Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 36 | Issue 5 Article 2

8-3-2020

LOCAL POLICE SURVEILLANCE AND THE ADMINISTRATIVE FOURTH AMENDMENT

Fidler, Mailyn

LOCAL POLICE SURVEILLANCE AND THE ADMINISTRATIVE FOURTH AMENDMENT

By Mailyn Fidler[1]

Police surveillance has become a problem of governance, not a problem of procedure. The introduction and use of sophisticated surveillance technologies, once reserved for elite central governments, in local policing has raised questions about the sufficiency of existing approaches. Judicial oversight—applying standard Fourth Amendment inquiries—falls short, limited to the facts of and parties to the case, rather than systems of surveillance, and with judges often unaware of or unable to access key technical details of the case. Other alternatives, including legislative guidelines for police technology and local police rulemaking, are lacking in other ways. This Article argues that the proper response to use of sophisticated investigative technologies by local police is local administrative governance by city councils or local administrative agencies. Having an external administrative body make rules about police technology brings with it an ability to consider expanded concerns about technology, timeliness, and an ability to regulate interactions with private actors. There are reasons to be worried about this proposal, too. But, drawing on the nascent literature about local administrative governance, this proposal is most likely to be

[1] J.D., Yale Law School, 2020. The author would like to thank Collin Anderson, Kade Crockford, Jason Eiseman, Barry Friedman, Heather Gerken, Ben Green, Christine Jolls, Scarlet Kim, Susan Landau, Lily Z. Liu, Asaf Lubin, Jonathan Mayer, Edin Omanovic, Daphna Renan, Alan Rozenshtein, David Schleicher, Kate Stith, Jonathan Zittrain, David O'Brien and the Berkman Klein Center for Internet & Society Cybersecurity paper workshop, and the Tufts Graduate Student Symposium in Cybersecurity Policy. The author would also like to thank the journalists who helped with this piece (Joseph Cox, Freddy Martinez, Michael Morisy, and Sam Richards), the Bloomington City Clerk's Office, the Water Protectors of Standing Rock (whose experiences navigating surveillance inspired this article).

responsive, accountable, and effective in the local context. In addition to offering a set of legal arguments, this paper contains two novel descriptive contributions. First, where other papers have focused on the legal risks of certain technologies, this paper compiles a comprehensive look at a range of police technologies and systematically analyzes the risks they pose both legally and at the local level. Second, this paper offers the first comprehensive assessment of the current efforts that localities have made towards implementing this kind of local administrative governance for police technology.

CONTENTS

INTRODUCTION

Local police now have access to surveillance tools once reserved for elite central governments. These surveillance technologies and their use at the local level bring new risks with them. Fourth Amendment judicial review, an ex post liability regime that imposes sanctions only after surveillance occurs, is insufficient as a system of oversight over local surveillance. Local police surveillance needs to be met with a system of ex ante governance that addresses questions beyond police procedure. This Article argues that local administrative governance of police surveillance is the way to achieve this goal.

The technologies local police are using are now "more powerful than those used by superpowers during the Cold War," a 2014 presidential report noted.[2] Surveillance tools trickle down to local law enforcement departments from the federal government and are increasingly accessible directly on a robust private market. Many police departments are using these powerful technologies in new ways, too. Police are engaging in what scholars have termed "programmatic surveillance," which involves broader searches that rely on court-sanctioned protocols that fall short of Fourth Amendment individualized suspicion.[3] Examples of these programs include use of facial recognition technology, checkpoints, searches of businesses for evidence of regulatory violations, drug testing of groups, DNA sampling of all arrestees, and use of automated license plate readers or electronic tolling tools like EZ Pass for investigative purposes.[4] Data gathered from any of these practices can be fed into databases and sophisticated data analytics software, increasing the utility of the data for law enforcement.[5]

---

[2] John Podesta et al., *Big Data: Seizing Opportunities, Preserving Values*, EXEC. OFFICE OF THE PRESIDENT (May 2014).

[3] Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039 (2016).

[4] Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine,* 102 GEO. L.J. 1721, 1727 (2014); Barry Friedman and Maria Ponomarenko, *Democratic Policing*, 90.6 NYU L. REV. 1827, 1874 (2015); Dan Glaun, *Massachusetts Police Use Electronic Tolling System to Track People in Ongoing Investigations*, GOV. TECH. (Aug. 11, 2017).

[5] For example, CellHawk is software that takes in raw call record details and turns out easy-to-use analyses of that data, including maps; *see* Sean Curtis, *Get More Answers from Call Detail Records Using CellHawk Software*, POLICEONE (July 7, 2017) (thanks to Sam Richardson with the NStarPost for the example); *see also* Sarah Brayne, *Big Data Surveillance: the Case of*

Critics of judicial-only oversight of these practices, such as Daphna Renan, have argued that courts are "hamstrung in their ability to supervise the sprawling, interacting, and overlapping administrative policies shaping the modern power to search."[6] Friedman and Ponomarenko argue that these limitations render "traditional constraints on the sweep of criminal law enforcement largely meaningless."[7] Furthermore, courts operate at a purposefully careful pace, but this feature means that courts have taken up to a decade to converge on the proper applicability of Fourth Amendment protections to law enforcement use of new technologies, leaving a legal gap.[8] This judicial caution has some benefits, but it also results in law enforcement being able to anticipate years of warrantless application of newly introduced devices. Moreover, the ways in which local police typically gain access to sophisticated surveillance technology, often conditioned on non-disclosure agreements with manufacturers and/or the FBI, also shield the use of this technology from effective judicial oversight.

These risks are exacerbated or augmented when we move from the federal to the local level. State courts may fare even more poorly than federal courts in terms of expertise about or exposure to such cases to deal adequately with these technologies. Similarly, state defense counsel may face substantial resource constraints, reducing their ability to bring novel legal arguments about technology to the attention of judges. Beyond courts, the private sector may be able to exert more pressure in local contracts to keep details of technology out of courts: some local governments will be less sophisticated negotiating partners than the federal government. The sheer number of local governments available as potential customers will mean that technical training supplied to officers, NDAs, and advertised use cases will vary much more than at the federal level. And, in most cases, these private contracts will be shielded from any local political oversight.[9]

Policing, 82.2 AM. SOC. REV. (2017); *see also* Craig Timberg and Ellen Nakashima, S*tate Photo-ID Databases Become Troves for Police*, WASH. POST (June 13, 2016); Tami Abdollah, *Private Database Lets Police Skirt License Plate Limits*, SAN DIEGO UNION-TRIBUNE (Oct. 7, 2015).

[6] *See* Renan, *supra* note 3, at 1045.

[7] *See* Friedman and Ponomarenko, *supra* note 4, at 1874.

[8] *See infra* Section II(B)(3)(a) for an account of a ten-year delay in the case of stingray devices.

[9] *See* Catherine Crump, *Surveillance Policymaking by Procurement*, 91 WASH. L. REV. 1595, 1597-98 (2016). For an example of a centralized procurement office, see the Baltimore Bureau of Procurement, https://procurement.baltimorecity.gov/. For an example of departmental

Similarly, federal government grant programs to localities usually bypass local political control.[10] Last, local law enforcement also deals with a wider range of crimes than does federal law enforcement, which means their use of these technologies disperses the technologies and their risks more thoroughly through communities. In particular, local law enforcement officers also serve as the typical responders to protests, which further disperses these risks onto wide sections of the population.

This Article's argument for local administrative governance of surveillance technology takes inspiration from existing, influential scholarship on this question of police governance at the federal level and in other non-technology contexts at the local level.[11] Daphna Renan, the author of the most relevant work examining Fourth Amendment administrative governance at the federal level, argues that a "[federal] administrative overseer . . . can engage in a more holistic, granular, and data-driven Fourth Amendment interest balancing than courts have shown a willingness to undertake."[12] Renan writes that a federal administrative approach to Fourth Amendment issues "opens a broader prescriptive conversation," noting local policing in particular deserves examination.[13] I take up this prescriptive conversation and argue that administrative governance at the local level is needed, especially given the special risks of the context. The nationwide appetite for this kind of local governance has only grown in recent years. Michael Brown's killing in 2014 and the resulting surveillance of protesters focused attention on reform of local police governance in a serious way. Local reform of police has only taken on increased urgency and political plausibility in wake of protests responding to

---

procurement, *see* Bismarck, North Dakota, https://www.bismarcknd.gov/DocumentCenter/View/4478/Handgun-RFP1.

[10] Crump, *supra* note 9, at 1600, 1656.

[11] *See generally* Renan, *supra* note 3; *see also* Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570 (2018); Slobogin, *supra* note 4; *see also* Kenneth Culp Davis' work on administrative governance of police, including KENNETH CULP DAVIS, DISCRETIONARY JUSTICE: A PRELIMINARY INQUIRY 188 (1969) and Kenneth Culp Davis, *An Approach to Legal Control of the Police*, 52 TEXAS L. REV. 703 (1974); Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974); Donald A. Dripps, *'Perspectives on the Fourth Amendment' Forty Years Later: Towards the Realization of an Inclusive Regulatory Mode*l, 100 MINN. L. REV. 1885 (2016); Carl McGowan, *Rule-Making and the Police*, 70 MICH. L. REV. 659, 690 (1972).

[12] *See* Renan, *supra* note 3, at 1045.

[13] *See* Renan, *supra* note 3, at 1046 n.24.

George Floyd's 2020 killing. Governance of local police surveillance is an important part of this broader reform discussion.

Administrative governance looks different at the local level than at the federal level—and will vary widely between differently structured local governments. This Article focuses on three defining features to capture what administrative governance looks like at the local level. Practically, administrative governance will happen through the blended legislative-executive functions of city councils or through separate appointed bodies. In terms of defining features, first, an administrative body has "institutional remove from [the] front-line actors" it regulates.[14] Second, the body has the ability to state the rules by which decisions will be made and the further ability to make those specific decisions at distinct points in time. Last, the predominant, although not exclusive, mode of administrative decision-making is ex ante, rather than ex post. These features allow administrative governors to take a systemic view of issues, one that can consider social and policy concerns, not one scoped to the rights or circumstances of an individual.[15] In addition, these aspects impart the benefits of speed and adaptability. In the context of local police surveillance technology, these advantages translate to an ability to govern in a technologically neutral manner,[16] place finer-grained controls on investigative powers, reach police interactions with private parties (not just with defendants), and shift a regulatory regime in response to new information.

Importantly, this kind of administrative governance approach to the Fourth Amendment would still rely on the final judgment and review of courts. But, in this context, courts would review police action that would have been first taken pursuant to a transparent and accountable administrative process, acting within the bounds of legislated powers.[17] Courts could also potentially review the administrative procedures themselves.[18] Such an approach incorporates the best of judicial expertise, expert knowledge, and democratic accountability.

The first Part of this Article compiles details about the use of two categories of police surveillance technology and systematically

---

[14] *See* Renan*, supra* note 3, at 1045; *see also* Maria Ponomarenko, *Rethinking Police Rulemaking*, 114 NORTHWESTERN U. L. REV. 1, 5 (2019).

[15] *See Renan*, *supra* note 3*,* at 1051 (discussing transactional versus programmatic regulation of surveillance).

[16] For a general discussion and critique of technology-neutral regulation, *see* Brad Greenberg, *Rethinking Technological Neutrality*, 100 MINN. L. REV. 1495 (2016).

[17] *See* Renan, *supra* note 3, at 1075.

[18] *See infra* section III(D).

analyzes the legal risks they pose, especially at the local level. Whereas most other papers in this area focus on one specific technology's risk, this synthetic treatment is important because it highlights the risks that surveillance technologies in general (rather than one specific tool) present in a local context governed only by courts. The second Part of this Article then presents the case for administrative governance of police surveillance technology at the local level and argues against alternatives. The Article closes with the first comprehensive assessment of current efforts localities have made towards implementing this kind of local administrative governance for police technology. This analysis reveals early signs of promise that local administrative governance of surveillance technologies can help ensure Justice Brandeis' hope "that the 'progress of science' does not erode Fourth Amendment protections."[19]

I. LEGAL & LOCAL CHALLENGES OF SURVEILLANCE TECHNOLOGY

A. Background

In 2014, the Supreme Court held in *Riley v. California* that a warrantless search of a cellphone and its contents incident to arrest was unconstitutional.[20] The Supreme Court's decision in *Riley* was, to quote Orin Kerr, "a big deal."[21] Kerr argues that "*Riley* can be fairly read as saying that computers are a game-changer" and as a signal that the Supreme Court endorses "treating computer searches differently than physical searches."[22]

The devices addressed in this article all enable surveillance of cell phones, essentially mini-computers, tools which the Supreme Court has recognized as fundamentally sensitive.[23] These technologies share a set of distinct features, including the ability to collect multiple types of data from devices in the possession of surveillance targets, making them a distinct category that can be analyzed together. Other

---

[19] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (quoting Olmstead v. United States, 277 U.S. 438, 48 S. Ct. 564 (1928) (Brandeis, J. dissenting)).
[20] *See* Riley v. California, 134 S. Ct. 2473, 2474 (2014).
[21] Orin Kerr, *The Significance of Riley*, THE WASH. POST (June 25, 2014, 8:56 AM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley/.
[22] *Id.*
[23] *See* Riley *supra* note 20*,* at Ct.2494-95 (2014) ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'").

technologies, such as facial recognition and predictive policing technologies, have also "trickled down" from federal use.[24] This Article confines its analysis to cell-phone related technologies, however, for three reasons: first, for brevity, and second, because the Supreme Court has helpfully recognized cell phones as fundamentally different and sensitive from other past kinds of technology, providing a good legal basis for grouping them.[25] Third, it does so for a conceptual reason: other technologies, such as facial recognition and predictive policing, do not rely on access or interference with devices owned by citizens and, as such, do not involve questions of property, an important legal distinction.

The following section introduces two technologies used for cell-phone surveillance: stingray devices and mobile forensics devices. Each subsection in this Part describes how the technology works and documents the technology's movement from federal to local law enforcement. In addition, each section surveys the legal issues that these technologies raise, specifically noting where state and local use exacerbates or complicates these legal issues.[26] Specifically, these sections highlight how existing court-centric Fourth Amendment oversight has fallen short.

Of these technologies, stingray devices have diffused through the local and state law enforcement scene most thoroughly. As such, they are the least novel technology analyzed, but exploring stingray devices provides a complete case study of trickle-down technology and the insufficiencies of a standard, court-driven approach to accompanying privacy challenges. For the sake of brevity and clarity, this paper refers to all instances of this technology as "stingray devices," regardless of

---

[24] Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where it Falls Short*, N.Y. TIMES (Jan. 12, 2020); *City of Bridgeport Predictive Policing Technology and Police Radio Acquisition*, BYRNE-JAG AWARD 2016-DJ-BX-0647, 2016.

[25] *See* Riley *supra* note 20*,* at Ct.2494-95 (2014).

[26] For a more in-depth look at these issues as identified at the federal level, *see, e.g.,* Mayer, *supra* note 11; *see also* Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 MISS. L.J. 1229, 1229-31 (2012); *see also* Gus Hosein and Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071, 1093-97 (2013). *But see* Steven M. Bellovin et. al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 2 (2014) (arguing that lawful hacking is "on balance, preferable to adding more complexity and insecurity to online systems.").

their actual brand names (alternative brand names to the Stingray brand include Triggerfish or KingFish, or the generic term is cell-site simulators/IMSI catchers).

Technology rapidly changes. As surveillance reporter Joseph Cox writes, "there's always a new player in the law enforcement hacking industry."[27] Although the specifics of the technologies used by local law enforcement may change going forward, general patterns emerge in certain areas from a study of a subset of specific tools. These patterns include the transfer from federal to local use, legal questions common across technologies, and similar judicial responses to new technologies. These common aspects can be used to build an analysis of needed governance mechanisms.

The local context adds to the legal risk these tools raise. Even at the federal level, there has been widespread confusion about the legal frameworks for these tools. There, only a few centrally coordinated agencies and federal courts are relevant decisionmakers. With dozens of state agencies and courts now joining the interpretation game, the legal landscape will grow even murkier. As the Introduction noted, expertise of judges and counsel, increased bargaining power of the private sector, the lack of political oversight, and the range of crimes investigated by local police add specific local concerns to the legal worries.

B. Stingray Devices

1. Stingray Basics

As protesters in Chicago gathered in the wake of the controversy surrounding Michael Brown's 2014 death in Ferguson, Chicago police seemed to possess detailed knowledge of local organizer Kristiana Rae Colón's phone.[28] A watchdog group recorded police discussing Colón: "She's been on her phone a lot . . . you guys picking up any information where they're going, possibly," with a second officer responding, "Yeah, we're keeping an eye on it," and "we'll let you know if we hear

---

[27] Joseph Cox, *Government Malware Company 'Grey Heron' Advertises Signal, Telegram Spyware*, MOTHERBOARD (Mar. 7, 2018, 8:05 AM), https://www.vice.com/en_us/article/bj54kw/grey-heron-new-spyware-brochure-hacking-team.

[28] Fruzsina Eördögh, *Evidence of 'Stingray' Phone Surveillance by Police Mounts in Chicago*, CHRISTIAN SCI. MONITOR (Dec. 22, 2014), https://www.csmonitor.com/World/Passcode/2014/1222/Evidence-of-stingray-phone-surveillance-by-police-mounts-in-Chicago.

anything."[29] Based on the technical details, the Chicago police likely had a stingray device located near the protesters, sending data to remote officers for analysis. We do not know for sure, because here, as elsewhere, local police often use vague terms to describe their use of such technologies. For instance, Florida police have often referred to stingray device use with the euphemistic "electronic surveillance measures,"[30] also frequently referring to the devices as "confidential intelligence."[31] Another Florida court document merely stated that an investigator "arrived and determined" the location of a tracked phone, without any further detail.[32]

As of November 2018, at least 75 local and state agencies in 27 states have cell-site simulator technologies, colloquially known by a popular brand name—Stingrays.[33] Stingray devices mimic the normal cell towers that enable everyday use of mobile phones, allowing data to pass through a monitored channel rather than through the typical proprietary cell towers. [34] SIM cards in phones use a number called the "International Mobile Subscriber Identity" (IMSI) to interface with cell phone towers. These numbers are unique to each SIM card. [35] When a phone connects to a spoofed cell tower (the stingray device), the phone will reveal this IMSI number to the stingray device.[36] Police can use that number to identify the phone's owner.[37]

In addition to identifying a phone, stingray devices can track the location of a particular phone by measuring the strength of its signal over time using a technique called trilateration.[38] To do so, the stingray

---

[29] *CPD possible Stingray use at #BrownFriday protest,* CLYP (2014), clyp.it/sv23cozu.

[30] Tallahassee Police Dep't Incident Report, Case Report No. 00-08-013508 (Apr. 26, 2008) (on file with the ACLU).

[31] Tallahassee Police Dep't Incident Report, Case Report No. 00-08-037256 (Dec. 01, 2008) (on file with the ACLU).

[32] Tallahassee Police Dep't Incident Report, Case Report No. 00-11-031679 (Nov. 17, 2011) (on file with the ACLU).

[33] *Stingray Tracking Devices: Who's Got Them?* ACLU https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them (last updated Nov. 2018) [hereinafter ACLU].

[34] *See IMSI Catchers*, PRIVACY INT'L (Aug. 6, 2018), https://www.privacyinternational.org/explainer/2222/imsi-catchers.

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] Yomna N, *Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks*, EFF (June 28, 2019).

device must be in proximity to those under surveillance (the data can be sent elsewhere for remote analysis, as with the Colón example above).[39] Given that they mimic cell towers, stingray devices collect data about *all* phones within range, even if the police are only interested in select phones.[40] Some stingray devices apparently have the technical capabilities to collect content information as well as identifying numbers and location, although DOJ policy as of 2015 requires federal stingray devices to be configured so this capability is not in use.[41]

2. Use Statistics

As of November 2018, fourteen federal agencies had stingray devices, which have been used by the federal government since at least 1995.[42] Since 1995, local and state agencies have been able to borrow the equipment from the FBI for their investigations in "exceptional circumstances."[43] It was not until the mid-2000s that state and local forces began acquiring their own equipment, often with federal grant money as part of anti-terrorism efforts.

---

[39] *Id.*

[40] *Id.*

[41] *See Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, U.S. DEP'T OF JUST., 2 (Sep. 3, 2015) ("[C]ell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).").

[42] Federal agencies possessing Stingrays as of November 2018: FBI, DEA, NSA, Secret Service, U.S. Marshals, ICE, ATF, IRS, the Army, Navy, Marine Corps, National Guard, CBP, and U.S. Special Operations Command. *See* ACLU*, supra* note 33; *see also* Ryan Gallagher, *FBI Files Unlock History Behind Clandestine Cellphone Tracking Tool*, SLATE (Feb. 15, 2013, 2:34 PM), https://slate.com/technology/2013/02/stingray-imsi-catcher-fbi-files-unlock-history-behind-cellphone-tracking-tool.html (The brand name "Stingray" first came on the market in 2001) [hereinafter *Gallagher I*]. *See also* Ryan Gallagher, *Meet the machines that steal your phone's data*, ARS TECHNICA (Sep. 25, 2013, 10:00 AM), https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/ [hereinafter *Gallagher II*].

[43] *Gallagher I*, *supra* note 42; *see also FBI* FOIA Release *No. 1182490-000*, U.S. DEP'T JUST. (Feb. 7, 2013), https://epic.org/foia/fbi/stingray/FBI-FOIA-Release-02222013-OCR.pdf.

As stated above, at least 75 local and state agencies in 27 states have cell-site simulator technologies as of November 2018.[44] The earliest record I have found of local acquisition of stingray devices is for the Miami police in 2003.[45] Michigan State Police began using stingray devices by at least 2006.[46] The funding came exclusively from the federal government through the Homeland Security Grant Program.[47] Purchase documents note:

> [T]he ability to track the location of a mobile phone in real time as well as collecting signaling information is vital to the war on terrorism. This equipment will allow the State to track the physical location of a suspected terrorist who is using wireless communications as part of their operations.[48]

Internal documents obtained in 2015 show that the devices have not been, in fact, used for terrorism investigations, but rather to investigate a range of more standard crimes including homicide, fraud, and burglary.[49]

The Los Angeles Police Department (LAPD) acquired Stingray technology in 2004 through a federal government grant program, the Fiscal Year 2004 Homeland Security Grant Program.[50] In 2005, the city council file authorizing the purchase states that, "[i]n response to the recent bombings in London . . . [the LAPD] has responded with a substantial increase in terrorism prevention . . . [and] the LAPD is requesting the expedited purchase" of a stingray device-like technology called a Digital Receiver Technology (DRT).[51]

---

[44] ACLU*, supra* note 33.

[45] *Gallagher II*, *supra* note 42.

[46] Nathan Freed Wessler, *Police Citing 'Terrorism' to Buy Stingrays Used Only for Ordinary Crimes*, ACLU (Oct. 23, 2015, 9:00 AM).

[47] *See* Mich. Dept. of State Police, FOIA Response (to August 10, 2015 Appeal by Daniel S. Korobkin (on file with the ACLU) [hereinafter *Michigan Response*]; *see also* City of Tacoma, Responses to June 20, 2014 FOIA Request.

[48] *Michigan Response*, *supra* note 47, at 11.

[49] Joel Kurth, *Michigan State Police Using Secret Cell Tracking Devices Since '06, Documents Show*, DETROIT NEWS (Oct. 22, 2015, 11:32 PM), https://www.detroitnews.com/story/news/local/michigan/2015/10/22/stingray/74438668/ (last updated Oct. 23, 2015). *See also* Crump, *supra* note 9, at 1598.

[50] Office of the City Clerk, City of Los Angeles, Council File 04-2499-S2 (Aug. 24, 2005).

[51] *Id.*

3. Stingray Device Litigation History: What Legal Authorization is Required?

One of the central questions surrounding stingray devices is what legal authorization police must obtain before using it. The following section sets out the history of litigation over this question in federal courts. Despite this Article's focus on the local and state context, these issues were first litigated and better documented in federal court than in state court. Nonetheless, this history essentially parallels the issues that state courts subsequently had to face.

At a high level, the history of oversight for stingray devices essentially alternates between policy and judicial requirements. First, the federal government had a policy of not obtaining even a court order for stingray device use. Federal courts affirmed this policy. As stingray devices began to be used for location tracking, not just identifying telephone numbers, courts pushed back and required heightened standards to obtain legal authorization. Still, whether law enforcement had to obtain a warrant for such use was not definitively settled in court. Subsequently, the federal government implemented a policy of requiring warrants for stingray use; it was only then that many state courts followed suit in legally requiring warrants. That said, only lower federal courts and some state supreme courts have ruled that searches using stingray devices require warrants as a legal matter; whether warrants are required for stingrays is still technically legally unsettled after more than a decade.

This legal history highlights two particularly important themes in assessing how administrative governance can supplement judicial oversight of new search tools. First, this history highlights a pervasive lack of transparency on the part of the government with not only the public but also with courts. Administrative governance offers the ability to require information disclosure from law enforcement in more ways than the Fourth Amendment does.[52] Specifically, defense counsel and the public were largely unaware of stingray device use until 2010; up to that point, law enforcement typically filed run-of-the-mill trap and trace pen register applications to use stingray devices, which essentially hid the change in technology.[53] Second, the litigation history shows the importance of the interaction between administrative agencies and the judicial branch in achieving up-to-date governance of

---

[52] United States v. Rigmaiden, No. 08-cr-00814-DGC 982, 983 (D. Ariz. Jan. 4, 2012).
[53] *Id.* at 995.

surveillance technologies. Administrative governance, important in its own right, can also prompt change in the judicial branch.

Table 1: Types of Legal Authorization for Seeking Data[54]
(Ordered from most stringent to least stringent)

Type of Court Order	*Type of Data*	*Legal Standard*	*Source*
Wiretap	Content	Super-warrant	18 USC § 2510-2522
Tracking device	Location	Probable cause	18 USC § 3117 (Rule 41)
Subscriber records	Business records	Specific, articulable facts	18 USC §2703(d) (SCA)
Pen register/trap & trace	Incoming/outgoing phone numbers	Certified relevance	18 USC 3121-3127 (Pen/trap statute)

Figure 1

a. No Authorization Required Era, 1995-2005

Early Department of Justice policy on stingray devices, first publicly documented in 1997, stated that neither the Fourth Amendment nor relevant statutes required judicial authorization for using stingray devices to gather non-content data.[55] The earliest documentable case featuring a stingray device involved federal officers seeking what was essentially a Pen/Trap order "out of an abundance of caution," despite contending no order was legally necessary.[56] The officer's application for a court order essentially sought to obtain a legally binding court ruling to that effect.

---

[54] This is adapted from Magistrate Judge Smith's opinion In re Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005). As a note, the dates are rough, because they correspond to public availability of policies; policy changes may actually have occurred earlier.

[55] *See* Executive Office for United States Attorneys, *Electronic Investigative Techniques*, 45.5 USA BULLETIN 1, 13-15 (1997). *See also* Stephanie Pell and Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap,* 16 YALE J. L. & TECH. 134, 158 (2016).

[56] In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 200 (C.D. Cal. 1995). Regarding the status of this case as the "first," court documents do not use standard terminology to refer to stingray devices, meaning large-scale searches for case literature can be limited by authors' term selection; cases may exist earlier than 1995. For papers tracing the history of legal cases relating to stingray devices, *see* Brian L. Owsley, *Triggerfish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183 (2014); *see also* Craig Curtis et al., *Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61 (2014). *See also* Pell and Soghoian, *supra* note 55.

It worked. The court initially rejected the application and asked for more detail from the government, including "who would operate the analyzer, under what circumstances, and how its use would be limited to detecting cellular phones used by the subjects of the . . . investigation."[57] But, upon receiving clarifications, the court determined that a court order was not required to use such a device to collect phone numbers in the manner described.[58] That said, the court included warning language that such devices, used in more invasive ways, might require legal authorization.[59] The court's worries proved prescient, as discussed below.

b. Courts Ratchet Up to Statutory Protections, 2005-2010

By 2005, federal policy changed dramatically, adopting the position that the Pen/Trap statute, as updated by the 2001 PATRIOT Act, applied to stingray device use.[60] Still, this positive policy change correlated with an increase in stingray device use. By the early to mid-2000s, law enforcement agents had more widely begun to use stingrays to identify location information in addition to phone numbers.[61] Federal agents sought legal authorization for prospective location data—obtained via stingray devices or otherwise—in one of two ways, both of which required meeting a "specific and articulable facts" standard.[62] First, they argued that legal authorization could be obtained through the Stored Communications Act (SCA); this view characterized location information as records held by a third-party provider.[63] Second, federal agents argued that the Pen/Trap Statute and the SCA together provided statutory authority for obtaining prospective location data, which became known as the "hybrid theory."[64]

To their credit, courts generally did not accept either version of this argument.[65] Most courts responded to these arguments by requiring

---

[57] In the Matter of the United States*, supra* note 56, at 198.
[58] *Id.* at 199.
[59] *Id.* at 201-02.
[60] Electronic Surveillance Unit, *Electronic Surveillance Manual: Procedures and Case Law Forms*, DEP'T OF JUSTICE, 1, 41 (2005).
[61] Reeve Wood, *The Prolonged Arm of the Law: Fourth Amendment Principles, the Maynard Decision, and the Need for a New Warrant for Electronic Tracking*, 64 ME. L. REV. 285, 311 (2011).
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id*. at 312.

the government to meet a probable cause standard to obtain prospective location information.[66] Still, some courts accepted arguments based on the "hybrid theory," and variation in legal standards emerged between courts.[67] In addition, despite increased judicial scrutiny, all of these debates occurred essentially behind the scenes between the government applicants and courts. Litigant challenges, and accompanying public scrutiny, did not enter the picture until 2010.[68]

c. Public Legal Battles over Warrant Status, 2010-2015

Around 2010, a new wave of legal challenges began.[69] Defendants discovered, and subsequently challenged, use of stingray devices in their criminal cases. Defendants generally argued that warrants, and highly specific ones at that, were required to use stingray devices. The 2010-2013 *United States v. Rigmaiden* litigation is considered the case that made debate over the correct legal authorization for stingray device use public. In this case, a determined pro se litigant uncovered that federal agents had used stingray devices to apprehend him. While in prison on tax fraud charges, Rigmaiden mulled over how the police possibly could have tracked him down; he had been using a tax fraud scheme to fund a largely off-the-grid life.[70] His only weak link, he realized, was the cellular AirCard he used to connect to the Internet to file the fraudulent tax returns.[71] What began as a hunch ([the authorities] sent "rays into my living room") turned into thousands of hours of jailhouse research and tens of thousands of pages of document

---

[66] *Id.* at 311-12 (noting that, as of April 2009, of the 28 reported decisions on prospective CSLI, 20 decisions found that probable cause was required to obtain a court order releasing the information).

[67] *Id.* at 312-13. *See* In the Matter of the Application of the U.S. States for an Order: (1) Authorizing the Installation and Use of a Peen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 411 F. Supp. 2d 678, 679-81 (W.D. La. 2006) [hereinafter *Hornsby I*].

[68] *See* Rigmaiden litigation*, infra* notes 69-76.

[69] *See* United States v. Rigmaiden, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012) [hereinafter *Rigmaiden I*]. United States v. Rigmaiden (Rigmaiden), No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *6 (D. Ariz. 2013) [hereinafter *Rigmaiden II*].

[70] Cale Guthrie Weissman, *How an Obsessive Recluse Blew the Lid off the Secret Technology Authorities Use to Spy on People's Cellphones*, BUSINESS INSIDER (June 19, 2015, 2:04 PM), https://www.businessinsider.com/how-daniel-rigmaiden-discovered-stingray-spying-technology-2015-6.

[71] *Id.*

review.[72] He discovered references in court documents to new "investigative techniques" associated with cell phone towers.[73] He then contacted the ACLU, which helped his legal challenge move forward.[74]

Rigmaiden's case is most notable for bringing public and litigant awareness to the use of stingrays by law enforcement. Rigmaiden lost his Fourth Amendment challenge when the court concluded that the government's legal process to obtain Rigmaiden's location information was sufficient.[75] Subsequent defendant challenges ended similarly, with courts concluding that stingray devices could be used in keeping with statutory (not warrant) requirements, declining to rule on Fourth Amendment grounds, and allowing evidence to appear at trial on the basis of the good faith exception.[76]

But two facets of the *Rigmaiden* case are important for this Article, demonstrating key shortcomings of judicial Fourth Amendment oversight that could be mitigated through administrative governance. First, a subsequent FOIA investigation raised doubts about the forthrightness of the government's representations in court during the *Rigmaiden* litigation.[77] Emails obtained through FOIA, together with the text of the order in question, "suggest agents obtained authorization to use a pen register without indicating they also planned to use a Stingray . . . [and at some point] the government attempted to

---

[72] *Id.*; *see* Manoush Zomorodi, *When your Conspiracy Theory is True*, WNYC STUDIOS (June 18, 2015), https://www.wnycstudios.org/podcasts/notetoself/episodes/stingray-conspiracy-theory-daniel-rigmaiden-radiolab (timestamp 8:15).

[73] Weissman, *supra* note 70*; see* LINDA LYE, STINGRAYS: THE MOST COMMON SURVEILLANCE TOOL THE GOVERNMENT WON'T TELL YOU ABOUT, A GUIDE FOR CRIMINAL DEFENSE ATTORNEYS *ACLU* FROM THE ACLU OF NORTHERN CALIFORNIA 39 (2014) Exhibit ("During the course of this investigation and conferring with TSD agents with the FBI and USPIS, we determined that doing a normal 'Trap and Trace' on the aircard would suffice. [redacted] Essentially we would ping the number associated to the card instead of collecting data from the aircard's connection . . . On 7/16/08, we were informed that they were able to track a signal and were using a 'Stingray' to pinpoint the location of the aircard.").

[74] Rigmaiden first sought discovery of related materials, but the court denied his discovery requests on the grounds of law enforcement privilege. *See Rigmaiden I*, *supra* note 69, at 995. *See also* Weissman, *supra* note 70.

[75] *Rigmaiden I*, *supra* note 69, at 995.

[76] *See, e.g.,* United States v. Espudo, 954 F. Supp. 2d 1029, 1031 (S.D. Cal. (2013). *See also* State v. Tate, 849 N.W.2d 798, 805 (Wis. 2014).

[77] Hanni Fakhoury, *When a Secretive Stingray Cell Phone Tracking "Warrant" Isn't a Warrant*, ELEC. FRONTIER FOUND. (Mar. 28, 2013), https://www.eff.org/deeplinks/2013/03/when-stingray-warrant-isnt-warrant.

transform that order into a warrant that authorized the use of a Stingray."[78] These doubts about law enforcement representations about technology in court reinforce the concerns about government transparency in Fourth Amendment judicial proceedings discussed in subsection 3(b) below.

Second, the *Rigmaiden* case underscores an aspect of Fourth Amendment law that makes judicial scrutiny of novel investigative tools difficult. The court rested its determination of the sufficiency of legal process on the basis that "there is no legal requirement that a search warrant specify the precise manner in which the search is to be executed,"[79] a conclusion well-grounded in Supreme Court precedent.[80] With this body of precedent, courts, acting alone, could find it difficult to force the transparency needed from government agents to allow accurate judicial scrutiny of new search tools and techniques.[81]

In 2012, a magistrate judge highlighted the obfuscation of technical details of new surveillance technologies in a now-famous opinion, refusing to grant the government's application for an pen/trap order for stingray use.[82] In this case, the government sought to use a stingray device to identify the phone number of a new phone that a known subject had begun using.[83] The government sought authorization under the Pen/Trap statute and the SCA, which it represented was the "standard application model and proposed order approved by [DOJ]."[84] But it was only during the actual *ex parte* hearing for the case that a law enforcement agent specified that a stingray device would be used in the investigation.[85]

This revelation informed Magistrate Judge Owsley's decision to deny the application. He pointed to concerns about lack of specifics

---

[78] *Id.*; *see also* Lynda Lye, *DOJ Emails Show Feds Were Less Than "Explicit" With Judges on Cell Phone Tracking Tool*, AM. C.L. UNION (Mar. 27, 2013, 11:06 AM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/doj-emails-show-feds-were-less-explicit-judges-cell.

[79] *Rigmaiden II*, *supra* note 69, at *16.

[80] *See* Dalia v. United States, 99 S. Ct. 1682, 1684 (1979). *See also* United States v. Grubbs, 126 S. Ct. 1494, 1501 (2006).

[81] *But see* In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012).

[82] *Id.* at 752.

[83] Pell and Soghoian, *supra* note 55, at 161.

[84] In the Matter of the Application of the United States, *supra* note 81, at 748-49.

[85] *Id.* at 748.

about how many locations the device would be used in, the duration of the surveillance, and lack of data minimization procedures for incidental data picked up from other phones.[86] He concluded that the government had not successfully provided support that the pen register statute was the appropriate legal authorization for stingray equipment.[87] In a later speech about this decision, Judge Owsley criticized the masking of technical details in orders:

> What they do is present an application that looks essentially like a pen register application . . . [s]o any magistrate judge that is typically looking at a lot of pen register applications and not paying a lot of attention to the details may be signing an application that is authorizing a Stingray.[88]

Indeed, further research through FOIA requests has uncovered additional cases involving stingray devices where the applications for court orders did not include this degree of specificity.[89] In the instant 2012 case, Judge Owsley denied the request and called for more details in future applications.[90]

d. State Law Enforcement Generally Did Not Seek Warrants

The above discussion dealt with federal cases. At the local level, law enforcement generally seems not to have sought warrants for stingray device use. Details are sparse, but one set of court documents from Tallahassee indicates that police used stingray devices 200 times between the spring of 2007 and August of 2010 and that they did not have a policy of seeking a warrant to use the device.[91] In addition, they did have a policy of trying to keep use of the device out of legal documents generally.[92] This held true even for location tracking: in a particular 2008 case, police used a stingray device to track an allegedly stolen phone to and then within an apartment building, entered the

---

[86] *Id.* at 749.
[87] *Id.* at 752.
[88] Ryan Gallagher, *Feds Accused of Hiding Information from Judges About Covert Cellphone Tracking Tool*, SLATE (Mar. 28, 2013, 12:09 PM), https://slate.com/technology/2013/03/stingray-surveillance-technology-used-without-proper-approval-report.html.
[89] Pell and Soghoian, *supra* note 55, at 163.
[90] In the Matter of the Application of the United States, *supra* note 81.
[91] Def.'s Motion to Suppress, Florida v. Thomas, No. 2008-CF-3350A 1, 26 (2010).
[92] *Id.* at 26-27.

apartment, and arrested the holder of the phone, all apparently without a warrant.[93] Similarly, public records requests to the LAPD reveal that the police relied on statutory grounds, not warrant procedures, to authorize stingray device use as of 2012.[94]

The first state case that appears in legal databases as explicitly dealing with a stingray device is *State v. Tate*, a 2014 case from the Wisconsin Supreme Court.[95] This court held that probable cause was the appropriate standard for stingray device authorization and that it was met. This is a laudable and rare decision; generally, explicit judicial pushback at the state level did not come until a later administrative—not judicial—change at the federal level.

e. Federal Policy Change Ripple Effect, 2015-Present

In 2015, the DOJ issued a policy guidance document stating that federal law enforcement agencies "must now obtain a *search warrant* supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure" (emphasis added) for both location-tracking and phone-number identifying uses.[96] In addition, the policy required the kind of technical and use specificity in the warrant application for which Magistrate Judge Owsley and others had called.[97] The DOJ had come under substantial pressure in the wake of allegations of surveillance of protesters reacting to a series of police killings of black citizens. The DOJ document clearly stated that this

---

[93] *Id.* at 25 (Court documents state that police determined they did not need a search warrant to enter the apartment, because they achieved consent to enter. That is hard to square from descriptions of the encounter.). *See* Kate Klonick, *Stingrays: Not Just for the Feds!*, SLATE (Nov. 10, 2014, 9:52 AM), https://slate.com/technology/2014/11/stingrays-imsi-catchers-how-local-law-enforcement-uses-an-invasive-surveillance-tool.html.

[94] Owsley, *supra* note 56, at 217-18.

[95] State v. Tate, *supra* note 76, at 812-13. See *infra* note 102 for search methodology. Given the lack of transparency in many stingray device cases, searches for cases dealing explicitly with these devices may miss earlier cases that, in actuality, did deal with them. For instance, Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) is a good candidate, referencing a pen/trap order, a confidential informant, and "cell site location information given off by cell phones when calls are placed." Although not definitive, these terms are certainly indicative of stingray device use. This court suppressed evidence obtained from warrantless real-time tracking. I credit Jonathan Manes' paper for this case example; *see* Jonathan Manes, *Secrecy and Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L. J. 503, 518-19 (2019).

[96] *See* Department of Justice Policy Guidance, *supra* note 41, at 3.

[97] *Id.* at 5.

new warrant requirement was one of policy, not of law.[98] Still, the department's policy change appears to have prompted a change in court rulings.

After this policy change, state and federal courts started ruling consistently that the government needed to obtain a warrant to use stingray devices. Federal courts explicitly referenced the DOJ policy change.[99] The first state-level decision came from the Maryland Supreme Court in 2016, and it referenced the DOJ policy change.[100] This decision prompted a cascade of conforming lower court decisions within the state.[101] In other states, all decisions issued since have consistently required a warrant for stingray device use; three of these also cited to the 2015 DOJ policy guidance.[102] It seems plausible that

---

[98] *Id*. at 3.

[99] For a list of non-exhaustive federal examples, *see* United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016); United States v. Ellis, 270 F. Supp. 3d 1134, 1139 (N.D. Cal. 2017); Jones v. United States, 168 A.3d 703, 705 (D.C. 2017). *See also* United States v. Tutis, 216 F. Supp. 3d 467, 482 (D.N.J. 2016) (where the district court decided that a state statutory requirement was not materially different from a search warrant and was, as such, sufficient). All of these cases referenced the 2015 DOJ policy change.

[100] State v. Andrews, 227 Md. App. 350, 357 n.20 (2016) (Notably, the case does not cite to the previous Wisconsin Supreme Court decision, *Tate*, even though neither the DOJ policy nor Wisconsin law is binding on Maryland courts.).

[101] The following cases were all consistent with the *Andrews* holding, although most did not grant suppression of evidence by virtue of the good faith exception, *see* State v. Copes, No. 0580, 2016 Md. App. (App. Oct. 25, 2016); Anthony Banks v. State, No. 553, 2017 Md. App. (App. Jan. 26, 2017); State v. Copes, 454 Md. 581, 165 A.3d 418 (2017); Morales-Caceres v. State, No. 1086, 2017 Md. App. (App. Dec. 5, 2017); Elmore v. State, No. 504, 2019 Md. App. LEXIS 649 (App. Aug. 2, 2019); Baskerville v. State, No. 2865, 2018 Md. App.(App. July 20, 2018); Edwards v. State, No. 205, 2018 Md. App. LEXIS 890 (App. Sep. 24, 2018); Hicks v. State, No. 629, 2019 Md. App. LEXIS 782 (App. Sep. 6, 2019); Diggs v. State, No. 1728, 2019 Md. App. LEXIS 1056 (App. Dec. 6, 2019).

[102] The Supreme Court of Massachusetts effectively required warrants for stingray use in Commonwealth v. Almonor, 120 N.E.3d 1183, 1193 (2019), but the court opinion only mentions stingray devices in a footnote. *See id.* at 1193 n.13. However, the case does reference the Supreme Court of Maryland's decision. *See id.* at 1202 n.2. Some State court opinions finding a Fourth Amendment violation also cite DOJ policy change. *See e.g.,* Jones v. United States, 168 A.3d 703, 721 (D.C. 2017); State v. Sylvestre, 254 So. 3d 986, 991 (Fla. App. 4 Dist. 2018) (cites DOJ policy change); People v. Gordon, 58 Misc. 3d 544, 546 (Sup. Ct. 2017); People v. Smith, IL App (1st)

the federal policy change had an effect on both state litigants' willingness to challenge stingray device use and to state courts' willingness to require warrant use.

Still, no final doctrinal answer on the device's constitutional status exists, given that higher courts have not addressed the question directly. Nor have they directly addressed the question of what legal authorization is required for prospective location tracking, although the majority of federal courts require warrants.[103] The Supreme Court did recently require a warrant for historical location tracking data in *United States v. Carpenter*, which lends constitutional credence to the customary warrant requirement for prospective tracking but does not definitively settle the question.[104] The stingray device case history demonstrates that courts have the benefit of slow evolution, but lack legal agility—a particularly acute problem when technological innovation enables novel means of surveillance. This litigation history also demonstrates the impact that administrative change can have on judicial constitutional decision-making.

4. Additional Legal Issues

a. Proprietary Interests Hinder Judicial Oversight

The above history of stingray device litigation demonstrates that sophisticated investigative technologies have not always gotten a fair airing in court, complicating judicial determination of what legal process properly applies. Government agencies have not disclosed, or have not disclosed the full extent of, the nature of stingray devices used during searches. In addition to the above examples, the experience of North Port, Florida (pop. ~70,000) is particularly telling. The North

---

141814-UB (Dec. 27, 2017) (ineffective assistance of counsel claim upheld based on lack of challenge to evidence of stingray use); People v. McDuffie, 2017 58 Misc. 3d 524 (Sup. Ct. 2017) (granting further hearing on whether surveillance had been lawfully obtained). In contrast, some state court opinions uphold use of stingray devices on the basis of adequate warrant. *See e.g.*, Jenkins v. State, 2017 Ind. App. LEXIS 2912; Andres v. State, 254 So. 3d (Fla. 2018) 283, 297-98; People v. Johnson, 25 Cal. App. 5th 588, 624-26 (2018); Commonwealth v. McLendon, 221 A.3d 323 1, 6 (Pa. Super. Ct. 2019); Wheeler v. State, 209 A.3d 24 1, 1 (Del. 2019).

[103] Eric Lode, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1, 17-20 (2015) (collecting cases).

[104] Carpenter v. United States, *supra* note 19, at 2218-21 (2018).

Port police amended a probable cause affidavit to remove details about stingray devices after pressure from an assistant state attorney, who himself seemingly acted at the request of the U.S. Marshals.[105] Court documents in Florida indicate police forces used a wide range of vague terms to substitute for descriptions of stingray devices, including "confidential intelligence."[106]

Private sector pressure contributes to this lack of transparency. Most, if not all, police forces that borrowed or purchased stingray devices signed non-disclosure agreements with the FBI and/or the Harris Corporation barring them from revealing details about the technology's use in court. For instance, in the Tallahassee apartment case described above, the police only revealed the use of stingray devices six years after the incident took place.[107] In Baltimore, the Police Department's nondisclosure agreement stipulated that the department and associated agencies, "shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation . . . beyond the evidentiary results obtained through the use of the equipment/technology."[108]

Pressure came not only from the private vendors but from the federal government. The Baltimore police were required to alert the FBI so it could intervene if it looked like any actor was seeking to introduce this kind of evidence in court.[109] This kind of intervention

---

[105] *See* E-mail from Kenneth Castro, Sergeant, Sarasota Police Department, to Terry Lewis, Chief, North Port Police Department (April 15, 2009, 11:25 AM) (on file with the ACLU) (Stingray device was not named but described in the emails as "equipment which enables law enforcement to ping a suspects cell phone and pin point his/her exact location.").

[106] *See* Tallahassee Police Dep't Incident Report, Case Report No. 00-08-03725 (Dec. 1, 2008) (on file with the ACLU) ("Confidential intelligence indicated that property stolen during the home invasion robbery was in the area ….").

[107] Klonick, *supra* note 93 ("[I]t wasn't until 2014, six years after Thomas' arrest, that his lawyers found out that a Stingray had been the basis for entering Thomas' apartment.").

[108] Letter from Ernest Reith, Acting Assistant Dir., FBI, to Frederick H. Bealefeld, III, Police Comm'r, Baltimore Police Department (July 13, 2011) (on file with the U.S. Dep't of Justice).

[109] *Id.* ("If the Baltimore Police Department [and other associated agencies] … learns that a District Attorney, prosecutor, or court is considering or intends to use or provide any information concerning the Harris Corporation wireless

actually did occur in Sarasota, Florida: U.S. Marshals raided a Sarasota police office to remove documents that were being reviewed in response to a FOIA request regarding Stingray use.[110]

The government has been so committed to these nondisclosure agreements that they have dropped cases when defense attorneys have pressed for technical details about investigative tools. In Baltimore, prosecutors quickly agreed to drop a case rather than reveal how crucial information was obtained when pressed by the defense.[111] In Tallahassee, after a judge asked for more information on the investigative tool used, the police offered a better plea deal in exchange for not revealing that information.[112] But, in many other cases, defense attorneys didn't press, or didn't know to press, for this information. The fates of defendants have, then, been dependent on the effectiveness of counsel rather than proper procedure—not the way the Fourth Amendment is supposed to work. The ubiquity of NDAs and the rapid withdrawal of cases when more information is requested means courts are being hobbled in functioning as proper arbiters this technology. Indeed, only a few judges have pushed back against the vagueness of government submissions about the tools used in searches.[113] Whatever

---

collection equipment/technology . . . in a manner that will cause law enforcement sensitive information relating to the technology to be known to the public, [these agencies] will immediately notify the FBI in order to allow for sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise.")

[110] Kim Zetter, *U.S. Marshals Seize Cops' Spying Records to Keep Them from the ACLU*, WIRED (June 3, 2014, 6:15 PM), https://www.wired.com/2014/06/feds-seize-stingray-documents/.

[111] *See* Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 23, 2015, 4:50 PM), https://www.usatoday.com/videos/tech/personal/technologylive/2015/08/24/32131267/) (last updated Aug. 24, 2015). *See also* Official Transcript of Proceedings (Motions Hearing), 73, State of Maryland v. Taylor, No. 114140031 (2014).

[112] Trevor Aaronson, *Hacking Team Data Breach Provides Links to Florida Law Enforcement*, TAMPA BAY TIMES (July 11, 2015) https://www.tampabay.com/news/publicsafety/hacking-team-data-breach-provides-links-to-florida-law-enforcement/2237006/.

[113] *See* In re Warrant to Search Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013) ("This 'method' of software installation is nowhere explained. Nor does the Government explain how it will ensure that only those 'committing the illegal activity will be…subject to the technology'"). *See also* Orin Kerr, *Executing Warrants for Digital Evidence: the Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV.

legal process courts decide to require for stingray devices use, this lack of transparency decreases the ability of that court oversight to actually reach these technologies.

b. The Human Factor: Multifunctionality, Mistakes, and Malfeasance

Stingray devices, as described above, can collect more types of data than phone numbers, with the same device potentially requiring different types of legal processes for different use cases. A 2005 copy of the DOJ's Electronic Surveillance Manual confirms that "[d]igital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications."[114] Guidance from a major stingray vendor states their devices that are capable of "intercepting outgoing calls and SMS messages sent by a target."[115] In response, DOJ policy required that, without further legal process, stingrays must be configured as pen registers.[116] Furthermore, after 2015, federal law enforcement requires warrants for stingray device use as a matter of policy, but not of law.[117]

The ability of one technological device to collect multiple types of data does not present an insurmountably difficult legal problem, but it does present a challenging human one. The government is capable of compliantly using a multi-capacity investigatory tool—by applying for the correct legal approval for each type of data collection. This complexity, however, raises the chances of mistakes and malfeasance. For instance, in the past, when the FBI has used malware that obtains multiple types of differently-protected data, it has sometimes failed to apply for the stricter form of legal process.[118] Similar failures could

---

1, 15 (2015) (for Orrin Kerr's arguments regarding particularity's problems with digital searches).

[114] Electronic Surveillance Unit, *Electronic Surveillance Manual: Procedures and Case Law Forms*, U.S. DEP'T OF JUSTICE 41 (2005).

[115] Gamma Group, *3G-GSM Tactical Interception & Target Location*, at 9. *See also* PKI Electronic Intelligence GmbH Germany, *Active GSM Monitoring System, available at* http://www.pki-electronic.com/products/interception-and-monitoring-systems/active-gsm-monitoring-system/.

[116] *See Electronic Surveillance Manual, supra* note 114, at 41. *See also* DOJ Stingray Guide (2015), *supra* note 41, at 2.

[117] DOJ Stingray Guide (2015), *supra* note 41, at 3.

[118] *See* In re Warrant to Search a Target Computer at Premises Unknown, *supra* note 113, at 759-61. *See also* Mayer, *supra* note 10 (activation of computer webcam required "super-warrant" protections, adherence to wiretap standards).

occur in the stingray device context. Of course, the lack of transparency regarding stingray device usage might frustrate judicial attempts to determine such failures. Similarly, law enforcement is required to minimize collected data not relevant to the ongoing investigation; but, based on volume alone, devices that collect a broader range of data increase the risk that minimization techniques will contain errors. Furthermore, local and state agencies do not have the same resources, legal advice, or coordination abilities as federal law enforcement, magnifying the potential for confusion or mistakes. Widespread use of these kinds of technologies by police puts pressure on *legal* protections to do more work—technologies with many capacities do not have the required embedded *technological* hard-stops.

Such technologies also put pressure on non-search-related legal processes. Acquisition of surveillance technologies have sometimes been kept from public view, skirting the intended oversight procedures. For instance, the Chicago police, which have had stingray devices since at least 2008, purchased at least a portion of these and other surveillance capabilities using a narcotics asset forfeiture fund, the "1505" fund.[119] Using these funds allows the police to bypass the City Council budget process.[120] Council members were thus not informed or aware of the police department's use of these technologies for four years, until activists started requesting public records.[121] As a consequence, they had no opportunity to undertake any oversight activities. Surveillance technology, in this manner, exerts legal pressure on multiple sites of governance.

c. Mission Creep and Enforcement Discretion

Even though state and local law enforcement grant applications often list anti-terrorism efforts as validation for acquiring sophisticated investigative technologies, these tools also end up being used to solve

---

[119] *See* Justin Glawe, *Freddy Martinez is Exposing Chicago Cops' NSA-Style Surveillance Gear*, VICE NEWS (Mar. 30, 2015, 9:00 PM) https://www.vice.com/en_ca/article/qbx89p/stingrays-and-secrets-how-the-chicago-police-department-was-forced-to-come-clean-330. *See also* Eördögh*, supra* note 28. *See Opening the Chicago Surveillance Fund*, MUCKROCK https://www.muckrock.com/project/opening-the-chicago-surveillance-fund-25/.

[120] Joel Handley, Jennifer Helsby, and Freddy Martinez*, Inside the Chicago Police Department's Secret Budget*, CHICAGO READER (Sept. 29, 2016) https://www.chicagoreader.com/chicago/police-department-civil-forfeiture-investigation/Content?oid=23728922.

[121] Glawe, *supra* note 119.

low-level theft, identify prison contraband, and locate witnesses.[122] These are permissible and legal exercises of police power. At the same time, enforcement discretion is a concept built into the criminal justice system.[123] Sophisticated investigative technologies reduce resource constraints and allow police to access more data for a wider range of crimes. Resource constraints motivate enforcement discretion; with lessened constraints comes fewer material reasons for such discretion.[124] Deciding when surveillance tools can be used purely on the basis of material constraints preempts a wider democratic discussion about the role of enforcement discretion in policing.[125]

C. Mobile Forensics Devices

1. "Hack and Crack" Introduction

If you've ever forgotten your iPhone's password, tried a few guesses, and then been informed you are running out of attempts and will be locked out of your phone, you have experienced some of the frustration police officers face when trying to unlock suspects' phones. Password cracking can sometimes be the only way to get into a phone, given default iPhone encryption—especially when suspects have died. Private companies have stepped in to provide devices that bypass the "too many guesses" protection: these devices first "hack" iPhones, exploiting vulnerabilities in the software that allow disabling of this protective feature. The devices can then proceed to crack the password in hours or days.[126]

---

[122] Baltimore Police Dep't, Response to Request 060815 (2015) (on file with *USA Today*).

[123] *See generally* DAVIS, DISCRETIONARY POLICING, *supra* note 11; *see also* David M. Jaros, *Preempting the Police*, 55 B.C.L. REV. 1149, 1149 (2014). *See* Harold E. Pepinsky, *Better Living Through Police Discretion*, 47 LAW & CONTEMP. PROBS. 249, 249 (1984).

[124] *See* Elizabeth E. Joh, *Discretionless Policing: Technology and the Fourth Amendmen*t, 95 CAL. L. REV. 199, 234 (2007).

[125] *See generally* Erik Luna, *Transparent Policing*, 85 IOWA L. REV. 1107 (2000); s*ee also* Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 Yale L.J. 2054, 2054 (2017); *see also* Dan M. Kahan and Tracey L. Meares, *Foreword: The Coming Crisis of Criminal Procedure*, 86 GEO. L.J. 1153, 1153 (1998). *See* Floyd Weatherspoon, *Ending Racial Profiling of African-Americans in the Selective Enforcement of Laws: In Search of Viable Remedies*, 65 U. PITT L. REV. 721, 725 (2004).

[126] Joseph Cox, *Cops Around the Country Can Now Unlock iPhones, Records Show*, MOTHERBOARD (Apr. 12, 2018, 9:52 AM), https://www.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police.

The story of mobile forensic devices mirrors the stingray device story in many ways: the devices trickled down from federal to state use, and their use has been marked by debate, although less extensive than in the stingray device context, over what legal authorization is required to use them. This section will focus, however, on two additional legal risks that mobile forensics devices pose. These risks highlight existing shortcomings in non-judicial systems of oversight of these technologies. First, these devices demonstrate the difficulties in crafting effective oversight at the site of exchange of technologies from federal to local law enforcement. The history of mobile forensics devices demonstrates how gaps can appear between systems designed for local governance and systems designed for federal governance when technologies move between the two. Second, the history of these devices demonstrates the shortcomings of relying on procurement policy alone to counter the risks that local police surveillance carries.

2. Technical Details and Use Statistics

Physically, mobile forensics devices are small, around four inches on a side, with cables that connect to iPhones.[127] The licenses to cheaper, newer models called Graykey made by the company GrayShift cost between $15,000 (allowing 300 unlocks at $50 per device) and $30,000 (unlimited unlocks) per year and work, as of April 2018.[128]

Cellebrite, one of the main companies selling these devices and licenses, has been in the mobile forensics market since 2007, the same year the first iPhone came out.[129] The FBI has contracts with this Israeli company going back to 2009.[130] Worldwide, Cellebrite has distributed 60,000 licenses in 150 countries.[131] The company's main model is the Universal Forensic Extraction Device (UFED), but it has offered a changing array of devices that adapt as mobile technology changes.[132]

---

[127] Thomas Reed, *GrayKey iPhone Unlocker Poses Serious Security Concerns*, MALWAREBYTES LABS (Mar. 15, 2018), https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/.

[128] Cox, *supra* note 126.

[129] *Company Profile*, CELLEBRITE, https://www.cellebrite.com/en/about/company/ (last visited Aug. 8, 2020).

[130] Kim Zetter, *When the FBI Has a Phone It Can't Crack, It Calls These Israeli Hackers*, THE INTERCEPT (Oct. 31, 2016, 8:12 AM), https://theintercept.com/2016/10/31/fbis-go-hackers/.

[131] Company Profile, *supra* note 113.

[132] *Id.*

The federal government released a report on Cellebrite technology performance on a range of phones in 2012, demonstrating widespread government interest in the technology.[133] Cellebrite's major competitor is Swedish firm MSAB, with reports of at least six other companies active in the space, including the relatively new U.S. firm GrayShift.

At least four federal agencies possess Cellebrite or Grayshift forensics technology, with the earliest acquisitions in 2009.[134] The FBI started acquiring other kinds of mobile forensics technologies around 2003, although it is likely an even older feature of federal law enforcement investigations.[135]

Local and state law enforcement first had access to mobile forensics capabilities through FBI programs. Initially, local and state agents could request full forensics examinations from FBI personnel, but extensive backlogs built up.[136] In response, the FBI introduced a fast-track option, "Cell Phone Investigative Kiosks," which were available for local and state agents to use at FBI field offices and Regional Computer Forensics Laboratories.[137] Agents could use the kiosks on a walk-in basis, and agents were usually required to use this

---

[133] NAT'L INST. OF JUSTICE, TEST RESULTS FOR MOBILE DEVICE ACQUISITION TOOL: CELLEBRITE UFED 1.1.8.6– REPORT MANAGER 1.8.3/UFED PHYSICAL ANALYZER 2.3.0, 70-197 (2012).

[134] FBI, DEA, State Department, and Coast Guard. For FBI, *see On February 16, DOJ Got a Warrant to Open an iPhone 6 Using Cellebrite*, EMPTYWHEEL (Mar. 23, 2016) https://www.emptywheel.net/2016/03/23/on-february-16-doj-got-a-warrant-to-open-an-iphone-6-using-cellebrite/. For FBI acquisition date, *see* Zetter, *supra* note 130. For DEA, *see* Joseph Cox, *The DEA Says it Wants that New iPhone Unlocking Tool 'GrayKey',* MOTHERBOARD (Mar. 28, 2018, 12:11 PM), https://www.vice.com/en_us/article/mbxba4/graykey-grayshift-dea-iphone-hack. For State Department, *see* Joseph Cox, *State Department Seemingly Buys $15,000 iPhone Cracking Tech Graykey*, MOTHERBOARD (Mar. 24, 2018, 9:45 AM), https://www.vice.com/en_us/article/kzxwwz/state-department-seemingly-buys-dollar15000-iphone-cracking-tech-graykey. For Coast Guard, *see* Thomas Brewster, *Did a Secretive US Government Unit Just Splash $30,000 on an 'Unlimited' iPhone Unlocking Tool?*, FORBES (May 11, 2018, 9:37 AM), https://www.forbes.com/sites/thomasbrewster/2018/05/11/coast-guard-buys-30000-iphone-hacking-company-grayshift-tech/#7a3388d2fbaa.

[135] DEP'T OF JUSTICE, FBI LABORATORY 2003 REPORT (2003).

[136] DEP'T OF JUSTICE, REGIONAL COMPUTER FORENSICS LABORATORY ANNUAL REPORT (2009) at 11, 41, 63.

[137] DEP'T OF JUSTICE, CELL PHONE INVESTIGATIVE KIOSKS–A HANDS ON DIGITAL PREVIEW SOLUTION TO HELP INVESTIGATORS GET THE RESULTS THEY NEED NOW (2009).

option before requesting a full forensic phone investigation from the FBI.[138] The kiosks were clunky and stationary, and could only extract and preview a limited amount of data. But they still provided some technical capabilities to state and local officers and demonstrated forensics cooperation between the FBI and other law enforcement agencies.

As of 2016, according to public records requests, twenty state agencies had mobile forensic capabilities.[139] As of August 2020, at least twenty-three local agencies had mobile forensics capabilities.[140] The most prevalent brand in use among state and local agencies is Cellebrite, but agencies also possess devices made by MSAB, Susteen, Grayshift, and Oxygen Forensics (a Russian company).

Based on a review of publicly available documents, most state law enforcement agencies first acquired these devices between 2010-2014.[141] Local departments tended to make their first acquisitions of Cellebrite between 2012-2016, with a few earlier and later outliers.[142] For instance, Baltimore County police purchased Susteen equipment in 2008 and Cellebrite technology in 2009, essentially at the same time as the FBI acquired Cellebrite technology.[143] Baltimore County, then, bucks the general trend that technology tends to be adopted first by the federal level and then by state and local level. Decreasing product prices and aggressive marketing by surveillance tech companies directed at local and state agencies may be shortening the expected time lag between federal and state or local acquisition—making the need to

---

[138] *Id.*

[139] Joseph Cox, *US State Police Have Spent Millions on Israeli Phone Cracking Tech*, MOTHERBOARD (Dec. 21, 2016, 6:30 AM), https://www.vice.com/en_us/article/aekqkj/us-state-police-have-spent-millions-on-israeli-phone-cracking-tech-cellebrite.

[140] For the local agency figure, I worked through the responsive documents available at MuckRock's Mobile Forensic Tools FOIA page, https://www.muckrock.com/search/?page=1&per_page=100&q=Mobile+Phone+Forensics+Tools.

[141] This date range was obtained by working through each of the documents appended to Cox, US State Police, *supra* note 139, available at https://www.documentcloud.org/public/search/projectid:30764-Mobile-Forensics-Document-Package.

[142] *See Cellebrite FOIA Requests*, MUCKROCK (2020), https://www.muckrock.com/foi/list/?q=cellebrite.

[143] *See* Baltimore Police Dep't Response to Mar. 29, 2017 FOIA Request by Curtis Waltman (June 5, 2017) (on file with MuckRock, filenames "MPIA – Susteen – 1 PO and 1 EA" and "Cellebrite P508164").

address the risks of these technologies at the state and local level all the more pressing.

3. Legal Issues

a. Police Use Technological Change to Broaden Existing Fourth Amendment Exceptions

As with stingray devices, mobile forensics tools have raised questions about appropriate legal authorization. But with these devices, I want to highlight a slightly different angle of this question: the push and pull over the right amount of legal authorization that accompanies changes in technological friction. The following example highlights the need for governance that can respond to changing circumstances.

In areas where legal friction is already low—such as the diminished Fourth Amendment protections that apply at the border and to searches pursuant to consent—the decreased technological friction of new surveillance technologies magnifies the legal risks. Indeed, police departments have already used mobile forensic technologies in border searches.[144] Police departments have also used them in searches pursuant to consent.[145] Courts have, so far, pushed back, recognizing that these areas of legal leeway were crafted before it was possible to "keep the intimate data available on modern cell phones indefinitely and search through it at any time."[146] Still, the law is still evolving, and ultimate legal answers may take years to emerge, as with stingrays.

Change in legal arguments can also happen in response to *increases* in technological friction. In 2018, Apple announced a software update that frustrated common police use of mobile forensic devices.[147] This update "locked" an iPhone's cable port after one hour of not being used to prevent police and others from using plug-in

---

[144] Sophia Cope and Adam Schwartz, *Ninth Circuit Goes a Step Further to Protect Privacy in Border Device Search*, ELEC. FRONTIER FOUND. (Aug. 22, 2019), https://www.eff.org/deeplinks/2019/08/ninth-circuit-goes-step-further-protect-privacy-border-device-searches; United States v. Cano, 934 F.3d 1002, 1013 (9th Cir. 2019) (border search exception does not justify use of mobile forensics devices to record data for further processing).

[145] United States v. Gallegos-Espinal, 2019 U.S. Dist. LEXIS 87258 2 (S.D. Tex. May 23, 2019) (digital forensics analysis of phone exceeded scope of *consent* to search).

[146] *Id.* at 51.

[147] Riana Pfefferkorn, *Exigent Circumstances: iOS 12's USB Restricted Mode and Warrantless iPhone Access*, JUST SECURITY (June 22, 2018) https://www.justsecurity.org/58345/exigent-circumstances-ios-12s-usb-restricted-mode-warrantless-iphone-access/.

mobile forensics tools. Thus, Apple introduced greater technological friction into the process. In response, law enforcement sought to reduce the legal friction required to use such tools. After this change was announced, the Department of Justice began contemplating using the "exigent circumstances" exception to Fourth Amendment procedures to gain access to devices in response to the shortened time frame.[148] Essentially, they wanted to implement a "copy first, get warrant later" approach to devices given the time pressures introduced by the Apple software update.[149] This approach could result in every suspect's phone being downloaded pursuant to an exception to the Fourth Amendment, perverting the nature of exigent circumstances. Based on unresponsive public records searches, this approach does not appear to have been adopted yet, but the example demonstrates the legal uncertainty that can happen in response to technological changes in surveillance tools, even when the underlying questions of law appear relatively settled (i.e., you do need a warrant to review the contents of a phone). This fluidity underscores the need for responsive Fourth Amendment governance.

b. Lack of Oversight at the Point of Trickle-Down

The movement of technology from the federal government to local agencies can also be a site of where existing systems of governance, judicial and non-judicial, fail. With stingray devices, we saw how non-disclosure agreements led to stingray devices being shielded form judicial scrutiny. Mobile forensics devices provide two additional examples of failure at the site of exchange. First, federal grants and loans undermine local control of policing by bypassing established channels of local governance.[150] As scholars have set out at length in other work, devices purchased or obtained through federal grants essentially short-circuit local governance mechanisms that are not built to consider this kind of outside funding.[151] Trickle-down surveillance technologies thus become a way for the federal government to assert its policy priorities within local institutions over which it has no formal control.[152] Thinking comprehensively about

---

[148] *Id.*

[149] *Id.*

[150] *See* Crump, *supra* note 9, at 1598. *See also* Elizabeth Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 20, 20-21 (2017).

[151] *See* Crump*, supra* note 9.

[152] *Id.*

governance of surveillance tools thus requires addressing municipal polices on accepting federal aid—an issue which certainly is not raised by individual Fourth Amendment challenges.

Second, gaps in oversight in local borrowing or use of federal tools can lead to increased possibilities for abuse.[153] In these circumstances, judicial review of abuse certainly provides a backstop—if such abuses come to light. Still, this risk is worth noting, and the cell phone investigative kiosks (CPIKs), an early form of mobile forensics trickle-down, provide a good example of such a gap happening. FBI field offices, regional computer forensic laboratories, and resident agencies (scaled-down field offices) house CPIKs that local and state agencies can use to view, extract, and store data on a cell phone.[154] Multiple FBI audits have reported significant concerns about the potential for abuse of these walk-in hacking kiosks by local and state law enforcement.[155]

For example, the New Jersey office's kiosk is located in its reception area.[156] Although the device technically requires an appointment to use, local and state agents are not required to sign the visitors log and not required to demonstrate that all members of their party are related to the stated investigation.[157] A 2016 audit reported that the "check" in place at the New Jersey site involved keeping the cables needed to access the kiosk with an on-site official.[158] Although the audit concluded this method was sufficient, in reality, this method was ineffective. These cables are likely commonly available consumer electronics, meaning local or state agents could bring their own set, and, even if they are proprietary, such cables are probably available through other means to someone within law enforcement.[159]

More importantly, no effective system existed to verify that local and state officials possessed the necessary legal authorities to use the kiosks to search devices. The 2016 Inspector General's report on the

---

[153] *See* Office of the Inspector General, *Audit of the FBI's New Jersey Regional Computer Forensic Laboratory*, U.S. DEP'T OF JUSTICE (Mar. 2016), [hereinafter *NJ Audit*].

[154] *Id.* at 5.

[155] *Id.* at 7. *See* Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Philadelphia Regional Computer Forensic Laboratory,* DEP'T OF JUSTICE 14 (Apr. 2015).

[156] *NJ Audit*, *supra* note 153, at 5.

[157] *Id.*

[158] *Id.*

[159] Tim Cushing, *Inspector General Says FBI Not Doing Enough to Prevent Abuse of Cell Phone Forensic Equipment by Law Enforcement Officers*, TECHDIRT (Apr. 13, 2016, 3:26 AM).

New Jersey Regional Computer Forensics Laboratory (NJRCFL) stated that "neither the FBI nor the NJRCFL provided any confirmation to show that NJRCFL Kiosk users possessed the proper legal authority to search for evidence on the devices examined."[160] Specifically, the form users are required to fill out before using the kiosk "does not request that the person . . . list the specific legal authority for the examination, nor does it even offer a list of possible legal authorities for conducting such a search" against which the stated reason could be checked.[161] In addition, "the FBI did not provide us with any information regarding controls in place at the NJRCFL to ensure that users do not use the Kiosk for non-law enforcement matters, an inherent risk of Kiosks without adequate controls."[162] All of these features mean that local and state law enforcement officials, lacking proper knowledge, or seeking to skirt legal requirements, could do so.

This scenario demonstrates several risks common across local and state use of sophisticated investigative technologies. First, we only know about these failings in the kiosk context because of the Inspector General's report. State and local law enforcement agencies do not uniformly have that same kind of independent oversight, potentially allowing possible sites of abuse to go undetected. Second, the scenario raises two failings of the federal government when it comes to assisting local surveillance: the federal government has too much control in the sense that its grant process can bypass local procurement decision-making, and, simultaneously, the federal government has too little control, in the sense that it fails to implement adequate supervision for local use of federal tools.

c. Accelerated Marketing Targeting Local Police and Procurement Policy Pressures

The acquisition patterns of mobile forensics technologies suggest that, increasingly, surveillance tools will be sold directly to local and state law enforcement rather than flowing through the federal government to localities. The lag time between federal acquisition of the most recent generation of mobile forensics tools and local acquisition is significantly diminished compared to stingray devices. Where state and local acquisition of stingray devices lagged by half a decade or a decade behind federal acquisition, state acquisition of Cellebrite technology and similar devices lagged only by two to four

---

[160] *NJ Audit*, *supra* note 153, at 6.
[161] *Id.*
[162] *Id.*

years, with local acquisition still lagging five to ten years.[163] With a notable exception—Baltimore acquired its own Cellebrite devices in 2009, at the same time federal law enforcement agencies did.[164]

This acceleration at the state and local level is reinforced by the marketing practices of several other surveillance companies. Clearview AI, which sells a facial recognition product to law enforcement that allows agents to compare suspects with a database of online photographs, has experienced sales success by offering free trials to individual officers within police departments, who then lobby their departments to acquire the software and endorse the product within police circles.[165] Amazon has also aggressively targeted local police departments with marketing campaigns for its Ring surveillance doorbell.[166]

This direct-to-locals approach increases the ways in which private companies can assert leverage over police policies, including restricting what details they can reveal in court through NDAs or intellectual property-based challenges, causing transparency problems.[167] A reporter covering Clearview AI even discovered that the company monitors what faces police departments run through the app and rebukes them for speaking to the media—which indicates the ability to pressure departments regarding other uses, too.[168] Local departments, with limited resources and high local democratic pressure to solve crimes, may be more susceptible to aggressive marketing tactics and less sophisticated negotiating partners than federal law enforcement.

Procurement policy regulates how police acquire new tools. As such, it has been held up as a potential locus of oversight of surveillance tools. Procurement policy is definitely part of the solution, but it is not designed to provide the kind of comprehensive governance needed to

---

[163] *See supra* notes 134 and 141-142.

[164] *See* Baltimore Police Dep't, *supra* note 143.

[165] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (last updated Feb. 10, 2020).

[166] Kari Paul, *Amazon's Doorbell Camera Ring is Working with Police—and Controlling What They Say*, THE GUARDIAN (Aug. 30, 2019, 1:00 PM), https://www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor.

[167] *See, e.g.,* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV 1343, 1343-44 (2018).

[168] Hill, *supra* note 165.

address all of the risks that accompany these surveillance tools. First, procurement policy is a child of broader municipal or state budgeting processes, during which many competing factors, especially fiscal factors, matter. Second, such processes do not necessarily afford opportunities for a range of stakeholder voices to be present, raising concerns about the democratic accountability of such processes. Third, the central goal of procurement policy is to determine whether and how a tool should be acquired; it is not structured to provide the kind of fine-grain control over use of technologies that these tools' risks require. Fourth, placing oversight solely at the site of acquisition encourages police to skirt formal processes in favor of other procurement avenues. For instance, Chicago police, have used $417,000 worth of civil asset forfeiture money from 2010-2016 to purchase stingray devices, bypassing normal procurement procedures.[169]

Procurement policy can offer helpful lessons for administrative governance and form a part of a comprehensive governance scheme. Indeed, procurement provisions can be a helpful part of broader administrative strategies. For instance, a broader administrative governance scheme could require that procurement contracts cannot be accompanied by non-disclosure agreements with private entities. But, overall, non-judicial governance needs to be broader than what procurement policy can offer.

D. Summary of Limits of Judicial Oversight

The next Part investigates how local administrative governance can respond to these challenges. But, I'll first bring together the legal difficulties of local surveillance technology for a more comprehensive picture. These sophisticated investigative technologies both exacerbate existing criticisms of judicial oversight and introduce new concerns.

The above sections tell a story of judicial deference: when sophisticated investigative technologies present questions of unsettled law, courts have tended to defer to government arguments over the arguments of defendants. Courts did not always do so; indeed, courts rightly challenged government policy regarding the legal authorization required for using stingray devices for location tracking. But, at the early stages of the technology's use, and towards the later stages, courts were generally deferential towards government policy and sometimes only became stricter only after an administrative policy change at the federal government level. Judicial deference towards law enforcement

---

[169] Handley et al., *supra* note 120.

is a well-documented phenomenon, but sophisticated investigative technologies aggravate this trend.[170] This deference likely contributes to the failure of courts to decide crucial questions about investigative technologies in a technologically meaningful timespan. Courts are notoriously slow; although this staid pace has the advantages of caution, it is particularly mismatched to the pace of technological change, in several instances leaving crucial questions unanswered and vulnerable groups unprotected for a decade.

Judicial deference towards government or law enforcement perspectives motivates another oft-raised criticism of judicial oversight, that it lacks democratic legitimacy.[171] Clearly, enough pressure existed for the federal government to change its policy on stingray devices, but the courts were not responsive to this same pressure until that federal administrative policy change occurred. Until that point, the courts, as described above, continued to bolster law enforcement perspectives. This dynamic raises the possibility of needing some external force—legislative or administrative—to prompt judicial change.

The involvement of private companies as vendors of sophisticated investigative technologies introduces significant concerns about transparency in legal proceedings, limiting the ability of courts to carry out proper adjudication of Fourth Amendment questions. A double pressure towards secrecy exists with regards to sophisticated investigative technologies: governments want to keep investigative methods secret and vendors want to protect trade secret information. This double pressure may require external intervention to require or incentivize transparency on the part of the government and/or vendors to allow courts to carry out effective oversight.

The technologies above raise considerations that the traditional Fourth Amendment analysis is not built to analyze.[172] In typical Fourth Amendment analyses, courts do not ask the questions raised here: is this tool appropriate for use in relation to *this* crime? Did the federal government set up adequate controls over technology *before* lending or giving it to state and local agencies? Is this tool appropriate for use

---

[170] For general instances of courts privileging law enforcement perspectives, *see* Friedman and Ponomarenko, *supra* note 4, at 1891-92; Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 227-33 (2015).

[171] Friedman and Ponomarenko, *supra* note 4, at 1827.

[172] *See* Renan, *supra* note 3, at 1039 (Renan terms this typical method "transactional" Fourth Amendment analysis, between the defendant and the government).

despite the public externalities it generates? Did private actors restrict what government representatives can say in court or do in the field?

Courts are still a critical component of Fourth Amendment oversight and are equipped to address some of the complexities introduced by sophisticated investigative tools. Questions surrounding appropriate notice of digital searches, for instance, could be addressed by courts, and courts have shown early signs of pushing back against using technology to widen existing legal loopholes.[173] Although courts cannot prevent law enforcement from making mistakes with multifunctional devices, they can exert ex post penalties. Similarly, conflicts between federal and state or local use of overlapping digital tools are likely to arise, and courts, as the arbiter of preemption questions, would be the suitable forum to adjudicate such conflicts. Courts should remain a central and active component of Fourth Amendment oversight, but that does not preclude augmenting their judgment with other governance tools better suited to modulating the particular risks that accompany local use of surveillance tools.

II. THE CASE FOR LOCAL ADMINISTRATIVE GOVERNANCE

A. What is Local Administrative Governance?

1. General Structure of Local Administrative Governance: Two Models

Administrative governance has three key features: it separates the rule makers from those whom the rules regulate, limits the discretion by which decisions will be made, and establishes such criteria before decisions occur. When looking for administrative governance at the local level, it is these features this Article focuses on; many of the structural aspects of traditional administrative governance look different at the local level.

---

[173] Some courts have started requiring ex ante search protocols, including delineating particular pockets of stored data that are more sensitive and protections for examining them. *See, e.g.*, In re [Redacted]@gmail.com, 62. F. Supp. 3d 1100, 1102-04 (N.D. Cal.) (re a cloud service search, suggesting that the government must request information subject to date restrictions and commit to disposing the information after its relevant use); In re Search of Info. Associated with [Redacted]@mac.com, 25 F. Supp. 3d 1, 4-9 (D.D.C. 2014) (calling for use of screening criteria to narrow a request to an online service); United States v. Winn, No. 14-CR30169-NJR, 2015 U.S. Dist. LEXIS 15240, at *25-35 (S.D. Ill. Feb. 9, 2015) (invalidating a warrant to search a phone for "any or all files contained on said phone" as insufficiently particular).

Local administrative governance of police investigative technology looks something like this: a city council or appointed commission would be empowered to regulate the acquisition and use of surveillance technologies by local police. The rules made by such a body would establish the general principles by which specific decisions about particular technologies would be made as they arise. As police seek to acquire new technologies, the body would apply these established principles of decision-making to particular scenarios. Among the general principles that these bodies should adopt are requiring approval for acquisition and use plans for technologies, banning or requiring transparency for NDAs, and granting standing to challenge acquisitions that fail to conform to the guidelines.[174] In addition, I argue that such principles should include warrant requirements, restrictions on sharing or borrowing equipment with other local or state law enforcement agencies, and approval requirements for borrowing from the federal government.

This approach broadly describes what a small but growing number of cities are doing with respect to surveillance technologies. Cities have generally implemented one of two versions of local administrative governance of surveillance. The first form is closer in form to traditional administrative governance, involving a separate administrative agency, and is often adopted by better-resourced cities. Here, a city council establishes an administrative agency or board that receives and reviews surveillance impact and use plans and annual reports. Even in this form, however, the city council usually retains final approval, a key difference from traditional administrative governance. Another difference is that the regulated agencies draft the initial use plans and present them to the administrative body for approval—rather than the administrative body acting as the drafter of those plans.

The second form of local administrative governance operates similarly, but no separate administrative body exists—the city council performs both legislative and administrative functions. In this model, the city council, in its legislative capacity, passes an ordinance establishing the procedures for review of rules about surveillance technologies. Then, in its administrative capacity, the city council reviews and approves or denies these policies. Practically, the differences between these two administrative governance models have

---

[174] These basic principles are included in a model bill put forward by the ACLU in AN ACT TO PROMOTE TRANSPARENCY AND PROTECT CIVIL RIGHTS AND CIVIL LIBERTIES WITH RESPECT TO SURVEILLANCE TECHNOLOGY (AM. CIV. LIBERTIES UNION (Oct. 2018).

efficiency and local political consequences. Legally, these different structures have consequences for judicial review of the underlying rules, discussed further below.

Based on my research, no city has adopted completely independent rulemaking by a separate administrative body, akin to traditional administrative governance, an approach I and other scholars endorse.[175] Given this reality, my analysis proceeds largely on the basis of the forms of local administrative oversight that currently exist, while recognizing that the more traditional model has desirable advantages. The remainder of this paper provides a theoretical grounding for existing efforts, presents the first structured survey of existing municipal efforts, notes where current efforts fall short, and demonstrates the possibilities of this approach moving forward.

2. Administrative versus Legislative Functions of City Governments

The intertwined structure of city governments—where legislative and executive power are often shared—offers an opportunity for a unique kind of administrative-style governance at the local level. Local governments, in contrast to the tripartite federal government, the focus of most administrative scholarship, take many different forms. Larger cities may have traditional, stand-alone agencies, while in others, city councils occupy both legislative and administrative roles. In these smaller cities, city councils can serve both as the legislating body (passing legislation) and as an administrative body (implementing specifics of legislation). Regardless of their structure, local governments do engage in tasks that can be classified as administrative governance. Local governments set zoning rules, for example. If a city has separate agencies, a zoning board might do this task; if not, local zoning rules may be passed by the city council itself, demonstrating the blended nature of administrative tasks at the local level.

Local governments have developed ways of distinguishing between the legislative and administrative roles that city councils shift between. When these roles are shared by councils, officially a legislative body, a common way to distinguish between these roles is to differentiate broader governing rules passed by councils and implementations of those rules. For instance, the state of New York gives municipal "laws" greater legal weight than municipal "ordinances," emphasizing that laws are more legislative in character

---

[175] *See especially* Ponomarenko, *supra* note 14.

and ordinances more administrative in character.[176] In my hometown of Bloomington, Indiana, a similar distinction exists. Broadly, "resolutions" state policy positions and "ordinances" implement them (note that in other cities, the meanings of these two terms are reversed, and ordinances are the broader mechanism).[177] The important point to grasp is that the *same* body, the city council, adopts both types of rules. To apply this structure to the local police technology context, a city council might, by exercising its legislative function through a resolution, state an intention to "increase protections for citizens regarding sophisticated police technology." The Council would then work to develop an ordinance that lays out the kinds of protections contemplated in Section 1 above (NDA prohibition, etc.). Once the ordinance is developed, the council would approve individual acquisitions on the basis of the principles outlined in the ordinance.

This vision of local administrative governance is not theoretical when it comes to law enforcement more broadly. San Francisco has implemented a version of this kind of governance with respect to their police force (although it does not deal with police technology). San Francisco has an appointed administrative body, the Police Commission, which oversees the police force. The Commission sets policies for the police department (through a mechanism called General Orders).[178] Beginning in 2008, the Commission promulgated a General Order requiring police have an elevated "reasonable suspicion" before beginning an investigation that might implicate First Amendment

---

[176] *See* NEW YORK STATE MUNICIPAL HOME RULE LAW, § 2(9) ("A law (a) adopted pursuant to this chapter or to other authorization of a state statute or charter by the legislative body of a local government, or (b) proposed by a charter commission or by petition, and ratified by popular vote, as provided in article four of this chapter or as provided in a state statute, charter or local law; but shall not mean or include an ordinance, resolution or other similar act of the legislative body or of any other board or body.")

[177] For instance, the 2018 Comprehensive Management Plan, adopted by *resolution*, stated an intention to "increase efficiency of parking inventory by providing more dedicated parking for two-wheeled motorized and non-motorized vehicles." A 2019 *ordinance* implemented part of this goal, with 15 pages of detailed code updates to address motorized scooters, down to specific portions of blocks that can be used as dismount zones. *See 2018 Comprehensive Plan*, CITY OF BLOOMINGTON (2018); Bloomington, In., Ordinance 19-09 To Amend Title 15 of the Bloomington Municipal Code Entitled "Vehicles and Traffic" (July 31, 2019).

[178] *General Orders*, SF POLICE, https://www.sanfranciscopolice.org/your-sfpd/policies/general-orders.

activities.[179] However, the City sometimes cooperated with the FBI, and the City's agreement with the FBI required officers to conform to a lower suspicion standard.[180] Controversy over this discrepancy ensued. The city council responded by building on the administrative General Order by passing a legislative ordinance that required city officers to follow city rules even when cooperating with the feds; it also required future local-federal cooperation agreements to undergo public disclosure and comment.[181] This example shows the blending of legislative and administrative functions that can happen at the local level. Here, the city council delegated general police rulemaking to the Police Commission. The Police Commission issued an administrative order on investigation standards, and the city council stepped back in to reinforce the standard through a legislative ordinance. Yet, the council's introduction of a requirement for notice and comment on future cooperation agreements is also administrative in nature, echoing administrative practices by federal agencies. Administrative governance at the local level is almost always a blend of actions by legislative and administrative (in the traditional sense) bodies. Many of the aims of this kind of governance are the same as those of traditional administrative governance; at the local level, we can recognize the complexity of the actors and, at the same time, the administrative nature of the governance.

3. Police Rulemaking: the Wrong Kind of Administrative Governance

The majority of existing scholarship supporting administrative governance of the police advocates specifically for police rulemaking.[182] By police rulemaking, scholars usually mean something akin to the following, to use an example from the canonical work on police rulemaking: a police department passes a rule requiring formal lineups in addition to photographic exhibitions to identify suspects, and

---

[179] *Guidelines for First Amendment Activities, General Order*, SAN FRANCISCO POLICE DEP'T (8.10 ed., Oct. 1, 2008).

[180] Standard Memorandum of Understanding Between the Federal Bureau of Investigation and the San Francisco Police Department §V.B.3 (Mar. 1, 2007) https://brennancenter.org/sites/default/files/analysis/SFPD%20MOU-JTTF.pdf.

[181] Bridget Fahey, *Federalism by Contract*, 129 YALE L. J. 2232, 2403-04 (2020); *see also* San Francisco, Ca., Ordinance 120046 to Establish Policy Regarding Participation in Federal Counterterrorism Activities (passed by Board of Supervisors Apr. 3, 120046 (2012).

[182] *See generally* Amsterdam; Davis; and McGowan, *supra* note 11.

this rule is made legally enforceable.[183] This form of governance makes the police responsible for making the rules that govern themselves.

But police rulemaking is arguably better classified as self-regulation, when a body makes rules for itself, than as administrative governance, when a body makes rules that apply to third parties.[184] Police rulemaking has been critiqued for a variety of downsides: a desire to avoid legal liability might water down rules, potential noncompliance, its undemocratic nature, and problems getting the police to participate in such a program, to name a few.[185] Indeed, recent studies of police-made rules in the surveillance context highlight the rarity of police rulemaking, even absent a regime for its legal enforcement: just seventeen of the total fifty-three agencies in Massachusetts that used ALPRs developed written policies regarding their use in 2013.[186] Perhaps the deepest problem with police rulemaking is that self-regulation involves substantial legitimacy and independence problems, problems that do not accompany the kind of administrative governance examined by this paper.[187] Vesting the ability to make and enforce rules in one actor raises serious concerns about concentration of power.[188]

That said, this previous generation of scholarship deserves a brief look, given that its motivation and goals were much the same as this Article's project. Police rulemaking scholarship emerged in the 1970s in response to a concern about a lack of gradation in Fourth Amendment law—either police were required to get a warrant, or not—and the racially biased patterns that emerged from police discretion in the non-warrant space.[189] Scholars argued that a "wide range of procedural alternatives below the constitutional level" could achieve fairer and more accurate convictions.[190]

---

[183] McGowan, *supra* note 11, at 665-66.

[184] *See* Ponomarenko, *supra* note 14, at 5.

[185] *Id*. at 15-20.

[186] *Id*. at 31 (*citing* Shawn Musgrave, *License Plate-Reading Devices Fuel Privacy Debate*, BOS. GLOBE (Apr. 9, 2013).

[187] *Id*. at 20-21.

[188] Ronald Allen, *The Police and Substantive Rulemaking: Reconciling Principle and Expediency*, 125 PENN. L. REV. 62, 101 (1976).

[189] *See generally* Amsterdam, *supra* note 11; Davis, *supra* note 11; McGowan, *supra* note 11; Allen, *supra* note 188; "The Police," *The Challenge of Crime in a Free Society*, PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE 91*,* 103-04 (1967).

[190] McGowan, *supra* note 11, at 689.

These scholars' chosen vehicle for procedural alternatives was legally enforceable police rulemaking. Under this proposal, police would create more granular rules to govern their own conduct, rules that would be subject to subsequent judicial review.[191] This rulemaking would serve as "a needed check on arbitrariness in the conduct of various searches and seizures that presently occupy a troubling fourth amendment limbo," so-called administrative searches exempted by courts from the warrant requirement, including border searches, vehicle stops, searches of impounded vehicles, mail inspections, and licensing inspections.[192] Rulemaking allows clarity and flexibility "without the cost of amorphousness" that, these scholars argue, arises from courts applying broad constitutional doctrines to ever-more specific factual scenarios, often deferring to post-hoc "local judgements that have either not been made responsibly or not been made at all" except according to one officer's discretion.[193] Despite the flaws of self-regulation, this scholarship built a base on which future work regarding ex ante local governance of criminal procedure would emerge, including the work of the scholars whose arguments are highlighted in the next subsection.

B. Arguments for Local Administrative Governance

Administrative governance allows for a more holistic and granular review of law enforcement practices, an opportunity to better incorporate technically complex and rapidly changing information, and an opportunity for a more iterative and interactive form of oversight.[194] Although most scholarship advocating for administrative governance of law enforcement has focused on the federal government, this body of work's assessment of the benefits and drawbacks of administrative governance is still largely applicable to the local context. The below

---

[191] *See generally* Amsterdam; Davis; and McGowan, *supra* note 11; "The Police," *Challenge*, *supra* note 189; *but see* Allen, *supra* note 188, at 87-98 (Allen viewed the application of administrative principles to the police as a fundamental misunderstanding of what the police did: they enforce, not create, law and rules. Although other administrative lawmaking generally takes place within the confines of specific expertise, police deal with the entire range of criminal conduct. Allen also raised separation of powers concerns, given that the power to make and enforce rules in our system is not usually given to one actor; similarly, legislatures may not be able to explicitly delegate rulemaking to police forces, depending on how nondelegation doctrines are interpreted at the state level.)

[192] Amsterdam, *supra* note 11, at 418.

[193] Amsterdam, *supra* note 11, at 418-19.

[194] Renan, *supra* note 3, at 1076.

analysis also draws on the few works written about administrative governance at the local level, mostly with regards to police conduct.[195]

1. Programmatic Scope

Administrative processes provide an opportunity to discuss questions that are important but difficult to incorporate into traditional judicial Fourth Amendment analysis. For each new potential surveillance technology acquisition, administrative mechanisms facilitate timely discussion of the more unorthodox risks of advanced surveillance technologies, risks that are often a poor fit with the structure of adversarial, procedural judicial proceedings. Specifically, administrative mechanisms are suited to considering the risks to communities at large, not just individuals. Indeed, many current local administrative surveillance governance schemes already do so.[196]

In addition, this decision-making structure would also allow for consideration of public cybersecurity risks—how certain technologies used for specific investigations can make everyone's devices less safe—in ways that do not fit into a cabined Fourth Amendment inquiry.[197] This kind of structure could also accommodate discussions of First Amendment risks of surveillance, as demonstrated by the San Francisco example above.[198]

Furthermore, judicial adjudication struggles to limit police mission creep. In contrast, administrative governance provides a structured environment for sanctioning or banning a range of possible use cases ahead of time, which can limit mission creep. This environment can also help avoid, or at least put in place procedures for responding to, mistakes down the line. Discussion of these issues does not mean that the results *will* be favorable to those who prioritize civil liberties—indeed, these city bodies may well decide to proceed with certain police technologies despite the discussed risks—but at least the debate would happen in a timely and public manner.

---

[195] *See generally* Ponomarenko, *supra* note 14; Erik Luna, *Principled Enforcement of Penal Codes*, 4 BUFF. CRIM. L. REV. 515 (2001).

[196] *See* discussion of Seattle below.

[197] For example, mobile forensics devices that rely on software vulnerabilities can only be used as long as those vulnerabilities persist, but fixing the vulnerabilities would make everyone's phone safer.

[198] *See generally* Katherine Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 BOS. COL. L. REV. 741 (2008).

2. Adaptability

Administrative procedures also allow for a high adaptability to changing circumstances. While courts offer limited avenues for changing settled doctrine, administrative procedures allow an option for adjustment each time a new technology is acquired and throughout the lifespan of a particular technology, at will. Addressing these questions does not depend on a defendant's willingness to or defense attorney's diligence in bringing a challenge. Administrative governance accomplishes this in part by forcing both the oversight providers and the overseen to the table at the same time, providing an information-forcing function that courts sometimes lack.[199]

Last, compared to legislative alternatives and court-only oversight, administrative governance can easily encompass a broad cross-section of technologies. Technologies with certain features, like high visibility, are more likely to capture the attention of a legislature. By contrast, less salient technologies can still be covered by broader, technology-neutral administrative policies.

3. Public-Private Regulation

The ability to place some constraints on public-private contracts is one of the main benefits of this kind of administrative control over police technology. As discussed earlier, courts have hesitated to force disclosure of evidence in court in violation of NDAs—and may not even be aware of an NDA's existence. Setting out conditions for public-private contracting as part of the administrative approval process provides the opportunity to regulate this relationship to whatever degree the city deems appropriate. City bodies are arguably more experienced than courts in municipal contracting, which may make them more knowledgeable actors on this topic, too. To the contrary, however, their close relationships with industry could leave them vulnerable to interest capture.[200]

4. Timeliness

Requiring administrative approval for acquisition of a certain technology accelerates the debate about risks and rewards, moving it up in time from a judicial determination. Indeed, from initial debate to

---

[199] For instance, courts have struggled to specify what level of technical detail warrants must include. The administrative governance approach could feasibly address this problem at the front end.

[200] Andrew Crespo, *Systemic Facts: Towards Institutional Awareness in Criminal Courts*, 129 H. L. REV. 2049, 2064 (2016); *see infra* Part II.C.

adoption, most of these ordinances took two years, as detailed below, compared to the ten years it often takes for judicial reconciliation of these issues. More specifically, administrative oversight offers the ability to have a technology-neutral framework readily in place to handle new investigative technologies as they arise, rather than waiting for a crisis to prompt new rules. Courts are notoriously slow to respond to technological changes, as discussed earlier in the paper. Even legislatures lag behind— see, for example, the seven-year gap between the decision in *Smith v. Maryland* and the enactment of ECPA—nor do legislatures regularly update statutes once passed.[201] Legislatures are also sometimes hesitant to act before the courts do.[202] On timing, administrative governance seems to come out ahead. However, the two models of local administrative governance of surveillance that we have seen emerge—council plus administrative body versus council-only—vary in their efficiency. In some places, adding an administrative body seems to speed up the governance process of surveillance tools; in others, adding an administrative body slows processes down. Cities would be wise to consider their own local context and historical track record when deciding which of the two models to implement to attain the best efficiency.

C. Worries Regarding Local Administrative Governance

Local administrative governance is not without its flaws. This section begins by isolating drawbacks of this proposal that are shared with other governance mechanisms and proceeds to analyze limitations that are particularly pronounced in this proposal. Andrew Crespo has critiqued proposals for administrative governance in the criminal law realm as failing to "examine closely what might be lost in the bathwater of institutional redesign."[203] Still, he frames institutional reform as a question of tradeoffs; I argue the tradeoffs favor administrative governance.

---

[201] Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 765-66, 769-70 (2005).

[202] Mayer, *supra* note 11, at 653; *see also* Dow Chem. Co. v. U.S., By & Through Gorsuch, 536 F. Supp. 1355 (E.D. Mich. 1982); Kyllo v. United States, 533 U.S. 27 (2001) (no Congressional action followed the decision in *Dow Chemical Co.*, but the Supreme Court essentially reversed *Dow Chemical Co.* later in *Kyllo*).

[203] Crespo, *supra* note 200, at 2060.

1. Limitations Shared with Other Solutions

a. Expertise

Neither judges nor legislators nor municipal officials will be experts on investigative technology. Each of these institutions has mechanisms, of varying effectiveness, for countering lack of expertise. Administrative oversight does not solve this problem, but its mechanisms for addressing the problem offer some advantages.

Courts access outside expertise largely through what the parties submit to the court. The information submitted depends, then, on the sophistication of the parties, or on invited amici. Courts also have what could be called an expertise bias towards property law views of the Fourth Amendment; other institutions may be more flexible in addressing search and seizure technologies.[204] Legislatures, in theory, have the ability to consult a wide range of experts, resulting in more nuanced, clear, and balanced rules with respect to privacy and safety.[205] As anyone who studies the legislative process knows, however, the ability to consult experts does not always result in a reality of experts consulted.

Compared to federal administrative bodies, local administrative bodies are not as well-resourced, potentially hindering their ability to maintain or consult experts. For instance, some standalone local agencies may only be staffed by part-time members, who also hold other jobs.[206] Administrative forums, though, are less procedurally constrained than courts in the ways in which they receive and weigh information, and could conceivably gather a wide range of expertise themselves and invite in outside experts when making decisions. As evident in the local processes examined below, two groups with differing expertise, the police and civil liberties organizations, were able to participate in public processes informing local administrative governance. Additionally, in localities that follow the council plus administrative body model, appointees to the administrative body could potentially be selected for their particular expertise.

---

[204] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 815-26 (2004).

[205] *Id.* at 806.

[206] Nestor M. Davidson, *Localist Administrative Law*, 126 YALE L.J. 564, 608 (2017).

b. Interest Capture

Consulting experts can, however, bleed into interest capture. Critics argue that administrative governance is just as much at risk of interest capture or prioritizing executive branch priorities over other perspectives. Specifically, administrative actors generally share law enforcement's aims of law, order, and safety.[207] Furthermore, law enforcement actors will have incentives to argue against specific rules, regardless of the forum in which the rules are promulgated.[208] Police unions already spend millions in lobbying city council members in major cities; this lobbying could easily extend to administrative appointees.[209]

These are real concerns. At the same time, administrative-style governance has features that could make administrative actors less deferential to police perspectives than courts. Local administrative bodies, whether independent commissions or carried out through existing councils, are allowed to hear a range of perspectives. In contrast, in most cases, a court hears from the defense and from the state. This broader exposure helps encourage decisions that respond to a range of viewpoints. In addition, repeat player dynamics in administrative settings differ from those in judicial settings. City councils and agencies perform a wide range of duties in which law enforcement is not always their counterpart, increasing the range of repeat actors to which the council is accountable. For independent police commissions, concerns about interest capture may be more similar to a judicial setting. But, compared to a judicial setting in which the police are repeat players and the other party a one-time defendant, administrative bodies allow repeat players on both sides, which reduces the advantage available to police actors to capture the relevant process.[210]

---

[207] Crespo, *supra* note 200, at 2061; *see also* Slobogin, *supra* note 4, at 1761-64 (arguing police have incentives to argue against more specific rules).

[208] Slobogin, *supra* note 4, at 1761-64 (arguing police have incentives to argue against more specific rules).

[209] Tom Perkins, *Revealed: Police Unions Spend Millions to Influence Policy in Biggest US Cities*, THE GUARDIAN (June 23, 2020, 06:15:00 AM), https://www.theguardian.com/us-news/2020/jun/23/police-unions-spending-policy-reform-chicago-new-york-la.

[210] Paul H. Rubin, *Why is the Common Law Efficient?,* 6 J. LEGAL STUD. 51, 53-56 (1977), *in* Patrick Luff, *Captured Legislatures and Public-Interest Courts*, 2013 UTAH L. REV. 519, n.126 (2013) (situations in which only one party has an interest in future cases will mean that party will exert pressure for their favored outcome).

My study of initial local governance efforts shows some evidence that these administrative processes are resistant to interest capture. First, none of the proposals adopted exactly mirror the "gold standard" put forward by the ACLU, suggesting that civil liberties interests did not bulldoze the process. Police interests also did not dominate the overall process: especially in cities that have revised or reformed their initial processes, the procedures explicitly expanded to include stakeholders that could balance law enforcement perspectives.[211] That said, in cities where efforts to implement administrative governance failed early on, police opposition was almost always evident.[212] Clearly, fourteen instances of this kind of governance provide the basis for only a limited analysis, but early results show some resilience to interest capture.

2. Unique Limitations of Administrative Control

a. Motivation Limitations: A Response to Federalism Concerns?

Struggles over federal versus local control of police resources served as the catalyst for many cities that have implemented administrative control of investigative technologies. Specifically, the one trigger of these debates was police departments accepting federal grant money without local government assent.[213] Questions exist about whether local governments will have the incentives to continue to develop administrative governance strategies absent such federalism conflicts.

This pattern is born out in the cities analyzed below. Ten of the fourteen local entities specifically mention the need to seek approval before soliciting or accepting federal funding for surveillance technologies, a feature the ACLU model bill included. Somerville, Berkeley, and New York do not, but federal acquisitions may be

---

[211] *See especially* details of Seattle's reform process below.
[212] *See* Lily Liu and Mailyn Fidler, *Four Obstacles to Local Surveillance Ordinances*, LAWFARE (forthcoming Sept. 2020).
[213] Crump, *supra* note 9, at 1640.

covered by other, broader provisions in the rules.[214] Madison carves out a separate, less rigorous review process for federal acquisitions.[215]

This federalism motivation may have been sufficient but not necessary to the development of local administrative governance on this issue. Other sources of pressure, including local activism, definitely played roles in some of the case studies below. The passage of Madison and New York's laws in the wake of Black Lives Matter protests over George Floyd's murder demonstrate this influence.[216] As more cities adopt these kinds of measures, more data will be available to analyze their motivations.

b. Democratic Legitimacy

Critics argue that administrative governance does not provide the democratic legitimacy that needs to undergird decisions about policing.[217] Critics also argue that, despite the public-facing parts of administrative decision-making, these processes are not necessarily easily accessible, or accepted, by marginalized community members on whom the burden of such policing decisions falls.[218] These critics argue that the adversarial judiciary the only government institution that guarantees a voice for marginalized actors in the form of state-provided representation.[219]

---

[214] Somerville, for instance, requires council approval for any technology acquired "without the exchange of monies or other consideration" which would include federal grant programs. Somerville, Mass., Ordinance 2019-20 (Oct. 10, 2019) at §10-65(a).

[215] Madison, Wis., Ordinance 20-00056 (Enactment date: June 20, 2020) ("Creating Section 23.63 of the Madison General Ordinances to establish Surveillance Technology guidelines for Departments"), https://madison.legistar.com/LegislationDetail.aspx?ID=4318039&GUID=DBDE2725-BD49-4062-8C51-A69F5349C520&FullText=1.

[216] Nathan Sheard, *Victory! New York's City Council Passes the POST Act*, ELEC. FRONTIER FOUND. (June 18, 2020), https://www.eff.org/deeplinks/2020/06/victory-new-yorks-city-council-passes-post-act.

[217] Friedman and Ponomarenko, *supra* note 4; Mayer, *supra* note 11, at 646-47 (noting that this view is evident in judicial opinions, including: In Re Askin, 47 F.3d 100 (4th Cir. 1995) (Wilkinson, J.); United States v. Graham, 824 F.3d 421, 438 (4th Cir. 2016) (Wilkinson, J., concurring); Dalia v. United States, 441 U.S. 238 (1979) (Stevens, J., dissenting); Riley v. California, 134 S. Ct. 2473 (2014) (Alito, J., concurring)).

[218] Crespo, *supra* note 200, at 2062-63; Rachel A. Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 812 (2012).

[219] Sklansky, *supra* note 170, at 227 ("Judicial hearings are by their nature

Administrative governance certainly provides more accountability than police-led rulemaking.[220] More importantly, the kind of hybrid legislative-administrative governance examined here offers underexplored benefits by combining existing systems of democratic representation with the staid values of administrative governance. In both council-led and council plus administrative body models, the council retains final authority. In addition to built-in electoral accountability, councils are well-suited to conducting public-facing hearings as part of the administrative governance process, adding to their ability to engage the public. Majoritarian pressure, interest group capture, and underlying concerns about local electoral fairness still could come into play.[221] But this hybrid model has been underexplored in existing administrative law literature.[222] Pursuing it further could open new possibilities regarding the democratic legitimacy of administrative governance.

One additional trend suggests cities might be cognizant of which decisions regarding surveillance require greater democratic legitimacy and which can satisfactorily be executed by administrative bodies. For instance, cities generally have passed legislative bans on facial recognition technology, rather than leaving such decisions to administrative oversight bodies, even when those bodies are already established.[223] This initial trend might suggest that cities turn to legislative avenues when *banning*, rather than regulating, surveillance technologies. This allocation of roles could work quite well, taking advantage of each body's relative strengths and weaknesses.

c. Administrative Default

In a similar vein, agencies lack the forcing function present in courts: courts must address the facts that are brought in front of them. Critics argue that, as a result, administrative bodies may dodge the most important questions, a problem Andrew Crespo deems "administrative

---

adversarial, though, which assures at least some representation for both sides, whereas legislative hearings on privacy issues in criminal investigations can easily be dominated by law enforcement interests.").

[220] Ponomarenko, *supra* note 14, at 56-57.

[221] Crespo, *supra* note 200*,* at 2063; *see also* Sklansky, *supra* note 170, at 227.

[222] Ponomarenko, for instance, argues for independent third-party bodies as administrative regulators of the police, which do not necessarily carry with them the democratic advantages of elected city councils. *See* Ponomarenko, *supra* note 14, at 5.

[223] For example, San Francisco, Oakland, Berkeley, and Somerville all turned to legislatively-enacted ordinances to ban facial recognition technology.

default."[224] Berkeley's surveillance governance process very nearly entered administrative default in its first review of a new acquisition, CycloMedia software, but legislative pressure helped stave off that result, yet another potential upside of the close blending of legislative and administrative functions of local governments.[225] So, yes, administrative default is a real risk—but courts *also* engage in question-dodging; they are not a better alternative on this front. We saw this repeatedly throughout the examples in all of Part I of this paper. Courts will often resolve cases on non-constitutional grounds, such as upholding the validity of an NDA that keeps certain evidence out of court, rather than tackling a thorny Fourth Amendment question.

d. Political Will & Downregulation

Administrative governance will only be as strong as communities are willing to make it. In the author's view, this is the most worrisome feature of local administrative governance of these issues. Relying on local administrative governance for a gradated Fourth Amendment could result in no action at all, or in the downregulation of protections. Developing more gradations of search and seizure procedures has many benefits, but police will likely try to obtain the lowest standard possible in many cases. If administrative processes allow sub-constitutional benchmarks, police will gravitate towards these, moving debates away from warrant requirements towards a much less protective standard. On the other hand, police are already often arguing for sub-constitutional protections in their arguments that certain actions do not constitute searches or require warrants. This reason is at the heart of the benefits of an administrative solution: providing more limits and measured ways of applying sub-constitutional protections could bring regularity and oversight to practices that are already happening on the ground. Administrative governance would regulate reality rather than wishful thinking.

D. Judicial Review of Local Administrative Governance

Legal challenges to local administrative surveillance governance could fall into two broad categories. Local governance could be challenged on substantive legal grounds—for instance, local rules do not provide satisfactory constitutional protection. Or, they could be challenged on the basis of improper exercise of authority, with state

---

[224] Crespo, *supra* note 200, at 2064; Friedman and Ponomarenko, *supra* note 4, at 1863.

[225] *See infra* note 330.

rules preempting local rules or local entities lacking the authority to promulgate such rules.

On the substantive point, this Article's proposal of local administrative governance envisions such rules as built on top of a constitutional floor.[226] Courts will remain the final arbiter of Fourth Amendment issues: administrative guidelines should not automatically be entitled to a presumption of constitutional reasonableness.[227] Retaining a central role for the courts in reviewing administrative guidelines is key to addressing concerns about downregulation through administrative governance. Administrative governance presents an earlier-in-time opportunity for non-constitutional, but still substantive, decision making on Fourth Amendment issues.[228]

How much deference courts should extend to local rules on surveillance technologies, on constitutional and non-constitutional questions, deserves further discussion. Friedman and Ponomarenko argue for judicial deference towards democratically-authorized rules about search and seizure, unless a clear constitutional doubt exists, largely as an incentive for localities to enact such rules.[229] As they point out, however, the Supreme Court has generally chosen not to predicate the type of deference a rule receives on prior legislative authorization.[230] So far, localities have been choosing to enact

---

[226] *See* Wayne A. Logan, *Fourth Amendment Localism*, 93 IND. L. J. 370 (2018) (making this argument in full).

[227] City of Ontario v. Quon, 560 U.S. 746 (2010) (provides support for the perspective that judicial assessments of reasonableness trump statutory considerations, but the opinion is narrow and has been criticized for its lack of specificity and clarity); *see, e.g.*, Adam Liptak, *Justices are Long on Words but Short on Guidance*, N.Y. TIMES (Nov. 17, 2010). For broader discussions of the intersection between administrative/statutory protections and reasonableness inquiries, *see* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 267-70 (2011); Renan, *supra* note 3, at 1079-82.

[228] Other scholars have proposed new roles for the court as a way to introduce or incentivize earlier-in-time decision-making opportunities. *See* Friedman and Ponomarenko, *supra* note 4, at 1891 (arguing courts should use varied incentives to prompt police rulemaking); *See also* Jaros, *supra* note 123, at 1165 (arguing for state court adoption of preemption doctrines to regulate police); John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 CAL. L. REV. 205 (2015) (arguing courts should use constitutional pronouncements to incentivize police rulemaking).

[229] Friedman and Ponomarenko, *supra* note 4, at 1897-98.

[230] *Id.* at 1898 (discussing United States v. Robinson and Gustafson v. Florida- a pair of cases involving similar circumstances where one police department had a prior policy authorizing the conduct in question).

governance of surveillance technologies without the need for any deference incentive incentive. Indeed, I am concerned about the potential downregulation effects of offering this incentive widely: such an incentive could reduce the seriousness with which cities design and implement rules, when the deference "reward" is the real aim.

That said, in cities where administrative governance is carried out by a separate administrative agency, administrative law standards of deference along the lines of *Chevron*, etc., would be applicable.[231] However, in a growing and recent trend, a number of states have enacted legislation prohibiting judicial deference to state agency interpretation of state legislation, and such opposition to deference may extend to the local level.[232] At the local level, deference on substantive questions seems unwise, and on interpretive questions, out of vogue.

Courts will also address legal challenges on the basis of improper exercise of authority and preemption with respect to local administrative surveillance governance. Regarding questions of local authority, the standard of review that courts use is an important threshold question. This standard will depend on the model of administrative governance a city has implemented. If a city has implemented a council plus administrative body model, the actions could be reviewed under principles of administrative law. Administrative law at the local level does exist.[233] Courts assess issues

---

[231] William Eskridge and Lauren Baer, *The Continuum of Deference: Supreme Court Treatment of Agency Statutory Interpretations from Chevron to Hamdan*, 96 Geo. L. J. 1083, 1092 (2008).

[232] Arkansas (2020), Wisconsin (2018), Florida (2018), Mississippi (2018), Arizona (2018), and Michigan (2008). *See State Responses to Judicial Deference (Administrative State),* BALLOTPEDIA (June 2020), https://ballotpedia.org/State_responses_to_judicial_deference.

[233] Davidson, *supra* note 206, at 605; for lengthier discussion of state APAs, *see* Kathryn E. Kovacs, *Superstatute Theory and Administrative Common Law*, 90 IND. L.J. 1207 (2015); *see also* Jim Rossi, *Overcoming Parochialism: State Administrative Procedure and Institutional Design*, 53 ADMIN. L. REV. 551 (2001).

of nondelegation from councils to local agencies,[234] procedural irregularities,[235] and grapple with issues of deference.[236]

However, cities that have adopted a council plus administrative body model generally limit the administrative body to a supervisory role; that is, the body reviews policies drafted by city agencies seeking to use surveillance tools rather than drafting the policies itself. This type of administrative function is not typically what we think of when we consider administrative governance—the kind accompanied by notice and comment rulemaking. But it is nonetheless reviewable administrative action. Federal agencies perform this kind of certification process, too; take, for example, the EPA's registration process for pesticides, which is essentially a review process. The EPA's registration decisions can still be challenged on APA grounds, for reasons such as failure to publicize or failure to base the decision on sufficient evidence.[237] The local administrative bodies in action could be challenged on similar grounds under local and state administrative law.[238]

Additionally, where citizens think too much power has been ceded to such administrative bodies, or improperly ceded, state and local nondelegation doctrine, much more robust than the moribund federal equivalent, can be used as a basis for challenge, too.[239] Scholars have

---

[234] *See* Davidson, *supra* note 206, at 620-621 (discussion of nondelegation issues in the New York soda portion size debate); *see also* Paul A. Diller, *Local Health Agencies, the Bloomberg Soda Rule, and the Ghost of Woodrow Wilson*, 40 FORDHAM URB. L. J. 1859, 1868-77 (2013).

[235] A handful of cities have their own administrative procedure acts, including one city included in this Article, Seattle. These acts often contain some form of notice and comment rulemaking requirements. *See* Casey Adams, *Home Rules: The Case for Local Administrative Procedure*, 87 FORDHAM L. REV. 629, 654 (2018).

[236] *See* Davidson, *supra* note 206, at 620-21; *see also* Diller, *supra* note 204, at 1877-78, 1897; *see also* Aaron Saiger, *Chevron and Deference in State Administrative Law*, 83 FORDHAM L. REV. 555, 558-60 (2014) (discussion of deference at the state level).

[237] *See, e.g.,* Ellis v. Bradbury, No. C-13-1266 MMC, 2014 U.S. Dist. LEXIS 54339 (N.D. Cal. Apr. 18, 2014); *see also* NRDC v. United States EPA, 857 F.3d 1030-31 (9th Cir. 2017).

[238] *See* Grant's Farm Assocs. Inc. v. Town of Kittery, 799 A.2d 799 (Me. 1989) (concluding local board's decision was supported by substantial evidence); Kosalka v. Town of Georgetown, 752 A.2d 183, 187 (Me. 2000) (striking down instructions to administrative board as providing insufficient guidance).

[239] Davidson, *supra* note 206, at 622; Josh Eagle, *The Practical Effects of Delegation: Agencies and the Zoning of Public Lands and Seas*, 35 PEPP. L. REV. 4, 835, 836-7 n.3 (2008).

pointed to the nondelegation doctrine's robustness at the local level as a potential backstop against local interest capture.[240] Widespread uptake of this kind of governance of surveillance tools, by expanding the areas in which local administrative law matters, could spur further legal development in the local administrative law field.

Most localities have, however, so far implemented city-council led administrative-style governance of local surveillance technologies; potentially due to the resource-intensive nature of setting up a separate administrative body. This architectural choice takes these decisions out of the realm of administrative law and into judicial review of proper use of municipal power. The precise standard of judicial review would turn on the legal status of a municipality within a state—whether the city operates under a type of home rule or under the more restrictive "Dillon's Rule." In both of these contexts, however, judicial review of local council actions would be limited to an up/down approval on the basis of whether the locality has the authority to regulate in the area.[241]

Some states allow cities to operate under home rule, which, coarsely put, allows localities to make rules in any area where the state did not explicitly bar or preempt them.[242] Many variations of home rule exist. At the extreme end lies constitutional home rule (often called *imperium in imperio*, empire within an empire), where local matters are generally immune to preemption as a constitutional matter.[243] These localities would have wide latitude to institute surveillance governance without state preemption challenges. A middle ground version of home rule assesses legislative intent and examines the particular domain of local regulation when deciding issues of preemption.[244] The softest form of home rule, statutory or legislative home rule, grants local governments full home rule powers until the state legislature explicitly restricts a particular power.[245]

---

[240] Davidson, *supra* note 206, at 624.

[241] *See generally* Harold H. Bruff, *Judicial Review in Local Government Law: A Reappraisal*, 60 MINN. L. REV. 669 (1976).

[242] David Schleicher, *The City as a Law and Economic Subject*, 2010 U. ILL. L. REV. 1507 n.37 (2010) (*citing* RICHARD BRIFFAULT & LAURIE REYNOLDS, CASES AND MATERIALS ON STATE AND LOCAL GOVERNMENT LAW, 332-36 (7th ed. 2008)).

[243] Lynn Baker and Daniel B. Rodriguez, *Constitutional Home Rule and Judicial Scrutiny*, 86 DENV. U. L. REV. 1337 (2009).

[244] Paul A. Diller, *Reorienting Home Rule: Part 2 – Remedying the Urban Disadvantage Through Federalism and Localism*, 77 LA. L. REV. 1045 (2017).

[245] Richard Briffault, *Our Localism: Part I – The Structure of Local Government Law*, 90 Colum. L. Rev. 1 (1990).

Other states operate under "Dillon's Rule," which requires explicit or necessarily implied grants of authority to localities.[246] Dillon cities may have trouble claiming that they have received grants of specific authority to regulate surveillance technologies, rather than a more general authority to regulate the police.[247] For Dillon cities, technology-neutral regulation offers an additional legal benefit: by framing surveillance rules as procedural rules governing the police, rather than rules governing specific technologies, cities may be better able to place these rules within the high-water marks of municipal power. Similarly, technology-neutral regulations are more likely to fall outside of state law preemption: states tend to regulate specific technologies and are unlikely to enact broad-reaching regulations of police forces.[248]

In either context, this authority-based standard of review seems to miss many of the important questions raised in the standards of review seen in administrative law, even at the local level. The kinds of rules made by city councils in this Article's proposal seem ripe for rational basis review or arbitrary-and-capricious analysis. This argument that administrative law should be incorporated into judicial review of municipal action has been made in other literature.[249] This Article's proposal—administrative-style governance executed by a city council—strengthens arguments for incorporating administrative law principles into judicial review of local action so that these actions are

---

[246] Aaron Saiger, *Local Government as a Choice of Agency Forum*, 77 OHIO ST. L. J. 424, 443 (2016).

[247] Among the five states in which cities have implemented rules, the split is relatively even between Dillon's rule and home rule states. Washington, California, and Tennessee apply some version of Dillon's rule, while Ohio and Massachusetts adhere to home rule. *See* Jesse J. Richardson, Jr., Meghan Z. Gough and Robert Puentes, *Is Home Rule the Answer? Clarifying the Influence of Dillon's Rule on Growth Management*, BROOKINGS INST. (Jan. 1, INSTITUTION (2003); *see also* Jon D. Russell and Aaron Bostrom, *Federalism, Dillon Rule, and Home Rule*, AM. CITY EXCH. EXCHANGE (2016), *available*).

[248] For a study of technology-specific state preemption of local privacy laws, *see* Ira Rubinstein, *Federal and State Preemption of Local Privacy Regulation*, N.Y.U. SCH. OF LAW, PUB. LAW RESEARCH PAPER NO. 18-17 (2018); *see* Richard Briffault, *Home Rule and Local Political Innovation*, 22 J.L. & POL. 1, 17–27 (2006) (for discussion of clear statement rules required for state preemption).

[249] Aaron Saiger, *supra* note 246, at 446; *see also* Gerald E. Frug, *The City as a Legal Concept*, 93 HARV. L. REV. 1057, 1062-67 (Apr. 1980); Paul A. Diller, *Local Health Agencies, the Bloomberg Soda Rule, and the Ghost of Woodrow Wilson*, 40 FORDHAM URB. L.J. 1859, 1863-65 (2013); Bruff, *supra* note 241, at 211.

reviewed for quality, not just authority. That said, this kind of drastic change in the standard of review of local action is unlikely. A more modest proposal might suggest submitting only specific decisions made pursuant to an ordinance to administrative review, while retaining up/down review of the ordinances themselves.

E. Federal and State Alternatives

There are two alternatives those who object to administrative governance might still suggest as solutions: federal administrative control of local police practices or state legislative control. These options do have attractive qualities, but are nonetheless not as viable as a local administrative governance approach.

1. Federal Control

Federal regulation of local police is an idea that is appealing to many—after all, for those inclined to favor administrative governance, federal administrative agencies are much more well developed than local ones.[250] Federal agencies would also be a streamlined solution, rather than relying on each locality to implement their own system. Jonathan Mayer suggested considering whether "certain hacking tools should be reserved for federal law enforcement," perhaps so limited by DOJ administrative rulemaking.[251] Rachel Harmon argues that "the federal government plays an ineliminable role in addressing the problem posed by the police."[252] She calls on more detailed Congressional regulation of policing, and points to (limited) conduct, remedies, training, employment, and transparency statutory regulations as evidence that the federal government can play such a role.[253] Indeed, Congress appears ready to explore new federal regulations on police forces in the light of the murder of George Floyd.[254] But, as Harmon herself points out, its ability to do so is circumscribed.[255] Under the constitution, the federal government has limited ability to regulate law enforcement within states, which is considered a power

---

[250] *See generally* Harmon, *supra* note 218, at 814-16 (for scholars favorably discussing federal administrative regulation of police); Renan, *supra* note 3, Part IV-V.

[251] Mayer, *supra* note 11, at 580 n.29.

[252] Harmon, *supra* note 218, at 814.

[253] *Id.*

[254] *See generally, e.g.*, George Floyd Justice in Policing Act 2020, H.R. 7120, 116th Cong., 2nd Sess. (2020).

[255] Harmon, *supra* note 218, at 815.

reserved to the states in the Tenth Amendment.[256] Some of these "partway" solutions would do a great deal of good—take, for instance, an administrative rule at the federal level requiring federal agencies to seek local political approval before disbursing grant money for new technologies.[257] That said, partway is the furthest we'd get with a top-down federal approach, given the limitations imposed by the federal system. Granularity, responsiveness, timeliness, and scope would all be challenges with top-down federal regulation.

2. Legislative Control

Some scholars have called for greater legislative action on police practices.[258] These proposals do have a historical basis; during the 1970s and 1980s, Orin Kerr notes that, "Congress rather than the courts has shown the most serious interest in protecting privacy from new technologies."[259] This congressional interest has waned for the

---

[256] Jared P. Cole, *Federal Power over Local Law Enforcement Reform: Legal Issues*, CONG. RESEARCH SERVICE (2016); Nathan James and Ben Harrington, *What Role Might the Federal Government Play in Law Enforcement Reform?* CONG. RESEARCH SERVICE (2018); Ponomarenko, *supra* note 14, at 60.

[257] Indeed, already, when federal actors "use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies," U.S. Dep't of Just. guidance applies; s*ee* U.S. Dep't of Just. Guidance 2015, *supra* note 41, at 6.

[258] Friedman and Ponomarenko, *supra* note 4, at 1875-84 (arguing for methods that preserve democratic participation in police rulemaking); *See* Erin Murphy, *The Politics of Privacy in the Criminal Justice System*, 111 MICH. L. REV. 485, 534-37 (2013) (showing the benefits and downsides of a legislative approach to Fourth-Amendment related practices; calls for a measured and mixed approach but notes many underappreciated benefits of a legislative approach).

[259] Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 855-860 (2004). Of its own initiative, Congress passed the Privacy Act of 1974 (allowing citizens to check and correct personal information in government databases), the Family Education Rights and Privacy Act of 1974 (FERPA), the Cable Communications Privacy Act of 1984, the Video Privacy Protection Act of 1988, the Health Insurance Portability and Accountability Act of 1996, and the Children's Online Privacy Protection Act of 1998 (not an exhaustive list). Responding to court decisions, Congress passed the Right to Financial Privacy Act of 1978 (after United States v. Miller, 425 U.S. 435 (1976)), the Privacy Protection Act of 1980 (after Zurcher v. Stanford Daily, 436 U.S. 547, 98 S. Ct. 1970 (1978)), and the Electronic Communications Privacy Act of 1986 (after Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577 (1979)).

technologies included in this paper, however. Little federal Congressional action on related has happened since the early 2000s.

State legislative activity could, however, provide a more responsive form of legislative governance.[260] Indeed, a few state legislatures have enacted laws that require local police forces to obtain permission from local government before accepting federal grants for surveillance technologies (New Jersey and Montana).[261] This kind of legislative activity on police governance issues is favored primarily for its democratic accountability, a feature that judicial review does not provide.[262] Supporters of legislative oversight contend that legislative rules are more comprehensive, balanced, clear, and flexible than judge-made rules, better able to keep pace with technological change, and more fully informed technologically.[263]

The primary drawback of legislative governance is, however, not what it could be, but what it tends to be. Legislative governance relating to police technology tends to be overly technology specific and responsive only to technologies that affect a wide swath of the population.[264] Drones, for example, have been the subject of much legislative action. As of 2017, 26 states have passed laws regulating government drone use in some way, and 18 of those require warrants for their use.[265] At least 19 states have passed laws regulating use of drones by non-governmental actors.[266] But drones are literally visible to constituents, could affect a wide swath of the population, not just defendants, have public and private uses, and are physical, hewing more closely to traditional American views of property-based privacy.

In contrast, only six states have passed laws regulating police use of stingray devices, which do not share the same visibility features.[267]

---

[260] *See* Ponomarenko, *supra* note 14, at 61-63.

[261] Sen. 2364, 216th Leg., Regular Sess. (N.J. 2015); H.R. 330, 2015 Leg., 64th Sess. (Mont. 2015).

[262] Jeremy Waldron, *The Core of the Case Against Judicial Review*, 115 YALE L. J. 1346, 1391 (2006).

[263] Kerr, *supra* note 259, at 807-08.

[264] This criticism applies even at the local level. *See* Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point*, N.Y. TIMES (Jan. 20, 2020) (for a critique of technology-specific local legislative measures).

[265] Amanda Essex, *Taking Off: State Unmanned Aircraft Systems Policies*, NAT'L CONF. OF STATE LEG. (2016); *2017 Unmanned Aircraft Systems (UAS) State Legislation Update*, NAT'L CONF. OF STATE LEG. (2018).

[266] *2017 UAS State Legislation Update*, *supra* note 265, at 3.

[267] Mike Maharrey, *New Maryland Law Bans Warrantless Stingray Spying;*

This legislative action was not any faster than judicial decision-making. The first state bill (California) prohibiting wireless use of stingray devices did not pass until 2015.[268] Legislative initiatives may not necessarily solve the time-lag problem of judicial decision-making.

Furthermore, drone statutes tend to display one of the key drawbacks of statutory approaches to police technology: they are technology-specific.[269] Gregory McNeal's study of state-level drone statutes finds that most laws are tailored to the technology rather than to the harm, which means legislatures are delivering piecemeal, rather than systemic, legislation on surveillance policy.[270] Legislatures can pass statutes tailored to the harms—the New Jersey and Montana laws discussed directly above are a good example—but they tend not to be.

Perhaps the best model of a state legislative law on California adopted a law in 2015 that requires local governments to approve police acquisition of "cellular communications interception technology" (aka stingray devices) at a public meeting.[271] In addition, the law requires local police to develop a use and privacy policy for the device and disclose cooperation agreements with other agencies regarding the use of such tools.[272] The law provides a private right of action, which was just invoked for the first time in 2020 to challenge the City of Vallejo's acquisition.[273] The law provides robust

---

Hinders Federal Surveillance Program, TENTH AMENDMENT CENTER (May 8, 2020); Mike Maharrey*, Signed as Law: New Mexico Strengthens Electronic Communications Privacy Act*, TENTH AMENDMENT CENTER (Mar. 9, 2020); Mike Maharrey, *New Hampshire Law Bans Warrantless Stingray Spying*, TENTH AMENDMENT CENTER (July 13, 2017); *AZ Senate Passes Bill Prohibiting Warrantless Stingray Spying*, ARIZONA DAILY INDEPENDENT (Feb. 28, 2017); Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy*, BRENNAN CTR. FOR JUSTICE (2018); Mike Maharrey, *Now in Effect: Sweeping Vermont Privacy Law Will Hinder Several Federal Surveillance Programs*, TENTH AMENDMENT CENTER (Oct. 1, 2016); Dave Maass, *Success in Sacramento: Four New Laws, One Veto—All Victories for Privacy and Transparency*, ELEC. FRONTIER FOUND. (Oct. 14, 2015).

[268] Maass, *supra* note 267.

[269] Murphy, *supra* note 258, at 496.

[270] *See* Gregory McNeal, *Drones and the Future of Aerial Surveillance*, 84 GEO. WASH. L. REV 354, 360 (2016).

[271] Cal. Gov. Code § 53166 (formerly S.B.SB 741); *see also* Maass, *supra* note 267.

[272] *Id.*

[273] Mike Katz-Lacabe, *Oakland Privacy Sues Vallejo Over Stingray Purchase*, OAKLAND PRIVACY (June 14, 2020), https://oaklandprivacy.org/oakland-privacy-sues-vallejo/; Petition for Writ of Mandate and Complaint for

transparency and democratic approval requirements, in addition to building an enforcement mechanism. It falls short in only applying to a limited range of technologies—but all of the structural elements of the bill reflect best practices being adopted by localities across the country. A state law inspired by this California effort, written in a technologically neutral manner and incorporating some of the more administrative-style requirements seen in local bills, would be a welcome way to ensure statewide local governance of surveillance technologies. Unfortunately, at least in California, efforts to pass a bill that did exactly that in 2017 failed in the California Assembly after passing the Senate, and such efforts have not been successfully revived.[274] State legislative efforts hold promise but have so far failed to live up to their potential.

F. Current Local Administrative Governance of Police Tech

As of August 2020, fourteen local government entities—thirteen cities and one county—have passed laws formalizing administrative control over police use of sophisticated investigative technologies.[275] Based on an analysis of these fourteen policies, each section below assesses a substantive portion of the ordinances: approval processes for

---

Equitable Relief Complaint, *Oakland Privacy v. City of Vallejo*, Cal. Super. Ct., No. FCS054805 (May 21, 2020).

[274] *See* S.B. 21, 2017 Leg. (Ca. 2017); *see Oakland Privacy Timeline*, OAKLAND PRIVACY, https://oaklandprivacy.org/timeline/.

[275] *See Community Control Over Police Surveillance*, ACLU (2020), https://aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance. *See also infra* Figure 2. For ordinances, see Seattle, WA., Ordinance 124142 (Mar. 18, 2013); Seattle, WA., Ordinance 125376 (July 31, 2017); Santa Clara Co., Cal., Ordinance NS-300.897 (June 21, 2016); Nashville, Tenn., Ordinance BL2017-646 (June 7, 2017); Somerville Exec. Order, Policy on Surveillance Technology (Oct. 4, 2017); Oakland, Cal., Ordinance Adding Ch. 9.64 to the Oakland Municipal Code Establishing Rules for the City's Acquisition and Use of Surveillance Equipment (Apr. 26, 2018); Palo Alto, Cal., Ordinance 5450 (Oct. 1, 2018); Cambridge, Mass., Ordinance 111918 (Dec. 10, 2018); Lawrence, Mass., Ordinance 133/2018 (Aug. 21, 2018); Berkeley, Cal., Ordinance 7,592-N.S. (Mar. 13, 2018); Davis, Cal.., An Ordinance of the City Council of the City of Davis Adding Article 26.07 of the Davis Municipal Code Regarding City Use of Surveillance Technology and Establishing the Penalty for a Violation Thereof (Mar. 20, 2018); Yellow Springs, Ohio, Ordinance 2018-47 (Nov. 19, 2018); San Francisco, Cal., Ordinance 107-19 (June 4, 2019); Somerville, Mass., Ordinance 2019-20 (Oct. 10, 2019); Madison, Wis., Ordinance 20-00056 (June 16, 2020); New York, New York, Law No. 2020/065 (July 15, 2020).

acquisition and use of technology, limits on contractual arrangements with private actors, and enforcement mechanisms. All but one of the ordinances contain approval requirements on acquisition and use.[276] Surprisingly, only four ordinances explicitly prohibit non-disclosure agreements (NDAs) with private entities. Last, nine of the twelve contain some grant of a private right of action to enforce the ordinance. Where entities had keyword-searchable records of city council deliberations, I examined these records to illuminate what drove the choices and patterns that emerged.

Some credit—or critique—the ACLU as spearheading the adoption of these kinds of laws. The ACLU has been active in advocating for this style of governance, and has made a model bill available to cities.[277] The analysis shows, however, that cities did not take up the ACLU model bill wholesale. Rather, cities made significant alterations in certain areas, particularly regarding NDAs and what kind of private right of action to extend.

Procedurally, all but one city passed city council ordinances updating municipal codes; Santa Clara County followed the same approach at the county level. The procedural approach only differed in Somerville, Massachusetts. There, the mayor first passed an executive order containing provisions similar to the other ordinances in 2017. Notably, Somerville is a particularly strong-mayor city.[278] The city council followed up two years later with a ban on facial recognition technology and a comprehensive ordinance in 2019.[279]

---

[276] New York is the exception and is discussed further below.

[277] *Community Control Over Police Surveillance (CCOPS) Model Bill*, ACLU (July 20, 2020).

[278] For local coverage of debate about Somerville's strong-mayor structure, *see, e.g*., Jo C. Goode, *Councilor Camara Proposes Changing City Government by Altering Charter*, HERALD NEWS (updated May 16, 2017, 4:46 pm), https://www.heraldnews.com/news/20170516/councilor-camara-proposes-changing-city-government-by-altering-charter.

[279] Katie Lannan, *Somerville Bans Government Use of Facial Recognition Tech*, WBUR (June 28, 2019), https://www.wbur.org/bostonomix/2019/06/08/sommerville-bans-government-use-of-facial-recognition-tech; Thalia Plata, *City Officials Discuss Surveillance Technology Guidelines*, THE SOMERVILLE TIMES (Feb. 5, 2020), www.thesomvervilletimes.com/archies/97194; Somerville, Mass., Ordinance 2019-20 (Oct. 10, 2019).

Table 2: Local Surveillance Ordinances[280]

Name	*Pop.*[281]	*Date*	*Status*	*Approved Tools*	*Policy Changes Req'd*	*Annual Reporting*
Seattle	754,000	2013/2017	Active	Yes	No	Yes
Sta. Clara	1,900,00	2016	Active	Yes	Yes[282]	Yes
Nashville	671,000	2017	*	*	*	*
Somerville	81,000	2017/2019	Inactive	No	No	--
Oakland	430,000	2018	Active	Yes	Yes	Yes
Palo Alto	65,000	2018	Inactive	No	No	No
Cambridge	119,000	2018	Active	Pndg	Pndg	Yes
Lawrence	80,000	2018	Inactive	No	No	No[283]
Berkeley	121,000	2018	Active	Pndg	Pndg	Yes
Davis	70,000	2018	Active	Yes	Yes[284]	Yes
Yellow Springs	3,700	2018	Inactive	No	No	No
SF	880,000	2019	Active	No	No	Yes
Madison	260,000	2020	--	--	--	--
New York	8,300,000	2020	--	n/a	n/a	--

* minutes not keyword searchable, no external media coverage
-- indicates passage was too recent for implementation

Figure 2

1. Passage and Procedures Actors Involved

These ordinances take about two years to pass from start to finish, significantly faster than judicial convergence and state legislative action. Typical government actors involved in the development of these ordinances included the city council and staff, the mayor's office, the police department, and various city legal and technology experts.[280] In some circumstances, the district attorney or county prosecutor and the public defender's office participated.[281] External actors typically included members of the public and local ACLU representatives; in some areas, civil society participation was broader, including ethnic

[280] Rubinstein, *supra* note 248, at 129; *City Manager Submits Surveillance Technology Documents to City Council and the Public*, CITY OF CAMBRIDGE, Nov. 27, 2019.

[281] For Seattle, *see* Rubinstein, *supra* note 248, at 126l; for Santa Clara, *see Finance and Government Operations Committee Special Meeting* (May 6, 2015, 4:08-4:12 PM); *Finance and Government Operations Committee Regular Meeting* (Mar. 12, 2015, 3:50 PM); *Finance and Government Operations Committee Regular Meeting* (Oct. 16, 2015, 3:08 PM).

minority advocacy groups.[282] Public comment took place through the normal channels for public input in each municipality, mainly involving public comments at the hearing, rather than formal notice-and-comment process. Revisions of ordinances usually involve an expansion of participants; Seattle's revision process broadened participation to include the staff of various city offices as well as additional public input, and Somerville saw a shift from the mayor's office to the city council.[283] Where independent police review commissions pre-date the ordinances, as in Berkeley, they were sometimes involved in developing ordinances.[284] In one of the smaller municipalities to pass an ordinance, Yellow Springs, Ohio, the measure appeared to be a smaller concerted effort between a local civil rights attorney, local ACLU affiliate representatives, and the municipal solicitor.[285]

Each ordinance varies slightly in the procedures it requires; as an overview, I will present the details of one city's, Oakland's, considered a gold standard. Oakland adopted a city council plus administrative body model. The ordinance allocates some duties to the city council and some to a separate body called the Privacy Advisory Commission (PAC).[286] The PAC and Council share approval duties for new acquisitions or new uses of surveillance technologies. A city agency seeking to acquire or change how it uses a surveillance tool must notify the PAC of its desire to seek funding or otherwise acquire the tools.[287] The agency must present the PAC with a surveillance impact report and use policy. The PAC reviews these documents and votes on a recommendation of how to proceed, which goes to the city council.[288] The city council then must make a final decision at a public hearing; if approved, the policies are adopted by resolution.[289] The impact report and use policy are also made public. The PAC bears primary oversight responsibilities for ongoing use of surveillance

---

[282] For example, the Council on Islamic Relations (CAIR) was involved in developing Berkeley's ordinance. *See* DJ Pangburn, *Berkeley Mayor: We Passed the "Strongest" Police Surveillance Law*, FAST COMPANY (Apr. 24, 2018).

[283] Ira Rubinstein, *Privacy Localism*, NYU PUBLIC L. & LEGAL THEORY RESEARCH PAPER SERIES WORKING PAPER NO. 18-18, 2018, at 129.

[284] *See* Pangburn, *supra* note 282.

[285] Megan Bachman, *Village Council—Surveillance Policy Passed*, YELLOW SPRINGS NEWS (Nov. 15, 2018).

[286] Oakland, Cal., Ordinance 13, 489 (May 15, 2018).

[287] *Id.*

[288] *Id.*

[289] *Id.*

technologies. Each year, an agency that uses an approved tool must submit an annual report of its use to the PAC, which can request further information and make a recommendation to the city council about whether any changes should be made; such changes would also be made by resolution. In cities with local surveillance ordinances that pursue a council-only model, the procedures look very similar, with the council performing the tasks the administrative body otherwise would.[290]

These procedures do not mirror formal notice and comment rulemaking, as in federal or state administrative law. Still, many of the same principles animate the procedures. Although no formal mechanism exists for public comment, public hearings accomplish some, but not all, of the same aims. In some jurisdictions, these public meetings are timed early in the process to afford ample time to consider public feedback; in others, they occur later. Similarly, the impact and use statements usually must be made public; but again, the timing of this publication varies.

These procedures differ substantively in one major way from traditional federal conceptions of administrative governance. Here, the regulated actors still draft the substantive rules themselves, subject to administrative and/or council approval. This model is not what we see at the federal level, where an administrative body makes the substantive rules for the regulated party, and these rules are not subject to any additional approval unless challenged in court. Still, these local procedures are more administrative in nature than they are legislative: an elected city council is not drafting detailed codes of use for every new software package that the police department acquires. The legislature is acting as a check, in its oversight capacity, rather than as rule-makers.

A discussion of passage would be remiss if it did not include a reflection on unsuccessful comprehensive ordinances. A review of failed ordinances suggests very few reach formal stages before being voted down—that is, when these efforts fail, they fail early. But in one locality, the city council of Lawrence, Massachusetts overrode a mayoral veto to pass its comprehensive surveillance governance scheme.[291] In several instances, proposals seemed to fizzle, appearing multiple times for council review but then disappearing from agendas,

---

[290] *See, e.g.,* Yellow Springs ordinance, *supra* note 275.

[291] Bill Kirk, *After Political Scrum, Surveillance Cameras Doing Job*, EAGLE-TRIBUNE (July 28, 2019).

but such fizzling does not rule out an eventual revival.[292] Many failed ordinances dealt only with surveillance cameras, with some councils rejecting the bills because they were too stringent and some because they were not stringent enough.[293] That we found many more instances of failures of single-technology ordinances than of broad surveillance ordinances may speak to the strength of a more flexible administrative, regulatory scheme that can change with time.

2. Acquisition and Use

Thirteen of fourteen municipal entities enacted policies that require approval of acquisition and use of new surveillance technologies by a city council or similar body.[294] Generally, these provisions require police (and other city agencies) to submit reports detailing a range of information about the technology they seek to acquire. This information usually includes: a description of how the technology works, when and in what contexts it will be used, where it will be used, and sometimes anticipated effects on vulnerable communities. In addition, ordinances usually require approval of use plans that detail, for example, authorized use scenarios, data privacy

---

[292] Particularly, St. Louis, Hartford, and Miami Beach have had proposals appear multiple times and then drop off agendas. *See* Lily Liu and Mailyn Fidler, *supra* note 212.

[293] *See* Jackson Cote, *Springfield City Council Passes Facial Recognition Moratorium*, MASSLIVE (Feb. 25, 2020), https://www.masslive.com/springfield/2020/02/springfield-city-council-passes-facial-recognition-moratorium.html (discussing that Springfield's threatened mayoral veto was based on the facial recognition technology being too restrictive); Bera Dunau, *Northampton City Council Overrides Mayor's Veto, Upholds Camera Ordinance*, DAILY HAMPSHIRE GAZETTE (Jan. 10, 2018, 11:17:41 PM), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjx8cHvg7DrAhWXvZ4KHYW-AgUQFjAHegQICxAG&url=https%3A%2F%2Fwww.gazettenet.com%2Fcamera-ordinance-14817532&usg=AOvVaw0EEd2-Uh1YG_q5fvvGCOZU (stating that the mayoral resistance in Northampton seemed to stem from a concern that the regulation was too specific); Teri Figueroa, *City Committee Rejects Smart Street Lights Surveillance Policy in San Diego, Wants a Law Instead*, SAN DIEGO TRIB. (Jan. 29, 2020) (noting that San Diego rejected a video surveillance ordinance in 2020 as not comprehensive enough); Ryan J. Stanton, *Video Surveillance Ordinance Falls Short at Ann Arbor City Council Meeting*, ANN ARBOR NEWS (July 2, 2013), (discussing that Ann Arbor rejected a video surveillance ordinance in 2013 as too restrictive).

[294] New York is the only ordinance that does not; it requires annual reporting. *See* New York ordinance, *supra* note 275.

plans, and mechanisms for internal oversight. Most also require approval for new uses of existing surveillance technology, as well as annual reports of instances of use. The bills surveyed did not require councils to make determinations on whether warrants are required for newly acquired technologies, an area for growth in terms of these kinds of ordinances. Ten of the fourteen entities also require federal funding or loans/gifts of technology to go through the administrative processes.[295] New York is the one city not to require approval of acquisitions; its ordinance requires publishing use policies and annual reporting.[296] Because of its governance structure, the New York city council is limited to this kind of transparency-based oversight of the police.[297]

3. Varied Approaches to Non-Disclosure Agreements

The local policies vary widely in their approach to non-disclosure agreements. Although the ACLU model bill included a ban on non-disclosure agreements with private vendors, only four entities explicitly prohibit NDAs, with one additional city requiring any NDAs be made public; one additional city requires the disclosure of contracts with private entities but is silent regarding NDAs.[298] The remainder of ordinances do not specifically address restrictions on NDAs.[299] As this

---

[295] Somerville, Berkeley, and New York do not explicitly mention federal acquisitions, although Somerville does require approval of data sharing with federal entities. Madison prescribes a less stringent administrative approval process for such tools. *See* Somerville ordinance, *supra* note 275; Berkeley ordinance, *supra* note 275; New York ordinance, *supra* note 275; Madison ordinance, *supra* note 275, at 23.63(6).

[296] New York ordinance, *supra* note 275, at §2.

[297] Mike Maharrey, *New York City Passes Ordinance that Takes First Step Toward Limiting Surveillance State*, TENTH AMEND. CTR. (June 19, 2020).

[298] Prohibiting NDAs: Oakland, CA, *supra* note 275, at §9.64.060; Lawrence, MA, *supra* note 275, at §9.25.110; Yellow Springs, OH, *supra* note 275, at §607.08; and Seattle, WA, *supra* note 275, at §14.18.040(C) (allowing government to share information in response to court orders and effectively overriding NDAs). Requiring public disclosure of NDAs: Berkeley, CA, *supra* note 275, at §2.99.080. Somerville requires disclosure of the existence of contracts with private entities, but is silent with regards to NDAs. Somerville, MA, *supra* note 275, at §1066(b)(9).

[299] Containing no restrictions on NDAs: Santa Clara County; Nashville, TN; Somerville, MA; Palo Alto, CA; Cambridge, MA; Davis, CA; San Francisco, CA; Madison, WI; NYC. *See* Santa Clara Co. ordinance, *supra* note 275; Nashville ordinance, *supra* note 275; Somerville Executive Order, *supra* note 275; Palo Alto ordinance, *supra* note 275; Cambridge ordinance, *supra* note

paper argues—and as the language in the model ACLU bill indicates—non-disclosure agreements with private vendors restrict availability of evidence in court and gives rise to many of police surveillance's troubling aspects. The variation in inclusion of NDA-related clauses is surprising and troubling.

What reason might cities have for forgoing this particular feature of local surveillance governance? Of the local entities with keyword-searchable city council minutes, Santa Clara County and Cambridge returned results for "non-disclosure agreements," so the following analysis is based on limited results. Some of the lack of discussion could be explained by evolution in best practices over time; bans on non-disclosure agreements were not included, for instance, in the first local surveillance ordinance to pass (Seattle's, in 2013, although Seattle later added provisions governing private entities). Santa Clara was only the second entity to pass a surveillance ordinance after Seattle's 2013 version. Debates leading up to the Santa Clara ordinance's passage did include discussion of the problems with non-disclosure agreements but notably only by public defenders.[300] The idea did not gain much traction with the Board, and remaining debate centered primarily around enforcement mechanisms. The final ordinance passed without explicit NDA restrictions.

In Cambridge, explicit non-disclosure language disappeared from early drafts. Non-disclosure restrictions were present in the initial 2016 draft. This language was subsequently dropped from later drafts and discussions, with no explanation present in the record. One explanation could be that the 2016 draft in its entirety was essentially scrapped. But some aspects of the original document made it into the final version—just not this one. Perhaps drafters considered NDAs covered by other sections of the ordinance (i.e. covered under general approval of contracts) or this feature was overtaken by debates about other aspects of the ordinance. Still, given the inclusion of NDA restrictions in the ACLU model bill and the initial 2016 bill, its absence from the debate and the final version of the bill still strikes me as odd. Interest capture could have played a role, but the public record does not include evidence to support that conclusion. The lack of uptake of this particular feature of surveillance governance, in Cambridge and

---

275; Davis ordinance, *supra* note 275; San Francisco ordinance, *supra* note 275; Madison ordinance, *supra* note 275; New York ordinance, *supra* note 275.

[300] *Spec. Meeting Before the County of Santa Clara Fin. and Gov't Operations Comm.* (May 6, 2015, 4:08-4:12 PM); *Reg. Meeting Before the County of Santa Clara Fin. and Gov't Operations Comm.* (Mar. 12, 2015, 3:50 PM).

elsewhere, demonstrates one of the limitations of this kind of governance: it is only as strong as local will and political dynamics make it.

4. Enforcement Provisions

Enforcement provisions vary between bills and often were contentious issues in debates leading up to passage. Cities are clearly making conscious choices about how enforcement of these ordinances should work, and, consequently, to whom relevant power runs. One of the reasons standing and enforcement provisions were so contentious is that, absent a private right of action or other statutory remedy, courts have a limited ability to enforce local administrative rules governing police technology on constitutional grounds. This complication is one reason advocates pushed so hard for private right of action clauses in local ordinances at the possible expense of other desired additions.

The ACLU model bill suggests providing citizen standing to sue for violations of the policy.[301] Only Oakland, Cambridge, Somerville, and Lawrence (MA) provide this broad citizen standing to sue for violations.[302] Santa Clara, Berkeley, Davis, and San Francisco provide limited citizen standing, and Seattle amended its 2013 ordinance in 2017 to provide limited standing.[303] Most of these limited standing clauses contain some variation of the following: standing for citizens comes into effect after providing written notice to the local government and allowing the government a period of, say, 90 days to come into compliance with the policy. Nashville, Yellow Springs (OH), Madison (WI), and New York contain no standing provisions, and Palo Alto explicitly prohibits a private right of action.[304]

Standing provisions were usually the most debated element of these ordinances. Santa Clara passed its ordinance over objection from the county counsel about its enforcement language; ACLU

---

[301] ACLU, *supra* note 174.

[302] *See, e.g.*, Cambridge ordinance, *supra* note 275, at §2.128.080(B) ("Any person injured by a violation of this Chapter may institute proceedings for injunctive relief, declaratory relief, or a court order in a court of competent jurisdiction to enforce the provisions of this Chapter.").

[303] Santa Clara County ordinance, *supra* note 275, at §A40-10; Berkeley ordinance, *supra* note 275, §2.99.080; Davis ordinance, *supra* note 275, at §26.07.070; San Francisco ordinance, *supra* note 275, §19B.8; Seattle ordinance (2017), *supra* note 275, at §14.18.070.

[304] Nashville ordinance, *supra* note 275; Somerville Executive Order, *supra* note 275; Yellow Springs ordinance, *supra* note 275; Madison ordinance, *supra* note 275; New York ordinance, *supra* note 275; Palo Alto ordinance, *supra* note 275, at 2.30.690.

representatives at Santa Clara meetings also repeatedly stressed enforcement, forgoing the opportunity to press for other inclusions.[305] Similarly, Cambridge's standing provisions were subject to fraught debate and went through many iterations. The first version of the bill contained language granting citizen standing, but this language was soon dropped. Instead, other early versions of the bill rested all oversight authority in the City Manager, garnering criticism.[306] Public pushback led to the Public Safety Committee, the relevant city committee, to recommend to the full council that citizen standing be included in the ordinance.[307] In response, the draft ordinance included a provision granting limited citizen standing: citizens could bring suit after giving notice to the City Clerk within 30 days of the violation, and after allowing a further 90 days for the city to remedy the situation.[308] Ultimately, after further debate, the City Manager suggested a revision striking the standing limitations from the bill.[309] The council adopted this language, producing an ordinance providing for broad citizen standing—back where the draft started.

The ACLU model bill also contained language that made violations of surveillance ordinances a misdemeanor for government employees. No local entity makes any violation a misdemeanor, but Santa Clara and Davis make intentional wrongful violations a misdemeanor; San Francisco struck this provision at the last reading and provided no alternate employment sanctions.[310] Oakland, Lawrence (MA), and Yellow Springs (OH) enact employment

---

[305] *Reg. Meeting Before the County of Santa Clara Fin. and Gov't Operations Comm.* (Mar. 12, 2015, at 3:22-3:24 PM); *Spec. Meeting Before the County of Santa Clara Fin. and Gov't Operations Comm.* (May 6, 2015, at 3:02 PM); *Reg. Meeting Before the County of*; *Santa Clara Fin. and Gov't Operations Comm.* (Dec. 10, 2015, at 2:46 PM).

[306] Cambridge City Council Public Minutes, Draft, at 197 (Nov. 21, 2016); Cambridge City Council Agenda Packet, Crockford Comments, at 122 (May 14, 2018).

[307] Craig Kelley, *Objectives of a Successful City Surveillance Ordinance*, Jan. 8, 2017, included in Cambridge City Council Final Action Packet, at 325 (Jan. 22, 2018).

[308] Cambridge City Council Public Minutes, Redline Version, at 102 (Dec.10, 2018).

[309] Cambridge City Council Public Minutes, City Manager Proposed Revisions, at 41, 54 (Nov. 26, 2018).

[310] Santa Clara County ordinance, *supra* note 275, at §A40-12; Davis ordinance, *supra* note 275, at §26.07.070(c); San Francisco ordinance, *supra* note 275, §19B.8(b) (struck).

consequences for employees who violate the policy.[311] Seattle, Nashville, Somerville, Palo Alto, Madison, and Berkeley contain no employee-specific consequences.[312] Again, these provisions were frequently debated. In Santa Clara, the county counsel objected on multiple occasions to the inclusion of the misdemeanor provision.[313] In Oakland, government representatives pushed back against all of the included enforcement measures.[314] Although standing remained in the final Oakland bill, the council removed the misdemeanor offense from the language and replaced it with employment consequences.[315]

5. Updating Local Administrative Governance

Many of the first local attempts at administrative governance of police technology have fallen short of the ideal on a few counts. Primarily, the repeated failure to use local governance to challenge NDA clauses is disappointing, given that the ability to do so is one of this mechanism's strengths. Private sector bargaining power and the intricacies of local procurement may have won out. Similarly, few localities actually included specific warrant requirements for classes of technology, although the case-by-case approval process may still reserve that ability for cities. Although many ended up including enforcement provisions, their effectiveness remains to be seen.

Still, local administrative governance is built to be updated in response to new information and implementation shortcomings in a way that is distinctly different from courts or legislative rules. Administrative governance is supposed to change over time to best conform to the broad goals it serves. And we can see the particular virtue of the administrative approach at work in Somerville, Massachusetts and Seattle already.

Somerville enacted an executive order regarding surveillance technologies in 2017.[316] The city council passed a ban on facial

---

[311] Oakland ordinance, *supra* note 275, at §9.64.050(D); Lawrence ordinance, *supra* note 275, at 9.25.100(B); Yellow Springs ordinance, *supra* note 275, at §607.10.

[312] Seattle ordinance, *supra* note 275; Nashville ordinance, *supra* note 275; Somerville Executive Order, *supra* note 275; Palo Alto ordinance, *supra* note 275; Madison ordinance, *supra* note 275; Berkeley ordinance, *supra* note 275.

[313] *Reg. Meeting Before the County of Santa Clara Fin. and Gov't Operations Comm.* (Feb. 11, 2016); *Reg. Meeting Before the County of Santa Clara Bd. of Supervisors* (June 7, 2016, at 9:32 AM).

[314] Oakland City Council Minutes (Mar. 22, 2018).

[315] Oakland ordinance, *supra* note 275, at §9.64.050.

[316] *See* Somerville Exec. Order, *supra* note 275.

recognition technology in 2019.[317] In the wake of this bill's passage, the council also passed a council-led ordinance regulating surveillance technologies.[318] What began as a mayoral initiative seems to be transforming into a more robust and democratic governance system in Somerville.

The reforms have been more dramatic in Seattle. Seattle, the earliest city to enact this kind of governance in 2013, made fairly substantial updates to its initial set of rules in 2017. Seattle's 2013 ordinance lacked enforcement provisions and turned out to contain an under inclusive definition of surveillance technology focused on hardware, to the exclusion of software.[319] It also contained a wide exception for temporary police use of surveillance technologies without council approval, allowing their use in such cases on the basis of reasonable suspicion, not a warrant.[320] A 2016 scandal, in which the Seattle police acquired the social media monitoring software Geofeedia without informing any of the parties required by city law, exposed the 2013 ordinance's weaknesses.[321] The 2013 version did, however, contain a provision for subsequent review of the ordinance's effectiveness.[322]

Instead of abandoning its effort, or resigning itself to subpar enforcement, the City updated the ordinance in 2017 and 2018. The updates added limited citizen standing as an enforcement measure, annual review requirements, and wider community engagement provisions.[323] Seattle also added language that placed some restrictions on private parties, although not going so far as to ban non-disclosure agreements. Seattle now has at least 29 technologies undergoing

---

[317] *See* Lannan, *supra* note 279.

[318] *See* Plata, *supra* note 279.

[319] Melissa Hellmann*, Seattle's Oversight of Surveillance Technology is Moving Forward Slowly*, SEATTLE TIMES (June 4, 2019).

[320] Phil Mocek, *Seattle City Council Pass Ordinance Restricting Surveillance Equipment After Councilmember Harrell Slips in a Gift for Police*, MOCEK.ORG (Mar. 19, 2013), https://mocek.org/blog/2013/03/19/seattle-passes-ordinance-restricting-surveillance-after-harrell-slips-in-gift-for-police/.

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

[322] Seattle ordinance (2013), *supra* note 275.

[323] Seattle ordinance (2017), *supra* note 275, at §14.18.070, §14.18.060, §14.18.050.

review.[324] Critics counter that the updated version is too unwieldy, requiring review processes of six months or more plus an additional review by a community stakeholder committee, and still does not address data sharing between government agencies.[325] Indeed, some of these measures may be an overcorrection.

This example shows that local administrative governance is not perfect—but it is built to be flexible and responsive to achieve its goals. Within the span of a few years, local administrative governance can be updated to address not only new technologies and new use cases, but also limitations in its own design. This adaptability is where local administrative governance really shines in comparison to court decision-making and even legislative rules.

6. Local Surveillance Governance in Action

Local surveillance ordinances have not been an empty letter. The procedures have worked, allowing municipalities to adopt use and privacy policies alongside new or existing surveillance technologies. Oakland, considered a leader on these issues, approved use and privacy policies for three technologies, stingray devices, Shotspotter (a gunshot detection system), and automated license plate readers (ALPRs).[326] Each of these technologies went through the entire required administrative processes before being voted on by the city council. The police have delivered, as required, annual reports on stingray device use, the earliest technology approved, in every year since approval.[327] Davis adopted use and privacy policies for the technologies its police department already had in use prior to adoption of the surveillance ordinance—body cameras, parking enforcement ALPRs, and

---

[324] Hellmann, *supra* note 319.

[325] *Id.*

[326] Special Concurrent Meeting of the Oakland Redevelopment Successor Agency/City Council Minutes (Nov. 19, 2019); Concurrent Meeting of the Oakland Redevelopment Successor Agency/City Council/Geologic Hazard Abatement Board Minutes (June 18, 2019).

[327] Serge Babka and Timothy Birch, *Cellular Site Simulator—2017 Annual Report*, OAKLAND PRIVACY COMMISSION MEETING AGENDA (Apr. 5, 2018); Omar Daza-Quiroz and Bruce Stoffmacher, Cellular Site Simulator – 2018 Report, OAKLAND PRIVACY COMMISSION MEETING AGENDA (July 24, 2019); Kathryn Jones, *Cellular Site Simulator — 2019 Annual Report*, OAKLAND PRIVACY COMMISSION MEETING AGENDA (Jan. 24, 2020).

Cellebrite forensics devices.[328] Under its new use policy, officers must obtain a warrant to use Cellebrite technologies.[329]

In at least both Oakland and Berkeley, the processes established by the surveillance ordinances stopped adoption (or unapproved adoption of certain surveillance technologies or practices. In Berkeley, the City Manager tried to acquire CycloMedia technology, which takes panoramic snapshots of city streets, outside of the procedures required by the city's surveillance ordinance.[330] The mayor and several city councilors opposed this effort and were successful in rerouting the acquisition through the procedures required by the surveillance ordinance, which includes requiring drafting a use policy prior to deployment.[331]

Oakland's Privacy Advocacy Commission, which serves as the body that reviews use and privacy policies, also pushed back on several occasions. Prior to 2017, the Privacy Advocacy Commission had recommended to the Council that the City sever ties between the Oakland Police Department and Immigrations and Customs Enforcement.[332] In 2017, the City Council passed an ordinance expanding the Privacy Advocacy Commission's oversight role to city participation or cooperation with federal surveillance operations.[333] Subsequently, in 2019, the Commission rejected the annual surveillance report pertaining to federal cooperation as insufficiently transparent.[334] Here, the City chose to expand the remit of the local administrative agency in response to advocacy from that agency itself, which resulted in pushback against the federal government.

Taking a different strategy, the Commission recommended in 2019 that the City amend its surveillance ordinance to permanently ban facial recognition technology; the City did so in the summer of 2019.[335]

---

[328] Anne Ternus-Bellamy, *Council Approves Continued Use of Surveillance Technology*, DAVIS ENTERPRISE: LOCAL NEWS (June 21, 2019), https://www.davisenterprise.com/local-news/council-approves-continued-use-of-surveillance-technology/.

[329] *Id.*

[330] J.P. Massar, *Eternal Vigilance is the Price*, OAKLAND PRIVACY (May 30, 2020); Berkeley City Council Meeting, May 26, 2020.

[331] *Id.*

[332] Timeline, *supra* note 274.

[333] Concurrent Meeting of the Oakland Redevelopment Successor Agency and the City Council Minutes (Oct. 3, 2017).

[334] Oakland Privacy Advisory Commission Minutes (May 2, 2019).

[335] Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology*, *Citing Bias Concerns*, S.F. CHRON. (July 17, 2019).

Instead of relying purely on administrative oversight to control the risks of this particular technology, the agency and the council together decided to pursue an essentially legislative strategy, a Council-led ban on the technology. Here, rather than expand administrative capacity, both bodies worked to affect a legislative solution; perhaps the actors desired the greater democratic accountability that such a solution would bring to a complete ban.

Local administrative governance of surveillance has not been without difficulties, however. Berkeley's consideration of surveillance device use policies has experienced extensive delays. The surveillance ordinance passed in 2018, and as of March 2020, only one policy (for body cameras) had received proper review by the City Council; review of a policy for ALPRs was still pending.[336] The smallest municipality to pass an ordinance—Yellow Springs, Ohio, population approximately 3,700—does not appear to have acquired any additional surveillance equipment since passage of its ordinance, based on a lack of responsive documents in a search of city council records since the adoption. However, a chance exists that the city did, and the acquisition did not go through the appropriate processes. These two scenarios demonstrate the real risk of administrative default in local administrative governance. The intertwined nature of the legislative and administrative functions of local governments may here be a blessing: as in the Berkeley CycloMedia acquisition example, sometimes local legislative pressure can help the administrative processes function properly.

[336] Timeline, *supra* note 274; Annotated Agenda, Berkeley City Council Meeting (Feb. 25, 2020).

Table 3: Features of Local Surveillance Ordinances

Name	*Acquisition Oversight*	*Annual Reports*	*Use Policy Oversight*	*NDA Ban*	*Citizen Standing*	*Employee Discipline for Misuse*	*Explicitly Restricts Federal Acquisitions*
Seattle	Yes	Yes	Yes	Effectively	Yes	No	Yes
Sta. Clara	Yes	Yes	Yes	No	Yes	Yes	Yes
Nashville	Yes	Yes	Yes	No	No	No	Yes
Somerville	Yes	Yes	Yes	No	Yes	No	No
Oakland	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Palo Alto	Yes	Yes	Yes	No	Banned	No	Yes
Cambridge	Yes	Yes	Yes	No	Yes	No	Yes
Lawrence	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Berkeley	Yes	Yes	Yes	Make public	Yes	No	No
Davis	Yes	Yes	Yes	No	Yes	Yes	Yes
Yellow Springs	Yes	Yes	Yes	Yes	No	Yes	Yes
SF	Yes	Yes	Yes	No	Yes	No	Yes
Madison	Yes	Yes	Yes	No	No	No	< scrutiny
New York	No	Yes	No	No	No	No	No

Figure 3

CONCLUSION

Police adoption of new investigative technologies will continue. We need a process that can handle the introduction of new technologies as they arise, not just in response to abuses. We need a process that can run even without the resources it takes to mount a public vote on allowing or banning a new investigative technology. Local administrative governance offers this kind of solution. Importantly, it offers fine-grained control in a setting that is able to take a wide range of interests into consideration and can respond to altered circumstances.

Local administrative governance does not solve the question of political will as it relates to police technology. If a polity does not want to regulate police technology, local administrative governance does not surmount that hurdle. But, it does offer a path of less resistance towards governance. Getting an existing city council to take on a new portfolio takes work, but fewer people need to be convinced in order for it to happen, compared to a legislative response.

This approach, like any, will not solve all problems related to police technology. Still, it offers distinct advantages over the current status quo, and those advantages are bearing out in early adopter cities. Oakland's Privacy Commission, for instance, has successfully received annual disclosures of police use of stingray devices.[337] In contrast, to get that data from Baltimore requires lengthy Freedom of Information

[337] *See* Babka and Birch, *supra* note 327; Daza-Quiroz and Stoffmacher, *supra* note 327; Jones, *supra* note 327.

Request battles.[338] In 2017, Oakland used its stingray devices three times, all for homicide investigations.[339] In 2014, Baltimore logged over 30 pages of stingray device uses, only about 14 percent of which related to homicides.[340] Many differences between the two cities exist, but this anecdote offers hope that local administrative governance of investigative technology offers a way to use the governance infrastructure we have as a control valve for the investigative technologies our police want.

[338] Baltimore Police Dep't, *supra* note 122.
[339] Babka and Birch, *supra* note 327.
[340] Baltimore Police Dep't, *supra* note 122.