occupy Wall Street movement.[98] Occupy Oakland participants repeatedly established encampments at various places in Oakland, which the police were then called upon to clear out.[99] Participants leveled charges of excessive use of force against police officers.[100] While most protesters were peaceful, a small share committed property damage and threw objects at police officers.[101] In a more recent and particularly shocking scandal, over a dozen officers are currently being investigated in connection with allegations that they had sex with a teenage prostitute, who may have been a minor at the outset of some of the sexual relationships.[102]

2. The Controversy over the Domain Awareness Center

Oakland's work on the DAC can be traced back at least to 2009. Just three days before the submission deadline for that year's federal Port Security Grant Program, city staff submitted an informational memorandum to the city council about their collaboration with the Port of Oakland on a grant application.[103] The city does not appear to have thought of the idea of creating a DAC itself. Rather, it seems to have

---

96. Demian Bulwa & Carolyn Jones, *Oakland Cuts Deal on Cops*, S.F. CHRON., Dec. 6, 2012, at A1; Dan Levine, *For Police Reformers, California City Shows a Rough Road*, REUTERS (Dec. 14, 2014), http://www.reuters.com/article/us-usa-police-oakland-insight-idUSKBN0JS0HL20141214 [https://perma.cc/WP5G-9H5W].

97. Levine, *supra* note 96.

98. *Occupy Oakland*, WIKIPEDIA, https://en.wikipedia.org/wiki/Occupy_Oakland [https://perma.cc/TC8Z-ZTLM].

99. *Id.*

100. *Id.; see also* Matthai Kuruvila, Justin Berton & Demian Bulwa, *Police Tear Gas Occupy Oakland Protesters*, S.F. GATE (Oct. 25, 2011), http://www.sfgate.com/bayarea/article/Police-tear-gas-Occupy-Oakland-protesters-2325544.php#photo-1830498 [https://perma.cc/6KMV-5HPZ].

101. *Id.*

102. Thomas Fuller, *A Young Prostitute, Police Scandals and a Rocky Renaissance in Oakland*, N.Y. TIMES (June 27, 2016), http://www.nytimes.com/2016/06/28/us/a-young-prostitute-police-scandals-and-a-rocky-renaissance-in-oakland.html?_r=0 [https://perma.cc/4PHK-EV4F].

103. Memorandum from Dan Lindheim, City Adm'r, City of Oakland, to Pub. Safety Comm., City of Oakland, 1–2 (June 23, 2009), http://clerkwebsvr1.oaklandnet.com/attachments/22406.pdf [http://perma.cc/WNH2-DAEL].

been a response to the decision of federal grant administrators to prioritize funding projects that "reflect 'robust regional coordination' and an investment strategy that institutionalizes regional security strategy integration."[104]

The grant proposed creating a DAC "to consolidate a network of existing surveillance and security sensor technologies and data to actively monitor critical Port facilities, utility infrastructure, roadways, *and ultimately establish a citywide system*."[105] City staff emphasized that "[t]he combination of a *maritime* monitoring and coordination center with the City of Oakland's [existing] inter-agency, *landside* monitoring and coordination center, [the Emergency Operations Center (EOC)] could have great potential and benefits in protecting people and critical infrastructure in both the City and the Port area."[106] City staff also envisaged the possibility that information sharing might eventually be regional in scope: "[T]he Center would provide functionality and a location where multiple agencies can access integrated regional capabilities and technologies including sensors, platforms, communications and information exploitation."[107]

The DAC, on its own, would not collect additional data. Rather, it was to be a data integration center, networking together the city's existing surveillance infrastructure. There are a couple of reasons why a city might want to do this. First, it makes the data the city is collecting more useful (although potentially more privacy-invasive). For example, it would enable police officers, within the confines of a single program, to look both at feeds from video cameras and data collected by license plate readers. As a result, if a police officer noticed suspicious activity while monitoring a surveillance camera feed, he or she could easily check plate-reader data to see who had driven through the area recently. This is more efficient than the status quo, in which camera footage is viewed and stored in one program and plate-reader data is viewed and stored in a separate program. Second, integrating data into one center, with a common format, makes it easier to share that data with others in the region and beyond who might have need for it, and perhaps reciprocally to obtain surveillance data from others.[108]

---

104. *Id.* at 2.

105. *Id.* at 3 (emphasis added).

106. *Id.* at 4 (emphasis in original).

107. *Id.*

108. How one feels about data integration probably depends on how one feels about surveillance in general. If one is of the view that the government is engaged in too much surveillance, then the barrier to surveillance posed by having to separately access, for example, surveillance camera feeds

In July 2010, city staff came before the council's public safety committee to request authorization to accept $2.9 million in federal funds.[109] No city council member asked a question, and no members of the public sought to comment. The committee unanimously granted the staff's request.[110] The entire process took less than two minutes. The request then went to the full city council, where it was one of sixty-five items on the consent calendar, a special list of non-controversial items that could be approved as a group through one vote rather than discussed and voted on individually. Neither members of the council nor the public commented on the issue.[111] The press also took no notice of this development.

The city and port worked on constructing the DAC for about three years. City staff integrated port and city surveillance cameras, the port's intrusion detection system, the city's gunshot detection technology, and mapping software[112] into the DAC.[113] In 2013, the project returned to the city council's docket because city staff needed council authorization to accept a second round of federal funds.[114] This time, city staff sought to accept up to two million dollars in additional port security grant funds to build out the DAC's capacity, primarily by incorporating additional data sources.[115] In its report to the council, the DAC team listed "City School Closed-Circuit Television (CCTV) System" and California Department of Transportation cameras as data sources to add, as well as unspecified "[s]urveillance enhancements for City of Oakland historically high crime

---

and license plate reader records can be viewed positively. An officer would need to be highly motivated to go through the effort of gathering data across systems. If, on the other hand, one does not object to data collection, then the idea of making the data more easily accessible, and easier to analyze and share, can be considered a net benefit.

109. *Special Public Safety Committee*, CITY OF OAKLAND, CAL., at 00:29 (July 13, 2010), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=706 (last visited Dec. 17, 2016) (statement of Renee Domingo, City of Oakland Director of Emergency Services and Homeland Security).

110. *Id.* at 3:00.

111. *Concurrent Meeting of the Oakland Redevelopment Agency/City Council*, CITY OF OAKLAND, CAL., at 01:23 (July 20, 2010), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=712 (last visited Dec. 17, 2016).

112. As the name suggests, this is software that provides a detailed map of the city.

113. CITY & PORT OF OAKLAND, JOINT DOMAIN AWARENESS CENTER, PHASE 2 CONTRACT AWARD RECOMMENDATION AND STAFF REPORT, at slide 7 (Jan. 28, 2014), https://oakland.legistar.com/View.ashx?M=F&ID=2867275&GUID=02B29757-4333-419B-9403-ED47610DEF90 [https://perma.cc/ZH8L-KQDP].

114. Oakland City Council, *Public Safety Committee*, CITY OF OAKLAND, CAL., at 2 (July 9, 2013), https://oakland.legistar.com/View.ashx?M=M&ID=253930&GUID=F28C607C-1680-4BED-A9C6-49AD169D1B01 [https://perma.cc/BHV2-KRLH].

115. *Id.*

areas."[116] City staff also floated the possibility of integrating private surveillance cameras into the DAC.

The matter of whether to accept the second round of federal funding was first referred to the council's public safety committee. Council member Dan Kalb asked about the DAC's integration of video cameras, and where those cameras would be located: "First of all, this is all on port property, including airport, all the port property, right? It's not the rest of the city."[117] Renee Domingo, the city's emergency manager, responded, "It will also integrate any existing cameras the city has."[118] Kalb followed up, "But on or adjacent to port property, not, like, four miles away from the port or anything, it's all that general area, is that right?" Domingo did not provide a direct answer to this question.[119] Kalb moved onto other topics, but then circled back to ask, "I assume none of these cameras go into people's living rooms or anything like that?"[120] Domingo replied that they did not.[121] The public safety committee then unanimously approved accepting the funding, resulting in the matter advancing to the full city council.[122]

The exchange between Kalb and Domingo did not go unnoticed by members of the public. When the full city council met the following week, and the question of accepting a second infusion of federal money came up on the consent calendar, the sailing was not so smooth.[123] About a dozen individuals spoke against the DAC during the public comment period and none spoke in support. Many speakers were concerned about the paucity of available information on what would be done with data gathered in the DAC. The following is a representative comment:

---

116. Agenda Report Memorandum from Teresa Delach Reed, Fire Chief, City of Oakland, to Deanna J. Santana, City Adm'r, City of Oakland 5 (June 23, 2013), https://oakland.legistar.com/View.ashx?M=F&ID=2554079&GUID=BFC8C979-8FA8-4B7E-B8ED-6C0F54A60FFC [http://perma.cc/K9F3-JKKE].

117. *Public Safety Committee*, CITY OF OAKLAND, CAL., at 00:27 (July 9, 2013), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1315 (last visited Dec. 17, 2016).

118. *Id.* at 00:28.

119. *Id.*

120. *Id.* at 00:30.

121. *Id.*

122. *Id.* at 00:31.

123. *Concurrent Meeting of the Oakland Redevelopment Successor Agency & City Council*, CITY OF OAKLAND, CAL., (July 16, 2013), https://oakland.legistar.com/View.ashx?M=A&ID=254282&GUID=902659F8-00DA-45CB-8368-C86C2D45CCFA [https://perma.cc/PY4J-EU4X].

> We don't know how long this data is going to be collected, we don't know what other agencies it's going to be shared with, we don't know, you know, they were talking about having access to it on mobile devices by OPD. Any officer? Only a limited number of people? There are so many unanswered questions that you really should put a stop to this until you have some actual oversight.[124]

Members of the council took these concerns to heart and decided to postpone action on the item until its next meeting.[125] By the time the issue again arose two weeks later, the DAC had become the object of significant national press attention. At the local level, it was sufficiently controversial to prompt fifty members of the public to show up to express their views.[126]

It is difficult to say with certainty why the DAC, which provoked no objection in 2010, proved so controversial in 2013. However, by 2013, the national political climate had grown considerably more hostile toward government surveillance. Just weeks before the DAC came before the council, the media began reporting a series of stories about the unprecedented scale and scope of the National Security Agency's surveillance programs.[127] Reporters based these stories on documents exfiltrated by government contractor Edward Snowden, whose dramatic escape to Hong Kong and subsequent flight to Moscow further fueled a media firestorm.[128] For the first time since 9/11, members of the public appeared increasingly skeptical of the federal government's surveillance initiatives. The DAC, although wholly unrelated to any of the programs

---

124. *Concurrent Meeting of the Oakland Redevelopment Agency & City Council*, CITY OF OAKLAND, CAL., at 02:52 (July 16, 2013), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1320 (last visited Dec. 17, 2016) (statement of David Colburn).

125. *Id.* at 03:34.

126. CITY OF OAKLAND, CAL., SPECIAL CONCURRENT MEETING OF THE OAKLAND REDEVELOPMENT SUCCESSOR AGENCY / CITY COUNCIL / GEOLOGIC HAZARD ABATEMENT DISTRICT BOARD, at 35 (July 30, 2013), https://oakland.legistar.com/View.ashx?M=M&ID=258725&GUID=E6ABC786-3DB3-4F03-83C8-1DED575F4AC6 [http://perma.cc/M945-9NCH].

127. *See, e.g.*, Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2016), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/32BA-YBL3]; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/JM86-PLFT].

128. Tania Branigan & Miriam Elder, *Edward Snowden Leaves Hong Kong for Moscow*, GUARDIAN (June 23, 2013), https://www.theguardian.com/world/2013/jun/23/edward-snowden-leaves-hong-kong-moscow [http://perma.cc/QTD7-N3HY].

disclosed by Snowden, nonetheless may have been caught in the crosshairs.

In response to increasing public concern, the city council imposed substantial privacy safeguards on the DAC. It limited the data that could be incorporated into the DAC to city- and port-owned sources,[129] and it required city staff to develop a privacy and data retention policy for the DAC.[130] Members of the public were largely unappeased because they wanted the entire enterprise shut down. However, the council approved the DAC, probably reflecting the sentiment expressed by council member (now Mayor) Libby Schaaf:

> We have tried our best to find the sweet spot. We are going to take advantage of the tools that we have at hand to make our city safe . . . and at the same time try and address the really legitimate and important concerns that have been raised . . . but if we do not approve this money tonight, we jeopardize losing valuable resources that will make the City of Oakland safer.[131]

Unfortunately for proponents of the DAC, two key missteps by city staff provided ammunition for those who felt that Oakland city officials were either not competent or not trustworthy, and in either case should not be afforded the increased power for surveillance the DAC would bring.

First, an investigation by the non-profit Oakland Privacy Working Group[132] demonstrated that the contractor building the DAC had been hired in violation of a city prohibition on doing business with entities involved in nuclear weapons work.[133] This revelation forced city staff to return to the city council on multiple occasions to secure approval of a new contractor,[134] with each appearance giving opponents an opportunity to ramp up their objections.[135]

---

129. CITY OF OAKLAND, CAL., *supra* note 126, at 34–35.

130. *Id.*

131. *Special Concurrent Meeting of the Oakland Redevelopment Successor Agency / City Council / Geologic Hazard Abatement District Board*, CITY OF OAKLAND, CAL., at 06:54 (July 30, 2013), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1330 (last visited Dec. 17, 2016).

132. Matthew Artz, *Nuclear Law Again Threatens Oakland Surveillance Hub*, CONTRA COSTA TIMES (Jan. 29, 2014), http://www.contracostatimes.com/news/ci_25019462/nuclear-law-again-threatens-oakland-surveillance-hub [http://perma.cc/UQM6-XHWF].

133. *Public Safety Committee*, CITY OF OAKLAND, CAL., at 03:28 (Nov. 12, 2013), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1391 (last visited Dec. 17, 2016).

134. CITY OF OAKLAND, CAL., *Meeting Minutes: Public Safety Committee*, at 5 (Nov. 12, 2013), https://oakland.legistar.com/View.ashx?M=M&ID=268611&GUID=D7918CB2-FFAE-4FC0-AC70-1E34F0EA11D2 [https://perma.cc/E4MQ-2E4S]; CITY OF OAKLAND, CAL., *Meeting*

By early 2014, the volume of opposition was sufficient to prompt the city staff to request policy guidance from the council on whether the project should continue at all and, if so, in what form. At this point the DAC included 137 port security cameras, the port's physical intrusion detection system, the city's gunshot detection technology,[136] the mapping program, and forty city traffic cameras.[137] A January hearing revealed the city staff's second major error: failure, despite the passage of eight months, to draft the privacy and data retention policy for the DAC that the city council had specifically directed them to draft. While staff then hurriedly put together what they called a draft privacy framework, city council members were harshly critical. They said that it should have come out months earlier, and one member characterized it "not as a draft of a set of policies" but "more like a draft of a draft of a draft."[138]

Things came to a head at a council meeting in March 2014, by which time the DAC had generated a truly remarkable amount of opposition. One hundred forty-nine members of the public submitted requests to speak at the meeting, and the comments they made were overwhelmingly negative. They came from a broad cross-section of the community. Dan Siegel, a prominent Oakland attorney and activist, specifically invoked the past use of COINTELPRO to attack the Panthers as a reason to oppose the DAC, as did some other older

---

Minutes: Concurrent Meeting of the Oakland Redevelopment Successor Agency & City Council, at 30 (Nov. 19, 2013), https://oakland.legistar.com/View.ashx?M=M&ID=274014&GUID=40979A84-886E-4AE6-A254-6BE7A4E0197D [https://perma.cc/VU9P-SVXK] [hereinafter Nov. 19 2013 Meeting Minutes].

135. For example, at a November 19, 2013 full-council meeting at which the DAC team returned to obtain authorization to select a new contractor, sixty-one speakers showed up to provide comment on the DAC, and nearly all of them expressed negative views. CITY OF OAKLAND, CAL., Nov. 19 2013 Meeting Minutes, *supra* note 134. The council did, however, authorize the DAC team to seek out a new vendor, with the proviso that the council would need to authorize going forward with that vendor. *Id.*

136. Gunshot detection technology is a network of microphones that is designed to detect gunshots and automatically report them to the police. Will Kane, *Oakland Cops Aim to Scrap Gunfire-Detecting ShotSpotter*, S.F. GATE (Mar. 14, 2014), http://www.sfgate.com/crime/article/Oakland-cops-aim-to-scrap-gunfire-detecting-5316060.php [https://perma.cc/N9E4-QJSC].

137. *Public Safety Committee*, CITY OF OAKLAND, CAL., at 1:56 (Jan. 28, 2014), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1437 (last visited Dec. 17, 2016). The figure forty is striking because the previous summer Domingo had told the council that the city had only four to five such cameras. It is unclear whether one of the figures was incorrect, or whether the city installed a substantial number of additional traffic cameras at the same time that members of the public were increasingly pushing back against the DAC.

138. *Concurrent Meeting of the Oakland Redevelopment Agency/City Council*, CITY OF OAKLAND, CAL., at 4:53 (February 18, 2014), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1449 (last visited Dec. 17, 2016).

Oakland residents.[139] Individuals who had recently participated in the Occupy Oakland demonstrations complained that the police department's conduct toward demonstrators showed they were untrustworthy.[140] Most strikingly, perhaps one-third of the public speakers expressly identified themselves as Muslim and grounded their opposition to the DAC in more general concerns about the surveillance of Muslims after 9/11.[141]

In the end, a closely divided council voted to restrict the DAC to monitoring only the port and to remove the forty city traffic cameras from the DAC along with the portions of its gunshot detection system not proximate to the port.[142] Further, the council forbade DAC personnel from sharing data with any local, state, or federal entity without a memorandum of understanding expressly authorized by the council, and it prohibited the addition of new "systems or capabilities" without council approval.[143] It also reiterated the requirement that the council sign off on a privacy and data retention policy prior to activation of the DAC and convened a citizen task force to develop this policy.[144] The DAC henceforth would be structured to focus on the immediate port area, with a close supervisory structure to ensure that the council would have to affirmatively approve any expansion of the DAC.

City staff worked to assemble a group of individuals to serve on the privacy policy task force, including those with expertise in technology and civil liberties, those from a broad range of Oakland neighborhoods, and representatives of the business community.[145] The resulting committee met dozens of times with city staff in meetings open to the public.[146] It first gathered information about the DAC from city staff and

---

139. *Concurrent Meeting of the Oakland Redevelopment Successor Agency & City Council*, CITY OF OAKLAND, CAL., at 3:41 (Mar. 4, 2014), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1462 (last visited Dec. 17, 2016) [hereinafter Concurrent Meeting]

140. *Id.* at 4:02 (public comment of unnamed, self-identified protest participant).

141. *Id.* (comments beginning at about 5:02).

142. *Concurrent Meeting of the Oakland Redevelopment Successor Agency & City Council*, *supra* note 139 (meeting minutes at 17).

143. *Id.* at 17–18.

144. *Id.* at 18.

145. Agenda Report Memorandum from Joe DeVries, Assistant to the City Adm'r, City of Oakland, to John A. Flores, Interim City Adm'r, City of Oakland 4 (Jan. 28, 2015), https://oakland.legistar.com/View.ashx?M=F&ID=3479358&GUID=6DD7CFF6-804F-48C6-AFDC-6DE72F3E1C3E [perma.cc/TJ8H-AW2Z].

146. *See id.* (the committee "met 18 times over six months" through January 2015); Agenda Report Memorandum from Joe DeVries, Assistant to the City Adm'r, City of Oakland, to John A. Flores, Interim City Administrator, City of Oakland 2 (Apr. 30, 2015),

formulated core principles to guide its work going forward. It then used these core principles to develop a draft privacy policy for the DAC.[147] The policy dealt with the key questions of data usage, storage, and dissemination.[148] The policy did so by limiting the DAC's uses to a specifically enumerated list (e.g., active shooter, bomb threat, earthquake); by forbidding the DAC to store data unless relevant to one of the enumerated uses; and by prohibiting data sharing except pursuant to court order or a written memorandum of understanding or contract approved by the city council.[149]

This process resulted in the creation of a policy that both city staff and the community members could support and that ultimately passed the city council unanimously.[150] Although it is difficult to generalize about what the public thought, segments of the public that had been critical of the DAC expressed satisfaction with this outcome.[151]

The process was so successful that city staff supported the committee's suggestion that a permanent standing privacy advisory commission be formed to examine privacy in the city as a whole and to develop a citywide surveillance equipment ordinance.[152] As the city staff member charged with meeting with the committee put it to the city council:

> This has been a new field for us as far as staff is concerned, partnering with the community, partnering with privacy advocates, bringing our first responders and law enforcement to the table. It's been a rich dialog and I think it will continue to be a rich dialog as more technologies are introduced to the marketplace, and having an ordinance that guides and creates a

---

https://oakland.legistar.com/View.ashx?M=F&ID=3728533&GUID=F9217BE0-83E6-479F-B072-A370FCFCB846 [http://perma.cc/YXM8-2DWJ] (noting a series of additional meetings in 2015).

147. *DAC Draft Privacy Policy Public Comments*, CITY OF OAKLAND, CAL., http://www2.oaklandnet.com/Government/o/CityAdministration/OAK051790 [http://perma.cc/MTA8-GEWC] (describing the committee's formation and its development of the privacy policy).

148. *See* OAKLAND, CAL., RESOLUTION 85,638 (June 2, 2015). The council had dealt with the threshold issue of what data was to be collected by passing legislation specifying what sources could be fed into the DAC. *See* OAKLAND, CAL., RESOLUTION 84,869 (Mar. 4, 2014).

149. OAKLAND, CAL., RESOLUTION 85,638 (June 2, 2015).

150. *Concurrent Meeting of the Oakland Redevelopment Successor Agency and the City Council*, CITY OF OAKLAND, CAL., at 8:59:00 (June 2, 2015), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1785 (last visited Dec. 17, 2016).

151. *Id.* at 9:04:00 (public comment period).

152. *Public Safety Committee*, CITY OF OAKLAND, CAL., at 1:01:45 (May 26, 2015), http://oakland.granicus.com/MediaPlayer.php?view_id=2&clip_id=1781 (last visited Dec. 17, 2016).

> public process to avoid surprises in the future is good government.[153]

The city council voted in favor of creating a permanent standing privacy advisory commission as well.[154]

3. Analysis of Surveillance Policy Making in Oakland

While the local police department in Seattle caused the backlash against its surveillance initiatives by proceeding secretly, in Oakland it was the elected representatives who misjudged the eventual public reaction by not understanding the implications of a new technology. The Oakland case study therefore highlights potential shortcomings of relying on local elected representatives to set surveillance policy. Council members have many matters to attend to that place severe constraints on their ability to devote time to, and develop expertise about, surveillance policy. Had the council members understood the technology, they might have avoided the protracted and strident controversy that unfolded.

As in Seattle, the federal government set the stage for these mistakes by allocating money for the DAC without requiring that anyone develop a policy for its use. This left both elected representatives and city staff scrambling to fill the void once the public and city council members grasped the DAC's capabilities.

In Seattle, the debate largely ignored the fact that the technologies were being promulgated in the name of national security. In Oakland, the fact that the DAC also served a federal national security purpose was an additional strike against it. Oakland's distrust of its police department may have been enough on its own to kill the DAC, but the Muslim community's feeling of being unfairly scrutinized by the federal government after 9/11[155] and the skepticism generated by Edward Snowden's disclosures poisoned the atmosphere still further.[156]

Oakland offers another path forward. The most innovative and successful piece of the Oakland story is the city council's creation of a

---

153. *Id.* at 1:04:00.

154. OAKLAND, CAL., ORDINANCE 13,349 (Jan. 19, 2016), https://oakland.legistar.com/View.ashx?M=F&ID=4220932&GUID=AA93003C-FE0C-45DB-9F0A-AD0C377D5B5A [https://perma.cc/4TTH-Q3YD].

155. *See Concurrent Meeting*, *supra* note 139, at 5:02.

156. Brian Hofer, *How the Fight to Stop Oakland's Domain Awareness Center Laid the Groundwork for the Oakland Privacy Commission*, ACLU OF NORTHERN CALIFORNIA (Sept. 21, 2016), https://www.aclunc.org/blog/how-fight-stop-oaklands-domain-awareness-center-laid-groundwork-oakland-privacy-commission [https://perma.cc/NHC6-PNCA].

citizen task force to draft a privacy policy for the DAC.[157] But as successful as the citizen privacy committee was in Oakland, it is unlikely to be replicable in very many places. The success of such a committee depends on a continued high level of interest and day-to-day involvement by members of the public. Oakland's strong tradition of activism (and cadre of dedicated activists willing to spend their evenings and weekends in city meeting rooms) and high level of concern about police abuses of power were key ingredients. Not many municipalities share these features.[158]

At the same time, the Oakland experience provides reason to be skeptical that Seattle-style surveillance equipment ordinances will result in meaningful oversight or achieve significant public buy-in. From the start, Oakland city staff did voluntarily much of what Seattle now mandates. They informed the city council prior to seeking federal funding[159] and, after they won the grant, presented information about the DAC to the city council in an open hearing.[160] These steps were not enough to provoke meaningful engagement by the council or to win the DAC much-needed political legitimacy.[161]

Whatever the differences between Oakland's and Seattle's surveillance controversies, both shared the bedrock feature that a city council was the ultimate policy-making body. This was not the case in the next case study, where a regional law enforcement authority received federal funds for a surveillance initiative, raising a host of additional transparency and accountability concerns.

C. San Diego Acquires Facial Recognition Technology

Beginning in 2007, a regional law enforcement authority in the San Diego area began using federal money to develop and deploy facial recognition technology. This technology allowed officers to determine whether individuals they encountered had arrest records simply by snapping photos of them. The public did not learn of the technology until 2013, by which time it was well established and widely viewed as a success. Publicity about the technology in 2013 prompted the regional

157. *See Concurrent Meeting*, *supra* note 139.

158. *See* Jonathan Mahler, *Oakland, the Last Refuge of Radical America*, N.Y. TIMES (Aug. 1, 2012), http://www.nytimes.com/2012/08/05/magazine/oakland-occupy-movement.html [https://perma.cc/3N4T-B5UT].

159. *See supra* note 103.

160. *See supra* notes 109–11 and accompanying text.

161. *Id.*

authority to adopt a fairly sound set of rules regulating the use of the technology to protect individual privacy.

1. History of the San Diego Association of Government's Automated Regional Justice Information System

In contrast to Oakland and Seattle, the trajectory of San Diego's surveillance initiative was divorced from broader questions of community-police relations. Instead, it was the product of the specific institution that fostered its development: the Automated Regional Justice Information System (ARJIS), a law enforcement authority embedded within a regional planning entity, the San Diego Association of Governments (SANDAG).

SANDAG coordinates the activities of nineteen local governments in the greater San Diego area.[162] Its primary focus is on regional planning issues such as transportation and housing, not law enforcement. Its visibility is low. Media and advocacy groups do not monitor its activities regularly, and few members of the public have heard of it. While SANDAG proceedings are open and offer opportunities for public comment, virtually no members of the public attend.[163]

ARJIS is a sub-entity of SANDAG.[164] Its mandate is "to share information among justice agencies throughout San Diego and Imperial Counties."[165] ARJIS has eighty-two member agencies, including local, state, and federal law enforcement organizations with operations in the

---

162. *About SANDAG*, SANDAG, http://www.sandag.org/index.asp?fuseaction=about.home [https://perma.cc/4TKN-XE4Y].

163. *SANDAG, An Assessment of its Role in the San Diego Region*, LEGISLATIVE ANALYST'S OFFICE, http://www.lao.ca.gov/2006/sandag/sandag_033006.htm#governance [https://perma.cc/5ALH-DJ8N] ("Few interest group representatives—and even fewer ordinary residents—attend SANDAG board meetings. Public comment is limited."). SANDAG's governance structure may be part of the reason why. Members of the public do not elect anyone to SANDAG. *See id.* Instead, SANDAG is controlled by a board of directors consisting of people elected to positions in one of SANDAG's member governments, who are then appointed to the SANDAG board as an additional duty. *Id.* For example, the board's chair is Ron Roberts, a member of the San Diego Board of Supervisors. *About SANDAG: Board of Directors*, SANDAG, http://www.sandag.org/index.asp?fuseaction=about.board [https://perma.cc/WVQ4-XHVT].

164. *ARJIS Governance*, AUTOMATED REG'L JUSTICE INFO. SYS., http://www.arjis.org/SitePages/Policies.aspx [https://perma.cc/69ZV-TX8U].

165. *See What Is ARJIS?*, AUTOMATED REG'L JUSTICE INFO. SYS., http://www.arjis.org/SitePages/WhatIsARJIS.aspx [https://perma.cc/TQJ3-582L]; AUTOMATED REG'L JUSTICE INFO. SYS., ARJIS TACIDS: TACTICAL FACIAL RECOGNITION IN THE FIELD, 1–3 (2013), http://www.theiacp.org/Portals/0/pdfs/LEIM/2013Presentations/2013%20LEIM%20Conference%20Workshop%20-%20Technical%20Track%20-%20TACIDS.pdf [https://perma.cc/VTK4-V658] [hereinafter ARJIS TACIDS].

area.[166] Many of these agencies contribute both money and the data they gather to ARJIS, which provides tools to allow law enforcement officers "to efficiently query various regional, state, and federal data sets for subject information and case leads."[167] In addition to facial recognition technology, ARJIS has created other tools, including a searchable repository of license plate reader data[168] and access to documentation regarding millions of police-citizen interactions, from traffic citations to arrest reports.[169]

Because ARJIS is a single-mission agency focused on information sharing, its structure is designed to facilitate that mission.[170] It has a formal technical working group, which evaluates new technologies prior to adoption.[171] ARJIS staffs this working group with a mix of end users (e.g., investigators, patrol officers) and managers to ensure the technologies are useful to everyone.[172] It also has a business working group that addresses legal, ethical, and regulatory issues.[173] Both groups must vet any significant change to an ARJIS system.[174]

ARJIS may sound unusual, but it is not an anomaly. It is one of many regional law enforcement agencies around the country. Researchers have identified over 250 public safety networks that develop inter-agency collaborations among public safety organizations at the local, state, and national levels and suggest that formation of these organizations has "gained additional impetus in the post 9/11 environment."[175]

---

166. *See* ARJIS TACIDS, *supra* note 165, at 1–3.

167. *See* BOARD OF DIRECTORS AGENDA, SAN DIEGO ASS'N OF GOV'TS (July 11, 2014), http://www.sandag.org/uploads/meetingid/meetingid_3849_17876.pdf [https://perma.cc/UA2E-7KCK] [hereinafter SANDAG Board Agenda, July 11, 2014] (agenda item no. 14-07-2A, "Public Safety Program Overview" and Attachment 1).

168. The repository is a searchable database of the times and locations where license plates were seen. ACLU, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 4 (2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/5J27-4N3F].

169. ARJIS TACIDS, *supra* note 165, at 3.

170. *See* Michael J. Tyworth, Reflections of Identity: How Information Systems Mirror the Organization as a Social Actor 128–29 (Dec. 2009) (unpublished Ph.D. dissertation, Pennsylvania State University) (on file with author).

171. *Id.* at 94–95.

172. *Id.* at 130–32.

173. *Id.* at 95.

174. *Id.* at 135.

175. Christine B. Williams, et. al, *The Formation of Inter-Organizational Information Sharing Networks in Public Safety: Cartographic Insights on Rational Choice and Institutional Explanations*, 14 INFO. POLITY 13, 15 (2009). In addition to ARJIS, other examples of such entities operating at the regional level include the San Francisco area's Bay Area Urban Areas Security Initiative (UASI), a regional authority with voting representation from the three major cities and

The history of ARJIS helps explain why it is an especially obscure component of SANDAG. While ARJIS is now part of SANDAG, that was not always the case. Established as a regional organization in 1980, ARJIS was a coalition of law enforcement agencies with a board of directors staffed with a member of each agency.[176] In 2004, ARJIS was consolidated into SANDAG to achieve greater administrative efficiency.[177] The ARJIS board was reconstituted as SANDAG's Advisory Committee (generally referred to as the "Public Safety Committee"), and its membership expanded to include some elected representatives.[178] However, it was still an outlier among SANDAG's committees, where usually only elected representatives are permitted to vote. At the time of the events described below, the Public Safety Committee's voting membership consisted of six elected representatives and nine law enforcement representatives.[179]

Even this makes elected representatives look more involved than they really were. According to an internal SANDAG audit, the Public Safety Committee's "primary function is to serve in an advisory capacity."[180] The real power rested with the Public Safety Committee's subcommittee, the Chiefs'/Sheriff's Management Committee.[181] Every member of the Chiefs'/Sheriff's Management Committee, except the San Diego district attorney, was a law enforcement officer of some type.[182]

---

some of the counties surrounding San Francisco Bay that allocates federal UASI funds to area governments. *See About the Bay Area UASI*, BAY AREA URBAN AREAS SEC. INITIATIVE, http://www.bayareauasi.org/about-us [https://perma.cc/6FBY-Q79Y]; *Programs*, BAY AREA URBAN AREAS SEC. INITIATIVE, http://bayareauasi.org/programs [https://perma.cc/D5E9-GRTC]. The DHS requires that cities and counties take a regional approach to implementation of the UASI program, which has led to the formation of various regional law enforcement authorities that exist for the purpose of expending federal UASI funds. *See, e.g.*, Memorandum of Agreement for Participating Orlando Urban Area Security Initiative (UASI) Agencies (July 29, 2010), http://www.edocs.ci.orlando.fl.us/asv/paperlessagenda.nsf/60f252ae0a55937d852573f50052d808/3e913aa55b621811852577a600515ebb/$FILE/UASI_FY_2009_MOA_OCSO0001.pdf [https://perma.cc/RJS4-EUWE]. Another is the Capital Wireless Information Net (CapWIN), a cross-jurisdictional organization of public safety entities in the greater Washington, D.C., area. *See About CapWIN*, UNIV. OF MD. A. JAMES CLARK SCH. OF ENG'G, http://www.capwin.org/about [https://perma.cc/UH3P-B9FN].

176. Tyworth, *supra* note 167, at 90–92.

177. *Id.* at 92–93.

178. *Id.* at 93.

179. SANDAG Board Agenda, July 11, 2014, *supra* note 167.

180. Tyworth, *supra* note 167, 93–94.

181. *See id.* at 94.

182. *See, e.g.*, SAN DIEGO ASS'N OF GOV'TS, CHIEFS'/SHERIFF'S MANAGEMENT COMMITTEE AGENDA 7 (Apr. 1, 2015), http://sandag.org/uploads/meetingid/meetingid_4124_18902.pdf

2. The Controversy Over San Diego's Facial Recognition Technology

In 2013, the Electronic Frontier Foundation (EFF) and Center for Investigative Reporting (CIR) jointly revealed that ARJIS had deployed facial recognition technology.[183] The technology allows officers on patrol to use a tablet to snap a photo of a person they encounter.[184] It then compares the photo to a database of photos of individuals who have been booked in the San Diego area.[185] Within ten to fifteen seconds,[186] the system displays a photo lineup of up to ten possible matches in ranking order of confidence.[187] If the officer confirms there is a match, the system automatically queries a variety of additional databases (e.g., a database of county warrants, DMV data) and returns information regarding the person's identity and criminal history.[188] EFF and CIR reported that twenty-five law enforcement agencies operating in the San Diego area, including local police departments and federal law enforcement agencies, were using the system.[189]

The widespread availability of facial recognition technology could transform the ordinary, daily experience of being in public. In the hands of private citizens, individuals would be able to identify and pull up

---

[https://perma.cc/A2XG-928A] (attendance sheet for March 4, 2015 meeting listing committee members and voting statuses).

183. *See* Jennifer Lynch & Dave Maass, *San Diego Gets in Your Face with New Mobile Identification System*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Nov. 7, 2013), https://www.eff.org/deeplinks/2013/11/san-diego-gets-your-face-new-mobile-identification-system [https://perma.cc/R6FF-DB8B]; Ali Winston, *Facial Recognition, Once a Battlefield Tool, Lands in San Diego County*, CTR. FOR INVESTIGATIVE REPORTING (Nov. 7, 2013), http://cironline.org/reports/facial-recognition-once-battlefield-tool-lands-san-diego-county-5502 [https://perma.cc/JLW9-CLZ2].

184. *See* Lynch & Maass, *supra* note 183; Winston, *supra* note 183.

185. *See* Lynch & Maass, *supra* note 183; Winston, *supra* note 183.

186. *See* AUTOMATED REG'L JUSTICE INFO. SYS., ACCEPTABLE USE POLICY FOR FACIAL RECOGNITION 3 (2015), http://www.arjis.org/RegionalPolicies/ARJIS%20Facial%20Recognition%20AUP%20-%20Approved%20-%20Rev150213.pdf [https://perma.cc/B86U-WN7X] [hereinafter ARJIS ACCEPTABLE USE POLICY FOR FACIAL RECOGNITION].

187. *Meetings Audio Archives, Public Safety Committee*, SAN DIEGO ASS'N OF GOV'TS (Jan. 18, 2013), http://sandag.org/index.asp?fuseaction=meetings.sc&mid=PSC011813 (audio at 0:43:15) (agenda item no. 7, "Facial Recognition in the Field") (last visited Dec. 17, 2016) (statements of ARJIS Program Manager Lloyd Muenzer and San Diego County Sheriff's Department Deputy Darrin Peralta).

188. AUTOMATED REG'L JUSTICE INFO. SYS., TACIDS: TACTICAL IDENTIFICATION SYSTEM USING FACIAL RECOGNITION 4 (2013) [hereinafter TACIDS], https://www.eff.org/document/11-tacids-final-report-final [https://perma.cc/JGW3-QV27] (final report submitted to U.S. Department of Justice).

189. *See* Lynch & Maass, *supra* note 183; Winston, *supra* note 183.

public information about strangers in their vicinity, and brick and mortar stores would be capable of identifying customers as soon as they crossed the threshold. The impact on law enforcement agents is also potentially significant; agents would be able to identify those they encountered and would be able to pull up their criminal histories, warrant information and threat assessment scores.[190]

When ARJIS first deployed facial recognition technology, the use of this technology was constrained by the way the system was designed rather than through a written use policy. The system only compares the images officers take to booking photos, and, if there is a match, officers have the option to display the subject's criminal history and any outstanding arrest warrants.[191] The guideline appears to have been that officers could deploy the technology on anyone they stopped as well as anyone who consented.[192]

ARJIS's development of facial recognition stretches back to at least 2007. In that year, the DOJ awarded ARJIS a $418,000 grant through a program to promote "information-led policing research, technology

190. For example, police in Fresno rely on a program to assign individuals they encounter threat assessment scores based on reviews of data on these individuals from "arrest reports, property records, commercial databases, deep Web searches and . . . social-media postings." Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score,'* WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html [https://perma.cc/K747-3BT5].

191. ARJIS could have built a more sweeping tool, for example by comparing photos officers take to those contained in the California Department of Motor Vehicles photo database, which would have allowed police officers to identify a broader range of people. The fact that ARJIS did not do that is an example of how a tool can be designed to protect privacy. For an exploration of privacy by design, see ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES, https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf [https://perma.cc/ET5F-R25A]; Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1436–38 (2000) ("[L]aw can and should establish a new set of institutional parameters that supply incentives for the design of privacy-enhancing technologies to flourish."); Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1413 (2011) ("This Article seeks to clarify the meaning of privacy by design and to suggest how privacy officials might develop appropriate regulatory incentives that offset the certain economic costs and somewhat uncertain privacy benefits of this new approach.").

192. *Compare Meetings Audio Archives, Public Safety Committee*, SAN DIEGO ASS'N OF GOV'TS, at 0:59:05 (Jan. 18, 2013), http://sandag.org/index.asp?fuseaction=meetings.sc&mid=PSC011813 (agenda item no. 7, "Facial Recognition in the Field") (last visited Dec. 17, 2016) (discussion of when use of facial recognition tool is permissible in 2013) *with* ARJIS ACCEPTABLE USE POLICY FOR FACIAL RECOGNITION, *supra* note 186, at 2 (2015 policy which more extensively limited the use of facial recognition technology).

development, testing and evaluation."[193] ARJIS dubbed its facial recognition program the Tactical Identification System, or TACIDS.[194] The project proved technically complex and its development stretched on for several years.[195] In 2011, ARJIS appears to have deployed TACIDS for the first time.[196]

Although it took ARJIS years to develop TACIDS, it used this time to conduct research with the goal of identifying an effective product.[197] ARJIS consulted with the FBI's Biometric Center of Excellence and the California Department of Justice, as well as local user groups.[198] It identified numerous vendors of facial recognition technology that catered to law enforcement customers and vetted them thoroughly through use of questionnaires, on-site visits, and product demonstrations.[199]

While the technical complexities of TACIDS may have slowed its rollout, it quickly proved to be popular once it got into law enforcement agents' hands. By 2013, when EFF and CIR alerted the public to the program, there were 178 tablets with facial recognition capability in use by officers, and other officers regularly emailed photos to those with tablets so the photos could be run through the system.[200] ARJIS staff members started to think bigger and bolder. They began to contemplate applying the software to fixed cameras from court buildings and public

193. *See NIJ Awards in FY 2007*, NAT'L INST. OF JUSTICE (Aug. 8, 2008), http://www.nij.gov/funding/awards/pages/2007.aspx [https://perma.cc/7UHK-WMWM] (grant no. 2007-RG-CX-K001).

194. *See id.*; Letter from Regina B. Schofield, Assistant Attorney Gen., Department of Justice, to Dr. Pamela Scanlon, Automated Regional Justice Information System 1 (Sept. 13, 2007), https://www.eff.org/files/2013/11/07/01_-_tacids_award_letter_2.pdf [https://perma.cc/9PVX-DUSL] (confirming the award of the grant from the Department of Justice); AUTOMATED REG'L JUSTICE INFO. SYS., NAT'L INST. OF JUSTICE FY07 FINAL PROPOSAL: INFORMATION-LED POLICING: TACTICAL IDENTIFICATION SYSTEM (TACIDS) 4 (2007), https://www.eff.org/files/2013/11/07/02_-_5214-mandatory_tacids_-_final_2.pdf [https://perma.cc/TFQ9-7SV8].

195. *See* NAT'L INST. OF JUSTICE, GMS PROGRESS REPORTS—COMPILATION (2012), https://www.eff.org/files/2013/11/07/12_-_tacids_report_summary_2.pdf [https://perma.cc/DN2G-V5ZG] (semi-annual TACIDS status reports for National Institute of Justice from Oct. 1, 2007 through June 30, 2012).

196. TACIDS, *supra* note 188, at 29–33.

197. *Id.* at 7–17.

198. *Id.* at 7–9.

199. *Id.* at 10–16.

200. *See* Lynch & Maass, *supra* note 183. ARJIS leveraged Samsung devices (250 tablets and 50 smartphones) obtained for Terrorism Liaison Officers. *See* SAN DIEGO ASS'N OF GOV'TS, PUBLIC SAFETY COMMITTEE AGENDA (Jan. 18, 2013), http://sandag.org/uploads/meetingid/meetingid_3535_15446.pdf [https://perma.cc/94R2-TF5E] (discussing agenda item no. 7, "Facial Recognition in the Field").

transportation facilities, presumably to screen for wanted persons.[201] An ARJIS staffer stated that "the facial recognition software is not currently used as surveillance as yet, but is in future plans."[202]

EFF's and CIR's investigations caused SANDAG board members to become concerned about the ARJIS facial recognition program.[203] At around the same time, SANDAG was sued over a different ARJIS surveillance program, the use of automatic license plate readers to capture and store the time and location of vehicles observed around the city.[204] These developments sparked an awakening for SANDAG board members, who realized they did not understand what ARJIS did or how it was managed.[205] Members reported being only dimly aware of the license plate and facial recognition programs, which they found alarming given that the entity they were charged with running had been sued over the former and was under public scrutiny because of the latter. Having been caught off guard, some SANDAG board members were concerned that decisions about SANDAG's law enforcement activities that implicated public policy were not flowing upward to the board.[206]

Lemon Grove Mayor Mary Sessom instituted a review of the Public Safety Committee and the programs it oversees for the SANDAG board.[207] The review concluded that the Public Safety Committee was

---

201. *See* SAN DIEGO ASS'N OF GOV'TS, *supra* note 200.

202. SAN DIEGO ASS'N OF GOV'TS, CHIEFS'/SHERIFF'S MANAGEMENT COMMITTEE AGENDA 6 (Apr. 3, 2013), http://www.sandag.org/uploads/meetingid/meetingid_3671_15747.pdf [https://perma.cc/8WGQ-CBNA] (statement of ARJIS staff member Lloyd Muenzer).

203. *See Meetings Audio Archives, Board of Directors*, SAN DIEGO ASS'N OF GOV'TS, at 0:08:38 (July 11, 2014), http://sandag.org/index.asp?fuseaction=meetings.sc&mid=BOD071114 (last visited Dec. 17, 2016) [hereinafter *SANDAG Board of Directors July 11, 2014*] (statement of Lemon Grove Mayor Mary Sessom) (discussing agenda item no. 2, "Public Safety Program at SANDAG").

204. *See* Lee Ann O'Neal, *SANDAG Knows Where You've Been*, SAN DIEGO UNION-TRIB. (June 17, 2013), http://www.utsandiego.com/news/2013/jun/17/license-plate-reader-LPR-san-diego-surveillance/ [https://perma.cc/CZ3W-KYU6]. The agency had amassed a database of some 32 million plate hits, which were accessible to agents throughout the region. The lawsuit did not allege that the plate reader program was unlawful. Rather, a private citizen sued ARJIS under the public records act, demanding to see what records it was keeping on the movements of his vehicle.

205. *See SANDAG Board of Directors July 11, 2014*, *supra* note 203.

206. According to SANDAG Board member Ron Roberts, a member of the San Diego County Board of Supervisors, "as a member here, it would have been impossible to know what was going on. [The Board] was buried in the budgets . . . it would have taken years of research to find exactly what was being done, what was money being spent on, to what extent were there policies that were guiding this." *SANDAG Board of Directors July 11, 2014*, *supra* note 203, at 1:23:37.

207. *See Meetings Audio Archives, Public Safety Committee*, SAN DIEGO ASS'N OF GOV'TS , at 1:06:17, 1:08:06 (June 20, 2014) http://www.sandag.org/index.asp?fuseaction=meetings.sc&mid=PSC062014 (agenda item no. 7, "Public Safety at SANDAG—Policy Review") (containing statements of SANDAG Strategic Advisor Diane Eidam and Lemon Grove Mayor Mary Sessom) (last visited Dec. 17, 2016).

out of step with SANDAG's overall structure.[208] Other SANDAG committees reserved their voting membership almost exclusively to elected representatives, but unelected officials, primarily from law enforcement, controlled nine of the Public Safety Committee's fifteen positions.[209] The committee was also unique in creating a standing subcommittee—the Chiefs'/Sheriff's management committee—"that is accorded more responsibility and authority than the Policy Advisory Committee itself."[210] The report concluded that "current policy and practice do not provide a mechanism to ensure that the [Public Safety Committee] and [SANDAG] Board have the opportunity to weigh in on public policy issues related to ARJIS."[211] To rectify matters, the review recommended reallocating votes so that elected officials had a 6-5 majority on the Public Safety Committee and also requiring that the SANDAG board approve all applications ARJIS wished to submit for federal grant funds.[212]

The SANDAG board did approve the grant application recommendation.[213] But it rejected a 6-5 vote split, and instead adopted a 6-6 allocation of votes between elected representatives and law enforcement agents.[214] Chula Vista Police Chief David Bejarano, speaking on behalf of the San Diego County Chiefs and Sheriffs Association, stated that preserving law enforcement agents' control would enable them to "use our hundreds of years of experience . . . as subject matter experts . . . so we continue to have, again, the best operational practices, the best policy as we move forward in maximizing our technology."[215] In addition, law enforcement agents framed the issue as one of equality between themselves and elected representatives. As Bejarano put it, "We simply want an equal voice at the table."[216] This

208. *See id.*

209. SANDAG Board Agenda, July 11, 2014, *supra* note 167 (Public Safety Program Review).

210. *Id.* at 13.

211. *Id.* at 14.

212. *Id.*; *SANDAG Board of Directors July 11, 2014*, *supra* note 203, at 1:21:44 (statement of Lemon Grove Mayor Mary Sessom).

213. SAN DIEGO ASS'N OF GOV'TS, BOARD OF DIRECTORS AGENDA (Sept. 26, 2014), http://sandag.org/uploads/meetingid/meetingid_3863_18225.pdf [https://perma.cc/VQ7Z-LRK5] (agenda item no. 14-09-18, "Public Safety at SANDAG—Policy Review") (recommending reducing the number of unelected members so that it was equal to the number of elected members).

214. *See id.*

215. *SANDAG Board of Directors July 11, 2014*, *supra* note 200, at 1:02:13 (statement of David Bejarano).

216. *Meetings Audio Archives*, *Executive Committee*, SAN DIEGO ASS'N OF GOV'TS, at 0:40:52 (Sept. 12, 2014), http://www.sandag.org/index.asp?fuseaction=meetings.sc&mid=EC091214 (last visited Dec. 17, 2016).

view—that there should be equal numbers of votes for elected and unelected representatives—prevailed, although there were some dissenters. SANDAG board member and Escondido Mayor Sam Abed's comment was representative of the dissenters: "We are the elected officials. If we have to answer to our voters, then we have to be in charge of policy. We are not compromising with other elected officials. We are compromising with staff. This is a very fundamental institutional issue."[217]

Throughout the debate, no civil liberties groups or members of the public showed up to express their views. SANDAG officials seemed unaware that drawing on community expertise was even an option. When asked by one board member whether ARJIS had consulted with local civil liberties groups, Sessom stated: "This is a new, emerging field, and there's not a lot of privacy experts here."[218] (In fact, San Diego has a robust local ACLU affiliate.)[219] ARJIS staff said that instead of turning to civil liberties groups, they had relied on the International Association of Chiefs of Police and the DHS for guidance.[220]

In the wake of public attention to facial recognition technology and board members' concerns regarding oversight, ARJIS created, and the SANDAG board adopted, an acceptable-use policy for its facial recognition technology.[221] The policy's data handling provisions are reasonably protective of privacy, allowing for only data collection and retention necessary for the program to meet its specified purposes. The policy states that facial recognition should be used "for official law enforcement purposes only," and that "releasing data . . . for non-law enforcement purposes is prohibited."[222] It further specifies that the technology should only be used under two circumstances. First, it can be used to assist in the identification of individuals who have been detained based on reasonable suspicion and who do not have identification or

---

217. *Meetings Audio Archives, Public Safety Committee*, SAN DIEGO ASS'N OF GOV'TS , at 0:49:33, 1:08:06 (Sept. 26, 2014), http://www.sandag.org/index.asp?fuseaction=meetings.sc&mid=BOD092614 (last visited Dec. 17, 2016).

218. *SANDAG Board of Directors July 11, 2014*, *supra* note 201, at 1:14:15 (statement of Lemon Grove Mayor Mary Sessom).

219. *Cf. Board and Staff Information*, ACLU SAN DIEGO, https://www.aclusandiego.org/about-us/board-and-staff-information/ [https://perma.cc/M8HV-ZZE9] (illustrating staff size).

220. *SANDAG Board of Directors July 11, 2014*, *supra* note 201, at 1:14:46 (statement of Pam Scanlon).

221. SAN DIEGO ASS'N OF GOV'TS, BOARD OF DIRECTORS MEETING MINUTES 2 (Feb. 13, 2015), http://sandag.org/uploads/meetingid/meetingid_4066_19049.pdf [https://perma.cc/GDQ7-FPYB].

222. *See* ARJIS ACCEPTABLE USE POLICY FOR FACIAL RECOGNITION, *supra* note 186, at 3.

who appear to be using false identification.[223] Second, it can be used to identify individuals who are unable to identify themselves, such as deceased or incapacitated individuals.[224] The only data collected are the photos officers take, and those are deleted within twenty-four hours.[225] The policy is silent on the issue of sharing but, given the aggressive data deletion schedule, sharing with other agencies would be out of step with the general tenor of the policy.

In the meantime, the TACIDS user base continues to grow. By February 2015, there were approximately 800 registered TACIDS users representing twenty-eight law enforcement agencies.

3. Analysis of Surveillance Policy Making by the San Diego Association of Governments

In this case study, ARJIS's status as a regional law enforcement authority was a major reason why San Diego rolled out facial recognition technology in a non-transparent fashion. The public is largely ignorant of SANDAG's existence. The normal, everyday trappings of legislative oversight are absent: SANDAG board members hold their meetings in front of empty public galleries, without much press attention.

Federal funding made it unclear whose job it is to set a use policy for facial recognition technology. Options include the federal government (because it paid for the technology), SANDAG (because it received the funding and developed and promulgated the technology), and end user law enforcement agencies (because they deploy the technology in the field). In contrast to Seattle and Oakland, the federal government funded TACIDs through a program specifically designed for law enforcement, not national security purposes. This meant the goals of federal funders and the local grantee were aligned. The grant was designed to promote information-led policing, and that is exactly what ARJIS wanted to do.

This case study provides little in the way of lessons for increasing transparency and democratic accountability for surveillance policy making. Although SANDAG did take steps to increase its oversight of ARJIS, its governance limitations are fundamental and due to the structure of the organization.

---

223. *Id.* at 2.

224. *Id.* at 3.

225. *Id.* at 5.

D. Lessons from Case Studies

Collectively, the case studies contain lessons about the structural and institutional factors that lead to surveillance policy making by procurement. They also demonstrate the confusion federal spending programs can generate about who is responsible for policy decisions and some of the spillover effects the federal government's national security programs can have on more routine forms of policing. Finally, they point toward some ways to bring a greater measure of transparency and accountability to local surveillance policy making.

The three case studies reveal strikingly different ways that law enforcement agencies set surveillance policy without the meaningful involvement of elected representatives or members of the public. In Seattle, the police department was chronically unable or unwilling to bring city council members into the loop regarding its surveillance initiatives.[226] In Oakland, city staff diligently kept the city council apprised of its plans, but it took a few years for council members and members of the public to grasp what they were being told.[227] In San Diego, SANDAG's organizational structure left ARJIS largely unsupervised, an issue compounded by SANDAG also being comparatively remote from residents of the geographic area it serves.[228]

In all three cases, the federal government provided funding for surveillance technology acquisition but did not require that any guidelines be developed for protecting civil rights and liberties or that there be meaningful involvement by members of the public or elected representatives. This left elected representatives scrambling to impose such guidelines retroactively after programs became controversial.

Further, the case studies highlight the interplay between federal programs designed to enhance national security and more routine local law enforcement practices. In Seattle, the federal government's national security objectives were irrelevant to the local debate, which turned on the impacts of surveillance technology on day-to-day policing.[229] In Oakland, the federal government's national security objectives were an additional strike against the surveillance center.[230] By contrast, it is worth asking whether the alignment between DOJ's goal of promoting

226. *See supra* section II.A.2.

227. *See supra* section II.B.2.

228. *See supra* section II.C.2.

229. *See supra* section II.A.2.

230. *See supra* section II.B.2.

information-led policing and ARJIS's organizational mission contributed to the successful adoption of facial recognition technology.[231]

The case studies also suggest ways in which local surveillance policy can be made more transparent and accountable, but none is likely to be a global fix. A Seattle-style surveillance equipment ordinance will require law enforcement agencies to produce data management protocols and, as a result, think through key data management issues. Whether the process of obtaining council approval will be pro forma or will result in meaningful public engagement remains to be seen. The Oakland innovation of forming a privacy advisory committee is a viable solution for that community, but likely depends too heavily on the time and expertise of local residents to work in many other places. San Diego restored some measure of democratic control over ARJIS's surveillance initiatives, but SANDAG is so divorced from the population it is designed to serve that it is hard to see this as a substantial improvement in accountability.

III. BROADER IMPLICATIONS OF SURVEILLANCE POLICY MAKING BY PROCUREMENT FOR ACCOUNTABILITY

This Part explores the broader implications of the case studies. It first considers what factors are relevant to setting surveillance policy. Surveillance technology has the potential to enhance public safety but also poses risks to privacy and other civil liberties and rights.[232] Because benefits and costs are empirically uncertain and setting surveillance policy requires trading off incommensurable values, there is no uniform answer to how much or what type of surveillance is appropriate.[233] However, there is widespread agreement that deployment of surveillance technology ought to be governed by a policy setting out how the technology will be used and that such policies should address the key issues of data collection, retention, use, and sharing.[234] Thus, the fact that all three case studies resulted in the proliferation of surveillance technology ungoverned by such policies suggests a structural defect in how surveillance policy is set.

This Part then considers the implications of the case studies for how we think about accountability when the federal government encourages local surveillance without requiring adoption of use policies. The

231. *See supra* section II.C.2.

232. *See infra* section III.A.

233. *See infra* section III.A.

234. *See infra* notes 241–43 and accompanying text.

Supreme Court has privileged federal interventions in the form of conditional grants-in-aid over federal interventions that commandeer state and local officials precisely because of its view that spending programs do a better job of preserving clear lines of accountability.[235] But the case studies show that spending programs can generate considerable confusion over who is responsible for policy choices. This may be particularly true when the government creates policy voids by incompletely addressing a policy matter.

Finally, this Part situates the case studies within the federal government's broader efforts to work more closely with local law enforcement agencies to prevent, investigate, and respond to acts of terror.[236] Particularly given the dual-purpose nature of much surveillance technology, these initiatives tend to bleed over into how local officers conduct routine policing.[237] This suggests that any cost-benefit analysis of the federal government's national security programs should consider not only their impact on national security but also on law enforcement, including transparency and accountability.

A. Considerations for Selecting Surveillance Policy

Optimizing surveillance policy requires assessing the capacity of technology to aid in the prevention and detection of criminal activity while identifying possible harms to privacy, free speech, and other civil rights and liberties. While there is no one-size-fits-all solution to how a surveillance technology should be utilized, every surveillance scheme raises the same basic questions about what data should be collected, how long it should be stored, what uses should be made of it, and with whom it should be shared. Thus, while surveillance outcomes may be heterogeneous, the basic factors that every policy maker should consider are the same.

Surveillance technology has many potential benefits for advancing public safety. For example, technologies facilitating data collection can gather information relevant to investigating crime, as in the case of wiretapping the telephone of someone suspected of illegal activity.[238] The value of the large-scale collection of data on individuals' activities made possible by modern computer-driven technology is less clear. Law

---

235. *See infra* section III.B.

236. *See infra* section III.C.

237. *See infra* section III.C.

238. *See, e.g.*, Katz v. United States, 389 U.S. 347, 348 (1967) (concerning electronic surveillance of a telephone booth).

enforcement agencies assert that large-scale data collection can play a role in investigating criminal activity, including terrorism, or in apprehending the perpetrators of such activity. Even data gathered with no immediate suspect or crime in mind can be useful in some future investigation. For example, New Jersey's attorney general claimed that "careful analysis of stored [automated license plate reader] data can . . . be used to detect suspicious activities that are consistent with the *modus operandi* of criminals."[239] In addition, deploying surveillance technology in a visible manner may deter crime.[240] For example, a prominent study in San Francisco demonstrated that the deployment of surveillance cameras resulted in a substantial decline in property crimes.[241] The impact was on larceny theft; the deployment of surveillance cameras had no impact on violent crimes.[242]

Against these benefits of surveillance technology and large-scale data collection, it is necessary to consider their potential to cause harm. Neil Richards has argued that surveillance can "chill the exercise of . . . civil liberties," particularly by threatening "intellectual privacy."[243] He also

---

239. OFFICE OF THE ATTORNEY GEN., STATE OF N.J., DIRECTIVE NO. 2010-5, 2 (2010), http://www.state.nj.us/lps/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf [https://perma.cc/W5EM-SN9Q] (italics in original). The Texas Department of Public Safety likewise asserted that stored license plate reader data "will enable various forms of crime analysis; for example, DPS will be able to trace the movements of felony vehicles over time (in hindsight) that travel specific routes from the border on a regular basis and help determine patterned movements associated with drugs/money/human trafficking." TEX. DEP'T OF PUB. SAFETY, PRIVACY IMPACT ASSESSMENT FOR THE COLLECTION, STORAGE, MANAGEMENT AND USE OF AUTOMATED LICENSE PLATE READER DATA 3, 26 (2014), https://www.txdps.state.tx.us/administration/crime_records/pages/LPRPIA.pdf [https://perma.cc/9QA4-PNZT].

240. *See, e.g.*, JENNIFER KING, DEIRDRE K. MULLIGAN & STEVEN RAPHAEL, U.C. BERKELEY CTR. FOR INFO. TECH. IN THE INTEREST OF SOC'Y, REPORT: THE SAN FRANCISCO COMMUNITY SAFETY CAMERA PROGRAM—AN EVALUATION OF THE EFFECTIVENESS OF SAN FRANCISCO'S COMMUNITY SAFETY CAMERAS 11–12 (2008); *The Effect of CCTV on Public Safety: Research Roundup*, JOURNALIST'S RESOURCE (Feb. 11, 2014), http://journalistsresource.org/studies/government/criminal-justice/surveillance-cameras-and-crime [https://perma.cc/VLV9-GSRW] (canvassing scholarly evaluations of the deterrent effect of surveillance cameras in public places).

241. KING ET AL., *supra* note 238, at 11–12.

242. *Id.*

243. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013). *But see* Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 265, 269 (2013) (criticizing Richards's approach as "too narrow" and contending that the real danger comes not just from diminishing the zone of intellectual privacy but from surveillance of many different types of activities where that surveillance is "broad, indiscriminate, and continuous"). *See also* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013) (elaborating on their theory that it is the quantity of data that is collected that causes harm); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008) (exploring the importance of intellectual privacy as a precondition for free expression).

contends that it can skew the balance of power between those engaged in surveillance and their targets, increasing the risk that targets will be subjected to "discrimination, coercion, and the threat of selective enforcement."[244] Focusing in on a narrower aspect of surveillance, Katherine J. Strandburg has emphasized the way surveillance of relationships, particularly emergent relationships formed online, threatens First Amendment-protected associational activity.[245] Practitioners have identified similar harms. For example, the International Association of Chiefs of Police stated, "the risk is that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance."[246] Surveillance technology may go beyond deterring conduct that is unlawful and inhibit or deter the legal and beneficial activities that citizens conduct in a free society.

The possibility that people will be targeted because of their political or religious beliefs is not merely theoretical.[247] In the mid-2000s, for

244. Richards, *The Dangers of Surveillance*, *supra* note 243, at 1935.

245. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 748 (2008) ("First Amendment freedom of association guarantees must provide an additional check, distinct from the Fourth Amendment's protections from unreasonable search and seizure, on overreaching relational surveillance potential."). Other scholars have also articulated the harm to First Amendment-protected activities that surveillance can cause. *See, e.g.*, Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 114 (2007) ("First Amendment activities are implicated by a wide array of law enforcement data-gathering activities."). More broadly, theories of privacy harm abound in legal scholarship. *See* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343 (2015) (contending that privacy harm results when previously obscure information becomes readily accessible); Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113 (2015) (asserting that privacy harm occurs when new technologies divulge information that was private previously, and that individuals react by modifying their behavior to achieve the prior level of disclosure); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 143 (2004) (positing that "a privacy violation has occurred when either contextual norms of appropriateness or norms of flow have been breached"); Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 299–303 (2011) (identifying myriad harms that mass surveillance can cause, including the likelihood of false positives, a greater risk of discrimination and profiling, and more potential for police corruption).

246. INT'L ASS'N OF CHIEFS OF POLICE, PRIVACY IMPACT ASSESSMENT REPORT FOR THE UTILIZATION OF LICENSE PLATE READERS 13 (2009), http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf [https://perma.cc/8YXW-EYPG].

247. In addition to the recent examples discussed in the accompanying text, there are historical examples as well. Handschu v. Special Servs. Div., 605 F. Supp. 1384, 1388 (S.D.N.Y. 1985), *aff'd*, 787 F.2d 828 (2d Cir. 1986) involved a challenge to various surveillance and investigative practices directed at political organizations by the New York City Police Department (NYPD) in the 1970s. The case was settled with a consent decree entered in 1985 in which the NYPD was prohibited from investigating political and religious organizations and groups unless there was "specific

example, the Maryland State Police engaged in surveillance of political groups ranging from Amnesty International to advocates of bike lanes, a practice the governor condemned as "undemocratic" and that the Maryland State Police later acknowledged was a mistake.[248] Human rights advocates and civil liberties groups criticized the New York Police Department's extensive surveillance of political protestors during Occupy Wall Street.[249] In Birmingham, United Kingdom, law enforcement agents installed a network of 200 cameras in predominantly Muslim communities on the pretense that it was a crime prevention measure.[250] When members of the public discovered that the cameras were actually part of a covert anti-terrorism initiative, many expressed concerns about discriminatory targeting based on religion.[251]

In addition to harms that result from official policy or practice, there is always the possibility of abusive use of surveillance equipment by individual officers for their own reasons. There are numerous examples of police officers using department GPS devices to track the vehicles of ex-girlfriends.[252] Access to databases can also be abused. In Minneapolis, a female police officer obtained a $1 million settlement

---

information" that the group was linked to a crime that had been committed or was about to be committed. *Handschu*, 605 F. Supp. at 1420–21. Another example is the Church Committee revelations. In 1975, the Church Committee, chaired by Senator Frank Church, held a series of hearings and published fourteen reports as it investigated intelligence operations by the CIA, NSA, and FBI, including attempts to assassinate foreign leaders, spying on Martin Luther King, Jr., and monitoring the political activities of other U.S. citizens. *See generally* S. REP. NO. 94-755, at pt. 3 (1976).

248. Lisa Rein & Josh White, *More Groups Than Thought Monitored in Police Spying*, WASH. POST, Jan. 9, 2009, at A01, http://www.washingtonpost.com/wp-dyn/content/story/2009/01/03/ST2009010302013.html [https://perma.cc/D66Z-EJYT].

249. *See, e.g.*, THE GLOB. JUSTICE CLINIC (N.Y.U. SCH. OF LAW) & THE WALTER LEITNER INT'L HUMAN RIGHTS CLINIC AT THE LEITNER CTR. FOR INT'L LAW AND JUSTICE (FORDHAM LAW SCH.), SUPPRESSING PROTEST: HUMAN RIGHTS VIOLATIONS IN THE U.S. RESPONSE TO OCCUPY WALL STREET 93–98 (2012), http://chrgj.org/wp-content/uploads/2012/10/suppressingprotest.pdf [https://perma.cc/KPV6-BB2X].

250. *See* Pete Fussey & Jon Coaffee, *Urban Spaces of Surveillance*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES 201, 207 (Kirstie Ball et al. eds., 2012); Paul Lewis, *CCTV Aimed at Muslim Areas in Birmingham to be Dismantled*, THE GUARDIAN (Oct. 25, 2010, 4:45 PM), http://www.guardian.co.uk/uk/2010/oct/25/birmingham-cctv-muslim-areas-surveillance [https://perma.cc/WSZ5-Q58S].

251. *See* Paul L. Lewis, *Surveillance Cameras Spring Up in Muslim Areas–the Targets? Terrorists*, THE GUARDIAN (June 4, 2010), https://www.theguardian.com/uk/2010/jun/04/birmingham-surveillance-cameras-muslim-community [https://perma.cc/CA2E-8NA5].

252. *See, e.g.*, Robert J. Lopez, *Officer Accused of Hiding GPS Device in Woman's Car*, L.A. TIMES (Apr. 22, 2010, 4:40 PM), http://latimesblogs.latimes.com/lanow/2010/04/costa-mesa-police.html [https://perma.cc/J4MA-WR3P].

after more than 400 of her colleagues accessed her driver's license record out of pure voyeurism.[253]

There is no single solution to whether and how a particular surveillance technology should be deployed. A high-crime community might tolerate more surveillance than a low-crime community. A community with a strong civil libertarian streak might prefer to face a greater safety risk than to restrict civil liberties. A community such as Oakland, which holds its police department in low regard, might be less willing than other communities to entrust its police department with potentially invasive surveillance technology.[254]

However, every data collection scheme implicates the same questions about data collection, retention, use, and sharing. What data should be collected? How long should the data that is collected be stored? What uses of stored data should be allowed? With whom should data be shared and on what terms? The importance of these basic questions to any data management scheme is broadly recognized.[255] For example, they are at the heart of the Fair Information Practices, "a set of internationally recognized practices for addressing the privacy of information about individuals."[256] They also form the core of the Privacy Act, which controls the collection, retention, use, and sharing of information about

253. Kim Zetter, *Female Cop Gets $1 Million After Colleagues Trolled Database to Peek at Her Pic*, WIRED (Nov. 5, 2012, 4:02 PM), http://www.wired.com/2012/11/payout-for-cop-database-abuse/ [https://perma.cc/FAZ7-T4KG].

254. *See* Ann Althouse, *The Vigor of Anti-Commandeering Doctrine in Times of Terror*, 69 BROOK. L. REV. 1231, 1259–60 (2004) ("There are varying local preferences about the balance between individual liberties and actions government might take to increase the physical security of its citizens. There is also variation in how much local citizens desire to exercise a particular liberty and how serious the threat to physical safety in their area is.").

255. *See generally* ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2015), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf [https://perma.cc/E538-X9QU]. The Fair Information Practices include additional elements, but some of them are a poor fit for the law enforcement context. For example, they state that data "should be obtained by lawful and fair means and, where appropriate, *with the knowledge or consent of the data subject.*" *OECD Privacy Principles*, OECD, http://oecdprivacy.org/ [https://perma.cc/4AYY-PX7X] (emphasis added). Needless to say, the government's interest in enforcing the criminal code would often be frustrated by requiring the government to obtain an investigative target's consent. Also, some scholars use slightly different labels to capture the core data management concepts, or break them down into more or fewer elements. *Compare* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1112 (2016) (referencing "collection, access, sharing, retention, and use") *with* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) (discussing "collection, use, and disclosure"). This does not appear to be a disagreement about what elements are important. Rather, the term "use" is sufficiently broad that it can include the concepts of retention and access. How granularly to break down the core data management concepts depends on an author's purpose.

256. GELLMAN, *supra* note 255, at 1.

individuals that is maintained in systems of records by federal agencies.[257] Thus, while surveillance policy outcomes may vary from community to community, the process by which surveillance policy is set should always involve consideration of the same factors. Yet in all three case studies, the federal government's decision to fund surveillance technology without requiring or encouraging adoption of a use policy had the practical result of no such use policy being promulgated. This in turn suggests that there is a structural flaw in how we are setting surveillance policy in this context.

B. Accountability and Levels of Government

In the case studies, the fact that the federal government funded acquisition of surveillance technology but was silent on protections for civil rights and liberties created genuine confusion over which elected officials bore ultimate responsibility for how such technology would be used. This observation is important because the primary reason the United States Supreme Court has privileged spending programs over initiatives that "commandeer" sub-federal officials is because of its assessment that spending programs do a better job of preserving clear lines of accountability. The case studies cast doubt on whether this is descriptively accurate, reinforcing existing scholarship that has made this point in other contexts or in more abstract terms.

The Supreme Court has held that the structural protections of the Constitution forbid Congress from commandeering sub-federal officials. The prohibition is absolute: "[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."[258] By contrast, Congress enjoys wide latitude to influence state and local actions by placing conditions on grants-in-aid to states. It can spend money in any area that promotes the general welfare, subject to a small number of modest restrictions: conditions on grants must be unambiguous, related to the federal interest in a national project or program, and must not induce the states to act unconstitutionally.[259] Moreover, these programs must not cross the "point at which pressure turns into compulsion."[260]

---

257. Privacy Act of 1974, 5 U.S.C. § 552a (2012); *see also id.* §§ 552a(e)(1)–(2) (imposing limitations on data collection, retention, and use); § 552a(b) (imposing limitations on data sharing).

258. Printz v. United States, 521 U.S. 898, 935 (1997).

259. South Dakota v. Dole, 483 U.S. 203, 207–08 (1987).

260. Steward Machine Co. v. Davis, 301 U.S. 548, 590 (1937).

Until its recent ruling invalidating a portion of the Affordable Care Act, the Court had never determined that a federal grant was impermissibly coercive.[261]

According to the Court, conditional spending is preferable to commandeering because spending programs preserve local political processes: "the residents of the State retain the ultimate decision as to whether or not the State will comply."[262] Thus, "[i]f a state's citizens view federal policy as sufficiently contrary to local interests, they may elect to decline a federal grant."[263] This, in turn, promotes accountability: "[w]here Congress encourages state regulation rather than compelling it, state governments remain responsive to the local electorate's preferences; state officials remain accountable to the people."[264] By contrast, "where the Federal Government directs the States to regulate, it may be state officials who will bear the brunt of public disapproval, while the federal officials who devised the regulatory program may remain insulated from the electoral ramifications of their decision."[265]

Some scholars have criticized the Court's accountability-based distinction between commandeering and spending, suggesting that if obscuring accountability is a problem, it "seems to condemn not merely federal laws that commandeer state or local services but also even *voluntary* intergovernmental cooperation."[266] Others dispute that

---

261. Nat'l Fed'n of Indep. Bus. v. Sebelius, ___ U.S. ___, 132 S. Ct. 2566, 2630 (2012) (Ginsburg, J., concurring in part and dissenting in part) ("The Chief Justice therefore—*for the first time ever*—finds an exercise of Congress' spending power unconstitutionally coercive." (emphasis in original)). For a discussion of the impact of National Federation of Independent Business on the federal government's spending power, see generally Lynn A. Baker, *The Spending Power After* NFIB v. Sebelius, 37 HARV. J.L. & PUB. POL'Y 71 (2014).

262. New York v. United States, 505 U.S. 144, 168 (1992).

263. *Id.*

264. *Id.; see also Nat'l Fed'n of Indep. Bus.*, 132 S. Ct. at 2602 ("Permitting the Federal Government to force the states to implement a federal program would threaten the political accountability key to our federal system."); *id.* at 2660 (Scalia, J., dissenting) ("Congress effectively engages in this impermissible compulsion when state participation in a federal spending program is coerced, so that the States' choice whether to enact or administer a federal regulatory program is rendered illusory.").

265. *New York*, 505 U.S. at 169. Some scholars question whether commandeering poses accountability problems. *See, e.g.*, Neil S. Siegel, *Commandeering and Its Alternatives: A Federalism Perspective*, 59 VAND. L. REV. 1629, 1632 (2006) ("[I]t seems likely that citizens who pay attention to public affairs and who care to inquire will be able to discern which level of government is responsible for a government regulation, and citizens who do not care to inquire may be largely beyond judicial or political help on the accountability front.").

266. Roderick M. Hills, Jr., *The Political Economy of Cooperative Federalism: Why State Autonomy Makes Sense and "Dual Sovereignty" Doesn't*, 96 MICH. L. REV. 813, 826 (1998) (emphasis in original); *see also* Vicki C. Jackson, *Federalism and the Uses and Limits of Law:*

spending programs can create meaningful accountability problems.[267] The case studies provide reason to side with the former group. Putting doctrine to the side for a moment, it is worth thinking through who was responsible for surveillance policy in the case studies. The federal government allocated millions of dollars for surveillance equipment acquisition but did not require anyone to think through key questions of data management. Local law enforcement agencies took the money, but also did not devise a data management plan. Local elected officials signed off formally, but with no or only a dim understanding of what the law enforcement agency it supervised was acquiring.

Which elected officials are to blame for the fact that no one thought through basic questions of data collection, retention, use, and sharing? Federal officials, because the federal government appropriated the money and designed the procedures through which localities could elect to participate?[268] Local elected officials, because they signed off on acquisition of the technologies? Both? Neither?[269]

Printz *and Principle?*, 111 HARV. L. REV. 2180, 2201–03 (1998) (pointing out that conditional spending programs can also be confusing for voters); Siegel, *supra* note 265, at 1681 ("Nor is it apparent generally that commandeering generates insurmountable accountability concerns, or that preemption, conditional non-preemption, and conditional federal spending avoid similar accountability problems."); Edward A. Zelinsky, *Accountability and Mandates: Redefining the Problem of Federal Spending Conditions*, 4 CORNELL J.L. & PUB. POL'Y 482, 483 (1995) ("Federal spending conditions tend to diffuse responsibility between Washington and the states, leaving the political system less monitorable and accountable than it should be."); Rebecca E. Zietlow, *Federalism's Paradox: The Spending Power and Waiver of Sovereign Immunity*, 37 WAKE FOREST L. REV. 141, 190 (2002) ("The reason for the anti-commandeering rule was the Court's fear that commandeering state officials would cause a lack of accountability and confuse state voters . . . . Yet conditional funding arguably creates the same concern about accountability since states agree to comply with conditions beyond their control in order to receive federal funds.").

267. Samuel R. Bagenstos, *The Anti-Leveraging Principle and the Spending Clause After* NFIB, 101 GEO. L.J. 861, 880 (2013) (questioning whether spending programs blur accountability to any meaningful degree); Brian Galle, *Federal Grants, State Decisions*, 88 B.U. L. REV. 875, 920 (2008) ("Standing alone this voter-confusion story is not very persuasive. It may be true that voters will in part blame their local officials for the results of conditional grants, but that is not confusion at all. It takes two to contract, and local officials who make bad deals should be held to account for them, whether those deals are with trash-collection contractors or Congress.").

268. Bridget A. Fahey, *Consent Procedures and American Federalism*, 128 HARV. L. REV. 1561, 1565 (2015) ("In every program and for every grant that relies on the states' voluntary participation, the federal government decides how the states volunteer: which official or institution gets to speak for the state, how the decision is presented to that speaker, what process the speaker must use to communicate the state's decision, and the timeline on which the decision must be made.").

269. Role confusion is not without historical precedent. When the Church Committee examined intelligence abuses that took place in the 1960s and 1970s, it concluded that the FBI dodged criticism for deployment of controversial intelligence collection techniques by relying on local police departments to do so. Waxman, *supra* note 10, at 298–99.

The Supreme Court rejected commandeering because it makes it difficult to know which elected officials are responsible for a policy decision. The federal programs in the case studies are spending programs, but all of the Supreme Court's concerns about accountability are present in this context as well. It was Congress that created the Port Security Grant Program and Urban Areas Security Initiative, not local representatives. Congress made the decision to allocate money for surveillance equipment acquisition without requiring anyone to think through data management. The consequences of these programs were specific and local: the acquisition of surveillance technology by local police departments to be used to engage in surveillance of local populations. Naturally, public ire targeted these departments' respective city councils. And this anger was appropriate, given that these bodies could have insisted on the formulation of policies but did not insist. But federal elected representatives also could have insisted on the enactment of policies; however, this inaction at the federal level has not been met with similarly widespread public criticism.

The case studies cast doubt on whether the distinction the Court has drawn between programs that commandeer and conditional spending programs furthers its objective. And while the Court's concern appears to be whether the *public* can discern which political actors are responsible for which decisions, there may be a deeper problem. It may be that there is no good answer to who ought to be held responsible for a policy choice.[270] In the case studies, the matter is genuinely unclear. Probably the best answer is that both federal and local officials should shoulder a portion of the blame—local officials for not attending to a matter traditionally under local control, and federal officials for intervening in such a matter without attending to all of the consequences of their actions.

C. Accountability and Policy Arenas

The case studies also highlight the possible collateral consequences of federal national security initiatives on local policing. Some have argued that the federal government must take a stronger hand at the local level if it is to successfully prevent and respond to acts of terrorism.[271] But given

---

270. Perversely, it may be that federal spending programs that permit the maximum amount of local flexibility and choice in implementation also foment the most serious difficulties in determining who is responsible for policy choices. *See* Hills, *supra* note 266, at 827–28 (discussing Martha A. Derthick's classic study of the operation of public assistance programs in Massachusetts).

271. *See supra* notes 257–60 and accompanying text.

the substantial overlap between the equipment and techniques used to combat terrorism and those used to carry out routine law enforcement functions, anti-terrorism initiatives are likely to have substantial spillover effects on routine policing. This suggests that any cost-benefit analysis of federal national security initiatives that incorporate local law enforcement agencies ought to account for these initiatives' impact on policing, including the transparency of police practices and the accountability of police for their actions, not just what they contribute to federal national security priorities.

Both policy makers and scholars have contended that the federal government must become more involved at the local level to advance the War on Terror. Most famously, the 9/11 Commission concluded that "[t]here is a growing role for state and local law enforcement agencies," but cautioned that "[t]hey need more training and work with federal agencies so that they can cooperate more effectively with those federal authorities in identifying terrorist suspects."[272] Some scholars have also endorsed this view,[273] articulating more specifically the areas in which

---

272. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 390 (2004), http://avalon.law.yale.edu/sept11/911Report.pdf [https://perma.cc/2FLJ-ZL5G]; *see also* PETER NEUMANN, BIPARTISAN POL'Y CTR., PREVENTING VIOLENT RADICALIZATION IN AMERICA, 43–45 (2011), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/NSPG.pdf [https://perma.cc/LR9C-9BWY] (criticizing federal efforts to catalyze local involvement in terrorism prevention as ineffectual); Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. NAT'L SECURITY L. & POL'Y 377, 377 (2009) (identifying calls by federal officials for greater federal-local collaboration to prevent, investigate, and respond to terrorism).

273. *See, e.g.*, RICHARD A. POSNER, COUNTERING TERRORISM 155–56 (2007) ("MI5 has been able to do what the FBI and the Department of Homeland Security have been unable to do—integrate local police into the national domestic intelligence system. It is a vital mission. Local police, border patrol, customs officers, and private security and intelligence personnel gather enormous masses of information at the source, as it were. They are well positioned to notice anomalies that may be clues to terrorist plotting. We need an agency that will integrate local police and other information gatherers into a comprehensive national intelligence network, as MI5 has done in Britain."); Lindsey Garber, *Have We Learned a Lesson? The Boston Marathon Bombings and Information Sharing*, 67 ADMIN. L. REV. 221, 238–44 (2015) (discussing the importance of state and local involvement to terrorism prevention measures); Steven R. Morrison, *The System of Domestic Counterterrorism Law Enforcement*, 25 STAN. L. & POL'Y REV. 341, 375 (2014) ("Over time, it became apparent that expansive terrorist structures, instantiated in the spread of ideology rather than institutional structure and the encouragement of lone wolf, homegrown operators rather than cells connected to a center, required a mirroring law enforcement response. That response includes calls for more local responses, is coded as traditional law enforcement, and is a relatively novel approach"); Mitch Silber & Adam Frey, *Detect, Disrupt, and Detain: Local Law Enforcement's Critical Roles in Combating Homegrown Extremism and the Evolving Terrorist Threat*, 41 FORDHAM URB. L.J. 127, 145 (2013) ("Since the September 11 terrorist attacks, it has become clear that local police departments have a role to play in the counterterrorism fight."); William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2160 (2002) ("Local police have already been affected by the terrorist attacks, and powerfully so. The FBI may have primary

collaboration is likely to be fruitful,[274] and identifying challenges that are likely to arise.[275]

One such challenge is the inherent inseparability of initiatives to combat terrorism from routine law enforcement functions. For example, as Samuel J. Rascoff has pointed out, it is precisely because local police officers develop rich and trusting relationships with local residents through routine policing that they are also well positioned to pick up information about possible terrorist threats.[276] This capacity for intelligence gathering presents an opportunity, but pursuing this aspect of the job too aggressively may undermine community relationships that are necessary to maintaining public safety and order.[277]

The entwinement of national security and law enforcement functions may be particularly acute when it comes to surveillance equipment. An automatic license plate reader can be used to determine whether a vehicle is registered to someone with an outstanding felony arrest warrant, or it can be used to determine whether the vehicle is registered to someone whose name is on a terrorist watch list. Stingrays, devices used to pinpoint the geographic location of cell phones, can be used to identify the locations of cell phone-carrying drug dealers, or they can be used to identify the locations of cell phone-enabled improvised explosive devices. Moreover, because terrorism is exceedingly rare compared to other forms of crime, a particular piece of surveillance equipment is vastly more likely to have an impact on criminal law enforcement than it is to have an impact on terrorism-related investigations.[278] This impact may be magnified given that local law

---

responsibility for investigating allegations, but that agency lacks the manpower to guard public places. Local police must do so."); Waxman, *supra* note 10, at 346–47 (contending that "many aspects of counterterrorism intelligence will require centralized federal control and high degrees of uniformity—even if they also necessarily involve coordination with local agencies").

274. *See, e.g.*, Samuel J. Rascoff, *The Law of Homegrown (Counter)Terrorism*, 88 TEX. L. REV. 1715, 1721 (2010) (advocating for "the creation of new federal-local collaborative structures that will simultaneously enhance the analytic rigor and the legal oversight of local intelligence while leaving undisturbed and exploiting to full effect the advantages that local intelligence possesses").

275. Waxman, *supra* note 272, at 378 (explaining that the article "examines three national security law challenges resulting from greater involvement of state and local police agencies in protecting national security, especially in combating terrorism").

276. Rascoff, *supra* note 274, at 1731–35.

277. *Id.* at 1738 ("This balanced portfolio—and the fact that local police are inevitably 'repeat players' in the communities in which they operate—does, in fact, create powerful incentives for police officers to negotiate a middle road when it comes to the more intrusive and potentially objectionable aspects of counterterrorism.").

278. This point is probably intuitive, but there is also some scattered empirical evidence to support it. For example, in February 2013, the Tacoma, Washington, City Council accepted some $190,000 in funds from the federal Port Security Grant Program to purchase an update to an

enforcement agencies have more experience and knowledge about routine criminal law enforcement than combatting terrorism and may therefore be more readily positioned to envision creative uses of surveillance equipment for law enforcement purposes.

The Seattle and Oakland case studies provide further support for the idea that, although the purpose of a federal program may be to combat terrorism, its effects may fall mostly on policing. (The San Diego case study does not fit this mold because the federal program that funded it was targeted at law enforcement practices.) Seattle paid for its drone using funds from the Urban Areas Security Initiative, a program to help urban areas prevent and recover from acts of terrorism.[279] Seattle did not have the opportunity to use its drone, but its plans for the drone's deployment stretched beyond terrorism to include documenting traffic accident scenes and searching for missing persons.[280] Seattle funded its wireless mesh network through the Port Security Grant Program, which is designed to help mitigate the risk that terrorists will exploit security

---

unnamed device, the purpose of which was "to assist in the prevention, detection, response, and recovery of improvised explosive devices." TACOMA CITY COUNCIL, MINUTES 1–2 (Mar. 19, 2013), https://cityoftacoma.legistar.com/View.ashx?M=M&ID=331085&GUID=2FD1B1C7-F7BD-4CED-87FD-2E7EB10DCA60 [https://perma.cc/65GZ-T32F]. Subsequent reporting by the Tacoma News Tribune revealed that the device was a stingray. *See* Kate Martin, *Tacoma Police Using Surveillance Device to Sweep Up Cellphone Data*, NEWS TRIB. (Aug. 26, 2014), http://www.thenewstribune.com/news/local/article25878184.html [https://perma.cc/LS8X-KDD4]. A privacy advocate's public records act request demonstrated that while the device had been used 168 times to investigate crimes from murder to assault to theft of a city laptop, not once had it been used to detect an improvised explosive device. TACOMA POLICE DEP'T, RESPONSE TO PUBLIC RECORDS ACT REQUEST OF PHIL MOCEK, https://d3gn0r3afghep.cloudfront.net/foia_files/partial_response.pdf [https://perma.cc/K295-BVQV]. Automatic license plate readers provide another example. In 2012, in a previous career as a staff attorney for the American Civil Liberties Union, I worked with colleagues to file a public records act request with the Maryland fusion center to obtain data on its use of automatic license plate readers. *See* ACLU, *supra* note 164 (describing multi-state public records act initiative to uncover use of automatic license plate readers). The data showed that between January and May of 2012, the fusion center collected about 35 million plate reads. MARYLAND STATE POLICE, PUBLIC RECORDS ACT RESPONSE (2012), https://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpra_msp_md%20(1).pdf [https://perma.cc/A6TK-RX6J]. Of these, 59 reads were of cars registered to individuals listed on a violent gang or terrorist organization watch list. *See id.* (that figure does not mean that these cars were actually driven by gang members or terrorists; it just means that a person associated with the car had been placed on a government watch list). By contrast, some 90,000 were associated with individuals driving on suspended or revoked licenses, or who had not complied with the vehicle emissions program. *See id.* The overwhelming majority pertained to the movements of vehicles whose owners were not suspected of anything at all. *See id.*

279. *See supra* Part II.

280. Christine Clarridge, *supra* note 58 (discussing traffic investigations); SEATTLE POLICE DEP'T, SEATTLE POLICE DEP'T UNMANNED AERIAL SYSTEMS, *supra* note 39, at 5.

vulnerabilities at ports.[281] The mesh network would have had important functions in an emergency, such as ensuring that first responders could continue to communicate with one another even if the cellular network became overloaded.[282] The mesh network facilitated the city's placement of surveillance cameras in downtown Seattle, cameras that were to have been used for routine law enforcement purposes.[283] The Port Security Grant Program also funded Oakland's DAC. Given that the purpose of the DAC was to improve port security by gaining a better understanding of events in Oakland through establishment of a citywide surveillance center, it, too, would have had a substantial impact on routine law enforcement.

It is also worth asking whether the disconnect between the federal government's objectives in funding the technologies and the local law enforcement agencies' objectives in acquiring them contributed to the failure of the Seattle and Oakland programs—and whether the identity of interests of the federal government's funding program and ARJIS's objectives was a factor in the success of ARJIS's facial recognition technology. The record is clear that Oakland tailored its proposal to create a DAC around federal funding requirements, and although there is inadequate information to draw this conclusion about Seattle's programs, it is a possibility. In San Diego, the obvious match, in interest and expertise, between the DOJ funding program and ARJIS may have contributed to the program being well-targeted at a pressing local law enforcement need.

These programs are not the only documented examples where federal initiatives created to combat terrorism by harnessing sub-federal law enforcement agencies have had substantial spillover effects on law enforcement practices. After 9/11, the federal government directed considerable resources toward expanding the nation's network of fusion centers, state and local government entities designed to enhance information sharing and analysis.[284] These centers have prioritized state and local objectives over federal goals.[285]

---

281. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-47, PORT SECURITY GRANT PROGRAM: RISK MODEL, GRANT MANAGEMENT & EFFECTIVENESS MEASURES COULD BE STRENGTHENED 1 (2011), http://www.gao.gov/assets/590/587142.pdf [https://perma.cc/DT2P-NM76].

282. *See supra* section II.A.2.

283. *See supra* section II.A.2.

284. Jason Barnosky, *Fusion Centers: What's Working and What Isn't*, BROOKINGS INSTITUTION (Mar. 17, 2015), https://www.brookings.edu/blog/fixgov/2015/03/17/fusion-centers-whats-working-and-what-isnt/ [https://perma.cc/646S-D4V8].

285. *See id.*

The observation that federal anti-terrorism programs have spillover effects on routine law enforcement functions matters because effectiveness of government programs ought to be evaluated in light of all of their consequences. When federal programs provide funding to sub-federal law enforcement agencies, any such evaluation should account for not only their impact on the federal government's national security agenda, but also the impact on local policing. Additionally, impact on local policing should be gauged in a holistic manner, accounting for both benefits to public safety and costs to civil liberties, as well as consequences on accountability and transparency of policing.[286]

IV. REMEDIES TO DEMOCRATIZE LOCAL SURVEILLANCE POLICY MAKING

The preceding Parts demonstrate that the federal government fails to ensure that local elected officials and members of the public are involved in decisions about surveillance technology acquisition, or that anyone develops a policy to govern this technology's use.[287] They also show that this failure can lead local law enforcement agencies to adopt surveillance technologies that are out of step with local preferences.[288] They further suggest that local input can play a valuable role in ensuring that surveillance policy is consistent with local crime rates, the competence and trustworthiness of the police department, and local political preferences.[289] Finally, the preceding Parts contend that while different communities may reasonably decide to engage in greater or lesser amounts of surveillance, all surveillance technology deployments should be governed by policies addressing data collection, retention, use, and sharing.[290]

Building off of this descriptive and normative account, this Part offers proposals for how to increase local democratic control of surveillance policy and ensure that this policy addresses key data management issues. Reform options include steps that elected representatives could take at the federal, state, and local levels. The menu of reform options works to

---

286. Rachel A. Harmon makes a broadly similar point in arguing that federal public safety programs should be evaluated in a way that accounts for the nonmonetary costs of policing, including the costs of coercion. *See* Harmon, *supra* note 8.

287. *See supra* Part I.

288. *See supra* Part II.

289. *See supra* Part II.

290. *See supra* section III.A.

capture all policy solutions that could work as a theoretical matter while acknowledging that some are more politically feasible than others.

A. Federal Remedies

If part of the problem is that the federal government does not require local elected representatives and members of the public to be involved in decisions about what technologies law enforcement agencies acquire and does not require anyone to develop use policies, then one possibility is for the federal government to condition receipt of funding on completion of these steps. A federal solution has particular appeal because only the federal government could devise a remedy that would apply comprehensively.

1. Require Involvement of Elected Representatives in Decisions About Technology Acquisition

There is nothing to stop the federal government from requiring that local elected officials be involved in decisions about what surveillance technologies local police departments acquire with federal money. As discussed previously, the federal government has sweeping power to place conditions on grants-in-aid.[291] Federal programs routinely designate which state or local actors must elect to participate in other federal programs.[292] To be sure, the case studies provide reason to doubt that incorporating elected officials into the decision-making process, without additional measures, will achieve meaningful oversight. But the opportunity to weigh in is still a necessary precondition to such oversight, and it is one local elected officials should be provided.

There are difficult and uncertain questions about how best to structure the involvement of local elected representatives. One such question pertains to timing. The sooner local elected officials become involved in decisions regarding surveillance technology acquisition, the greater the influence they will have over local surveillance policy. If local elected officials were required to sign off on grant applications prior to submission, then in theory it would not be too late for them to suggest acquisition of different technologies (e.g., a red light camera instead of a surveillance camera) or abandonment of the application altogether. By the time the federal government has funded a specific grant proposal and local elected officials face an up-or-down vote on whether to take the

291. *See supra* section III.B.

292. Fahey, *supra* note 268, at 1573–75.

money, there is not the same opportunity for creative input. Also, cash-strapped municipalities may be reluctant to reject free equipment, even if it is not the best match for local circumstances.

The case studies do not shed light on how pre-application involvement would work out in practice because in no case did local law enforcement agents seek such approval.[293] The fact that SANDAG's reform measures included Board review of grant applications prior to submission suggests that at least some local governing bodies would desire such authority.[294]

2. Require Meaningful Disclosure of Information to Elected Representatives

In addition to requiring that local elected officials have an early opportunity to weigh in on surveillance technology acquisition, the federal government could also mandate that local elected officials receive a written assessment of the impact of the surveillance technology at issue.[295] This assessment could encompass not only the benefits to public safety, but also the consequences for civil rights and liberties, especially (given the nature of surveillance technology) for privacy. However, assessments will only help when lack of information, rather than inadequate comprehension or interest, impedes participation by local elected representatives.

The federal government itself produces a couple of helpful models for how this could work in practice. The first, a privacy impact assessment, is a formalized "analysis of how personally identifiable information is collected, retained, used, [and] shared."[296] The E-Government Act of

---

293. Oakland city staff did provide the city council with an informational report about its plan to seek a grant before the grant application deadline, but it did not seek council approval. *See supra* section II.B.

294. SANDAG set up streamlined protocols for time-sensitive grant applications. *See* SAN DIEGO ASS'N OF GOV'TS, *supra* note 213.

295. Thanks to Deirdre K. Mulligan for this suggestion. In 2006, Mulligan recommended that the U.S. Department of Homeland Security require potential recipients of DHS grants for video surveillance systems to conduct a privacy impact assessment. Prepared Statement of Deirdre K. Mulligan before the Department of Homeland Security Data Privacy and Integrity Advisory Committee 2 (June 7, 2006), https://www.law.berkeley.edu/files/Mulligan_DHS_Statement.pdf [https://perma.cc/PDD7-3QT2].

296. *Privacy Impact Assessments*, FED. TRADE COMM'N, https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments [https://perma.cc/37H4-SULA]. For a detailed consideration of the challenges of using privacy impact assessments to get government agencies to consider privacy in addition to their primary objectives, see generally Kenneth A. Bamberger & Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-Making in U.S. Government*

2002 requires all federal agencies to conduct privacy impact assessments "for all new or substantially changed technology that collects, maintains or disseminates personally identifiable information."[297] Among other things, privacy impact assessments must "contain a risk assessment that specifically identifies and evaluates potential threats to individual privacy, discusses alternatives and identifies the appropriate risk mitigation measures for each."[298] The second, pioneered by the DHS Office for Civil Rights and Civil Liberties, is the civil rights and civil liberties impact assessment.[299] As the name suggests, this assessment covers a broader range of rights and liberties than a privacy impact assessment, but the general idea is the same.

To be sure, assessments will not be a cure-all. However, they would likely be an improvement on the status quo. If the federal government required local law enforcement agencies to conduct an assessment of any surveillance technology they wish to acquire using federal funds, it would help to ensure that these agencies thought through the impact of surveillance technologies on protected rights and liberties. The requirement to produce an assessment could be coupled with a mandate that the assessment be made available to the public and provided to local elected officials.[300] In that case, the assessment would also raise public awareness about a local law enforcement agency's surveillance plans and aid local elected representatives in weighing in on surveillance technology acquisition in an informed manner.

3. Require that Surveillance Technologies Be Governed by Use Policies

Finally, the federal government could require that all federally funded surveillance technology be governed by a data management protocol that addresses the fundamental questions of data collection, retention, use, and sharing. Ideally, draft protocols would be shared with representatives at the same time as the assessment described above, and

---

Agencies, *in* PRIVACY IMPACT ASSESSMENT 225, 225–74 (David Wright & Paul De Hert eds., 2012).

297. *Privacy Impact Assessments*, NAT'L ARCHIVES, http://archives.gov/privacy/privacy-impact-assessments/index.html [https://perma.cc/P84U-U2U4].

298. Bamberger & Mulligan, *supra* note 295, at 228.

299. *Civil Rights & Civil Liberties Impact Assessments*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/civil-rights-civil-liberties-impact-assessments [https://perma.cc/DMW4-TYKS].

300. Some federal programs already require that states take steps to publicize, and even obtain comment, on applications for grant funds. Fahey, *supra* note 266, at 1578.

would be approved by local elected representatives prior to deployment. The federal government already requires federally funded fusion centers to have privacy policies.[301] There is no reason that other programs that fund surveillance could not do the same.

* * *

The combination of early notice to elected representatives and meaningful provision of information to them, in the form of assessments and draft data management protocols, is consistent with scholarship suggesting that enhanced accountability through external oversight can help advance agencies' secondary goals.[302] While this model still depends on external oversight being conducted vigorously and thoughtfully, these reforms should lead to greater consideration of privacy and other civil liberties and rights than is currently the case.

B. State Remedies

States could also adopt the reform measures advocated in the preceding section. While states generally delegate policing policy to local governments, they are free to take on this topic themselves. Relying on every state to pass legislation is unlikely to result in a remedy as comprehensive in scope as a federal-level solution, but there may be more political willpower to tackle surveillance policy making by procurement at the state level.

In recent years, states have been remarkably active in passing legislation limiting law enforcement agencies' use of surveillance technologies.[303] In the aftermath of the heavily militarized response to

---

301. Barnosky, *supra* note 284.

302. *See, e.g.*, Bamberger & Mulligan, *supra* note 295, at 248.

303. For example, in 2015, California passed a comprehensive law, the California Electronic Communications Privacy Act, requiring warrants for digital records of emails, texts, and geolocation information, even when the data is stored in the cloud by service providers. CAL. PENAL CODE § 1546–1546.4 (West 2016). Virginia enacted legislation requiring law enforcement agencies to obtain a warrant (except in limited circumstances) before employing a drone. VA. CODE ANN. §§ 19.2–60.1 (2015). North Carolina adopted a bill that requires state and local agencies employing license plate readers to adopt a written use policy and sets limitations on data retention without a warrant. N.C. GEN. STAT. §§ 20-183.22–24 (2015). For a useful compilation of state legislation regarding drones (both pertaining to law enforcement use and otherwise), see *Current Unmanned Aircraft State Law Landscape*, NAT'L CONFERENCE OF STATE LEGISLATURES (Sept. 9, 2016), http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx [https://perma.cc/9J23-VN82] (thirty-two states have enacted laws and five have passed resolutions). For a similar compilation for ALPR legislation, see *Automated License Plate Readers: State Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Nov. 11, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/2014-state-legislation-related-to-

protesters in Ferguson, states have also considered (and New Jersey has passed) legislation requiring local government approval when police departments seek to obtain surplus military equipment.[304] Surveillance policy making by procurement resides at the intersection of these two issues and should therefore be of interest to state legislatures as well.

Reforms enacted on the state level would not provide as comprehensive a remedy as federal reforms because they would only go into effect in those states that adopted them. However, they would address more instances of surveillance policy making by procurement than would relying on each local government to enact its own legislative fix. Moreover, as Richard Briffault has pointed out, states have "greater resources and greater ability to mobilize public attention that comes from their relatively greater size and fewer numbers."[305] California's passage of a data breach notification statute, requiring businesses and agencies to provide notice to California customers whose personal information is subject to a data breach, led forty-six states to pass similar laws.[306] Action in one prominent state or a handful of states on surveillance policy making by procurement could lead to a similar snowball effect.

C. Local Remedies

Local elected representatives have the most straightforward remedy available to them: they can require that local police departments draft impact assessments and data management protocols and present these items for consideration and approval prior to applying for federal funding. Another option, at least for larger municipalities, is to institutionalize a privacy officer function and empower the privacy officer to oversee municipal data management practices. The disadvantage of depending on every local government to take one of

automated-license-plate-recognition-information.aspx [https://perma.cc/3746-6U2W] (in 2015 alone, eighteen state legislatures considered ALPR bills, four of which enacted legislation).

304. Jake Grovum, *Can States Slow the Flow of Military Equipment to Police?*, STATELINE (Mar. 24, 2015), http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/3/24/can-states-slow-the-flow-of-military-equipment-to-police [https://perma.cc/N3Y8-6PSK].

305. Richard Briffault, *"What About the 'Ism'?" Normative and Formal Concerns in Contemporary Federalism*, 47 VAND. L. REV. 1303, 1349 (1994).

306. Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191, 232 (2011).

these steps is that many municipalities will lack the resources or interest to do so.[307]

Seattle's surveillance equipment ordinance came close to taking the steps this Article recommends.[308] It has also inspired a few other communities to implement or consider similar measures. The Santa Clara County, California, Board of Supervisors recently passed an ordinance requiring officials wishing to deploy surveillance technology to provide an analysis of the privacy and due process impact of the technology, to obtain approval of a use policy prior to seeking funding for such technology, and to report annually on the use of the technology.[309] As discussed earlier, Oakland is now at work on its own surveillance equipment ordinance.[310] Although this is hardly a nationwide movement, prominent civil liberties groups have begun to throw their weight behind these ordinances, and they may yet spread.[311]

Another possibility, at least in mid-sized or larger municipalities, is to create a privacy officer position with a portfolio that includes addressing surveillance policy making by procurement. As a general matter, a privacy officer's job responsibilities include formulating and monitoring compliance with privacy policies, handling public requests for access to data as well as complaints, and serving as a general resource on privacy and other civil liberties issues.[312] The DOJ urges all law enforcement agencies collecting personally identifiable information to ensure that someone within the department serves the function of a privacy officer.[313] With respect to surveillance policy making by procurement,

---

307. As discussed in section III.A, while municipalities may reasonably differ on the substance of what surveillance policies they prefer, surveillance technology use should be governed by a data management protocol.

308. *See supra* section II.A.2.

309. SANTA CLARA CTY., CAL., ORDINANCE NS-300.897 (June 21, 2016).

310. *See supra* section II.B.2.

311. For example, the ACLU of California has developed a model ordinance to bring greater oversight and transparency to surveillance technology acquisition and deployment, suggesting that this organization will put resources behind seeing these types of ordinances adopted more widely. ACLU OF CAL., MAKING SMART DECISIONS ABOUT SURVEILLANCE 25–28 (2016), https://www.aclunc.org/docs/20160325-making_smart_decisions_about_surveillance.pdf [https://perma.cc/4JZG-XNV7].

312. U.S. DEP'T OF JUSTICE GLOBAL ADVISORY COMM., ESTABLISHING A PRIVACY OFFICER FUNCTION WITHIN A JUSTICE OR PUBLIC SAFETY ENTITY 1 (2014), https://it.ojp.gov/GIST/165/File/Final-Privacy-Officer-Function-Brochure-6-17-140.pdf [https://perma.cc/VP7K-3YDR].

313. *Id.* at 2. Currently, the Washington, D.C., Metropolitan Police Department appears to be the only police department in the nation with a designated, full-time privacy officer. *See* Angelique Carson, *She's Not a Cop, But She's Their CPO*, INT'L ASS'N OF PRIVACY PROF'LS (June 23, 2015), https://iapp.org/news/a/shes-not-a-cop-but-shes-their-cpo/ [https://perma.cc/4Z2F-C2KJ].

the privacy officer could work with municipal agencies acquiring surveillance technology to develop impact assessments or data management protocols, which could then be sent to local elected representatives to approval.

An advantage of the privacy officer model is that it gives a designated person both the time and incentive to develop expertise on privacy matters. A major disadvantage is cost: only a relatively small share of municipalities will be able to afford to fund such a position. This solution is probably most appropriate for municipalities that are interested in addressing privacy matters not just within law enforcement agencies, but across the board. Municipalities are under increasing pressure to make the data they collect more readily available (commonly known as municipal open data initiatives) and to collect more data to improve service provision (commonly known as "smart city" initiatives).[314] A privacy officer might be worth the investment for cities embracing these initiatives.

CONCLUSION

For good reason, federal programs that fund local law enforcement agencies' acquisition of military-grade weapons and equipment have been the subject of considerable public concern and extensive scholarly analysis. Although their consequences are less visible, federal programs that fund acquisition of surveillance technology by these same agencies also merit our attention. Given the rapid pace of technological progress over the past two decades, it is understandable that our legal framework for disseminating and regulating surveillance technology is under-developed. But now that technologies such as drones and license plate readers are both widely used and widely known, it is time for our system of governance to catch up. The policy proposals contained in this Article begin that work.

---

314. For an interesting and empirically-grounded discussion of municipal open data, particularly relevant to the topic of this Article because it also uses Seattle as a case study, see Jan Whittington et al., *Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government*, 30 BERKELEY TECH. L.J. 1899 (2015). While law review literature on the smart city is sparse (although not non-existent, *see, e.g.*, Annie Decker, *Smart Law for Smart Cities*, 41 FORDHAM URB. L.J. 1491 (2014)), the idea has gained considerable traction and enthusiasm among policy makers. Most prominently, in 2015 the White House announced a $135 million "Smart Cities" initiative. *See FACT SHEET: Administration Announces New "Smart Cities" Initiative to Help Communities Tackle Local Challenges and Improve City Services*, THE WHITE HOUSE (Sept. 14 2015), https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help [https://perma.cc/28UK-CLDA].