Surveying Surveillance: A National Study of Police Department Surveillance Technologies

Mariana Oliver* & Matthew B. Kugler**

Discussions of surveillance practices within U.S. law enforcement agencies often suggest that police departments have ready access to a wide range of high-tech tools. To date, however, most of the empirical evidence regarding police surveillance has come from either qualitative case studies of cities or surveys of the largest departments. While these studies have shed light on the surveillance capacities of large police departments located in larger jurisdictions, our current understanding of police surveillance is limited by a lack of empirical data on police departments in smaller jurisdictions. This study fills this gap by using data from an original nationwide survey of police departments. First, we discuss existing studies of police surveillance access and the legal regimes underlying each type of technology. Next, we use descriptive statistics to empirically examine the variation in police access to surveillance tools across different jurisdiction types. Our findings suggest that rates of police access vary widely depending on the type of technology and jurisdiction size. For instance, overall access to and use of cell phone location tracking far outpaces access to facial recognition and Stingray devices, and all surveillance technologies apart from body cameras are more common in larger jurisdictions. We discuss these findings and their implications for civil rights and liberties and the state of mass surveillance more generally.

INTRODUCTION

In the weeks after the Capitol Hill insurrection on January 6, 2021, federal and local law enforcement began the daunting task of attempting to identify

---

* Mariana Oliver is a J.D./Ph.D. candidate (June 2022, expected) in the Sociology Department at Northwestern University and Northwestern Pritzker School of Law. The authors wish to thank Anne Boustead, Sean Driscoll, Max Schanzenbach, David Schwartz, Victoria Schwartz, Nadav Shoked, Lior Strahilevitz, Zach Summers, Vanessa del Valle, and the participants of the 2021 Privacy Law Scholars conference for their comments on this project. The authors are also grateful to CivicPulse for its help in fielding our survey, Laynie Barringer for her research assistance, and, lastly, the police departments that took the time to respond.

** Matthew B. Kugler is an Associate Professor at Northwestern Pritzker School of Law.

anyone who might have partaken in the violent mob.[1] In this effort, they had an impressive range of tools at their disposal. The FBI acquired "thousands of hours" of video surveillance evidence related to the January riot and could use facial recognition to identify individual suspects.[2] Media outlets have shown how individual rioters can be identified and traced to where they reside using cellphone location data.[3] One suspect was even identified through aggregation of automated license-plate-reader data.[4] Prosecutions over the next several years will presumably further reveal the kinds of tools a well-resourced and highly motivated law enforcement agency can bring to bear.

This narrow window into the highest end of law enforcement surveillance makes it seem like we are living in a cyberpunk world of hyper-monitoring. Yet we know surprisingly little about the surveillance capacities of police departments nationwide at a local level. Which of the tools being used in the highest profile investigations are also available to small police departments? The 2021 insurrection at the Capitol is an instance where we might want police to have the greatest access to surveillance technology. We might also want police to have more body cameras given their potential for police transparency and accountability.[5] Conversely, extensive surveillance of peaceful marches may even be dangerous to civil liberties. But it is hard to have a normative debate about whether, when, and how law enforcement

---

1. *See* Greg Allen, *Law Enforcement and Social Media Identifying U.S. Capitol Mob Members*, NPR (Jan. 7, 2021, 3:45 PM), https://www.npr.org/sections/insurrection-at-the-capitol/2021/01/07/954518782/law-enforcement-and-social-media-identifying-u-s-capitol-mob-members [https://perma.cc/LRD7-WZMC].

2. Litsa Pappas, *FBI 'Working Around the Clock' Using Facial Recognition To Identify Capitol Riot Suspects*, BOS. 25 NEWS (Jan. 12, 2021, 10:58 PM), https://www.boston25news.com/news/fbi-working-around-clock-using-facial-recognition-identify-capitol-riot-suspects/E3G2F54KDJEUFNLKCZQBG4W3CM/ [https://perma.cc/S6QV-BH7U]; Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021. 9:00 AM), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ [https://perma.cc/LUP7-4Y6L].

3. Madison Hall, *The DOJ Is Creating Maps from Subpoenaed Cell Phone Data To Identify Rioters Involved with the Capitol Insurrection*, INSIDER (Mar. 24, 2021, 12:34 PM), https://www.businessinsider.com/doj-is-mapping-cell-phone-location-data-from-capitol-rioters-2021-3 [https://perma.cc/9PRU-QQFC].

4. Jenni Fink, *FBI Traced NYC Sanitation Worker to Capitol Riot with License Plate Readers*, NEWSWEEK (Jan. 22, 2021, 1:09 PM), https://www.newsweek.com/fbi-traced-nyc-sanitation-worker-capitol-riot-license-plate-readers-1563766 [https://perma.cc/RH47-4XS4].

5. *See* Ermus St. Louis et al., *Police Use of Body-Worn Cameras: Challenges of Visibility, Procedural Justice, and Legitimacy*, 17 SURVEILLANCE & SOC'Y 305, 306 (2019).

should be allowed to use surveillance technologies without first knowing the baseline of local police departments' surveillance inputs.

Police surveillance practices have generally been understood to be a black box.[6] Social and legal scholars have sought to open this box through qualitative case studies[7] and surveys[8] of police departments' access to surveillance technologies, but this work has generally focused on the largest jurisdictions. We know, for example, that departments like Baltimore,[9] Los Angeles,[10] Seattle, Oakland, and San Diego,[11] have acquired sophisticated

6. *See* Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503, 503 (2019).

7. *See generally* Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOCIO. REV. 977 (2017) (examining how the Los Angeles Police Department uses big data and new surveillance tools. While our study did not ask about the use of big data per se, some of the surveillance tools we ask about, such as automatic license plate readers and facial recognition, are associated with big data practices); Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1595 (2016) (examining the surveillance practices of police departments in Seattle, Oakland, and San Diego); ÁNGEL DÍAZ, BRENNAN CTR. FOR JUST., NEW YORK CITY POLICE DEPARTMENT SURVEILLANCE TECHNOLOGY 9 (2019), https://www.brennancenter.org/sites/default/files/2019-10/2019_NewYorkPolicyTechnology.pdf [https://perma.cc/HL9W-PTWJ] (evaluating the surveillance tools of the New York City Police Department); Benjamin H. Snyder, *"Big Brother's Bigger Brother": The Visual Politics of (Counter) Surveillance in Baltimore*, 35 SOCIO. F. 1315, 1316 (2020) (discussing Baltimore's experimental use of Wide Area Motion Imagery to address high homicide rates); Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.americaunderwatch.com/ [https://perma.cc/CVE3-VM39] (explaining how police in Detroit, Chicago, Orlando, Washington D.C., and New York City use facial recognition).

8. *See* Ian Adams & Sharon Mastracci, *Police Body-Worn Cameras: Development of the Perceived Intensity of Monitoring Scale*, 44 CRIM. JUST. REV. 386, 391 (2019) (using data from a survey of two large law enforcement agencies within the same county with a population of just over one million); DAN GETTINGER, CTR. FOR THE STUDY OF THE DRONE AT BARD COLL., PUBLIC SAFETY DRONES 1–9 (3rd ed. 2020), https://dronecenter.bard.edu/files/2020/03/CSD-Public-Safety-Drones-3rd-Edition-Web.pdf [https://perma.cc/VB52-6GDM] (presenting a database of public safety agencies with drones); Cynthia Lum et al., *The Rapid Diffusion of License Plate Readers in US Law Enforcement Agencies*, 42 POLICING: AN INT'L J. POLICE STRATS. & MGMT. 376, 376 (2019) (presenting evidence of the diffusion of automatic license plate readers in law enforcement agencies through a national survey of law enforcement agencies with 100 or more officers); SHELLEY S. HYLAND, U.S. DEP'T OF JUST., NCJ 251775, BODY-WORN CAMERAS IN LAW ENFORCEMENT AGENCIES, 2016, at 5 (2018), https://bjs.ojp.gov/content/pub/pdf/bwclea16.pdf [https://perma.cc/U3Z7-XFSA] (showing that the smallest police departments account for the largest share of body camera access).

9. *See generally* Snyder, *supra* note 7, at 1316.

10. *See generally* Brayne, *supra* note 7 (studying the Los Angeles Police Department's use of big data analytics).

11. *See generally* Crump, *supra* note 7, at 1595 (evaluating the procurement of surveillance technologies in Seattle, Oakland, and San Diego).

surveillance tools. Taken together, these studies suggest that large police departments gain access to and use surveillance tools with relative ease and in relative secrecy, unless outside pressure forces disclosure.[12]

Though these studies provide unique and important in-depth accounts of the surveillance inputs of some of the largest police jurisdictions in the country, in general, they have not examined rates of acquisition in small police departments.[13] Recent scholarship has pointed out that our policy prescriptions may be misguided if we fail to consider heterogeneity across jurisdictions.[14] Many such current policies cater to police agencies serving larger jurisdictions, despite the fact that policing in the United States remains a highly localized, non-uniform endeavor.[15] Most U.S. police departments are not Los Angeles, Baltimore, or New York City, in terms of both personnel and financial resources.[16] In fact, a 2016 survey of police departments found that more than two-thirds of all local police departments served populations of fewer than 10,000 residents.[17] To some extent, this over-emphasis on police departments in larger and urban areas is understandable given that most of the U.S. lives in urban areas and, consequently, is policed by urban departments. Nevertheless, given discussions of the proliferation of mass surveillance in policing,[18] we should know whether in fact access to surveillance tools is as ubiquitous to *all* police departments as current accounts would suggest.

---

12. *See, e.g.*, Crump, *supra* note 7, at 1605–15 (discussing the passage of a Seattle ordinance requiring city council approval prior to use of surveillance technology in response to public controversy over the police department's use of a drone).

13. *See* GETTINGER, *supra* note 8, at 5; HYLAND, *supra* note 8, at 2 (noting exceptions). However, the Gettinger study does not differentiate among agencies with fewer than 100 employees. Therefore, we do not know how many of the agencies in this sample would be considered "small" for the purposes of our study.

14. *See* ANNE E. BOUSTEAD, HOOVER INST., AEGIS PAPER SERIES NO. 1802, SMALL TOWNS, BIG COMPANIES: HOW SURVEILLANCE INTERMEDIARIES AFFECT SMALL AND MIDSIZE LAW ENFORCEMENT AGENCIES 1–2 (2018), https://www.hoover.org/sites/default/files/research/docs/boustead_webready pdf.pdf [https://perma.cc/YZ4R-PVWJ].

15. *Id.* at 2 (citing L. Edward Wells et al., *Community Characteristics and Policing Styles in Suburban Agencies*, 26 POLICING: AN INT'L J. POLICE STRATS. & MGMT. 566, 566 (2003)).

16. *Id.* at 5, 7 (noting police departments that serve larger jurisdictions employ more people and have greater access to resources, including surveillance tools, than those serving small and midsize jurisdictions).

17. BUREAU OF JUST. STAT., U.S. DEP'T OF JUST., NCJ 252835, SUMMARY: LOCAL POLICE DEPARTMENTS, 2016: PERSONNEL (2019), https://bjs.ojp.gov/content/pub/pdf/lpd16p_sum.pdf [https://perma.cc/Z6A6-8QR9].

18. *See generally* Brayne, *supra* note 7.

To have a more representative account of police department surveillance capacities, we need national evidence that accounts for the full range of police jurisdictions, including small, midsize, and large. An additional limitation of existing research is that we appear to know quite a lot about police acquisition of some surveillance tools, for example body cameras, but relatively little about others. Moreover, quantitative surveys of police surveillance generally do not consider the legal regimes underlying use of these technologies. What kind, if any, of federal and state restrictions govern law enforcement's use of surveillance technologies? This information matters because it provides context and potential explanations for why police jurisdictions do or do not have access to certain surveillance tools.

We begin to fill this gap. First, we review the legal regimes underlying each of the nine types of surveillance tools that we ask about in our survey. This overview shows which surveillance tools are restricted by legal process, and which are instead restricted by cost or expertise. Then, using a self-developed, national survey of U.S. police departments, we test the current scale of police surveillance acquisition for a variety of technologies in both large and small jurisdictions.[19] This has the effect of providing a baseline of what police surveillance capacities look like across a range of jurisdictional contexts. Understanding the acquisition trends among small police departments is important when we consider that "the overall median size [of local police departments] was 8 full-time officers" by 2008 figures.[20] In contrast, only 5% of departments employed 100 or more full-time officers.[21] Given the more limited resources of smaller police departments, it is likely that such departments will be more focused on meeting basic technological needs than on acquiring advanced surveillance technologies like facial recognition and Stingrays.

Our results confirm this hypothesis. Overall, we find that police departments are more likely to have access to cellphone location information and body cameras than other types of surveillance technologies. In fact, a strong majority of even the smallest departments requested cellphone location data from service providers. In contrast, fewer than 10% of departments reported using facial recognition technology or Stingray devices. Our finding regarding the prominent use of cellphone location information is

19. Our survey asks about drones, cellphone location, cell site simulators, facial recognition, and video surveillance.

20. *See* BRIAN A. REAVES, U.S. DEP'T OF JUST., NCJ 233982, CENSUS OF STATE AND LOCAL LAW ENFORCEMENT AGENCIES, 2008, at 4 (2011).

21. *Id.*

important, as it suggests that this particular surveillance tool deserves substantial scholarly attention. Similarly, our finding showing a high reported use of body cameras suggests these deserve similar attention from privacy and civil rights scholars. This also suggests that the movement advocating for body cameras as a tool of police accountability has achieved substantial success in at least getting the cameras into the hands of local police.[22] On the other hand, empirical evidence on the perceived effects of body cameras on police transparency remain mixed.[23]

Examining the results by jurisdiction size, we find that larger jurisdictions tend to have the highest concentration of police departments with access to surveillance technologies—this finding holds true across all of our survey's surveillance categories, excepting only body cameras. Our findings support existing case study work suggesting that large jurisdictions experience high-tech police surveillance. However, further work is needed to differentiate the most populous jurisdictions—Chicago, Los Angeles, San Francisco, New York, etc.—from the merely large ones. On the other hand, the fact that our results show that jurisdictions of under three thousand people have the highest percent of police departments with body camera technology suggests that jurisdiction size is not always determinative of police surveillance capabilities. As noted, one reason for this may have to do with pressures from outside groups on police departments to adopt body cameras as a tool of public accountability.

Our study also reveals that only a small share of departments have a designated data chief or have formal policies governing their surveillance technologies. Though a majority of all police departments in our sample reported having basic technology access, less than one-third reported having a designated technology chief. This means that were police departments to acquire more surveillance equipment in the future only a small percent would have someone specifically designated to oversee its use.

This study supplements insights from qualitative studies of surveillance with quantitative survey evidence. Part I reviews what we already know, empirically, about police surveillance technologies. Our review shows that existing studies over-represent the surveillance practices of police departments located in larger—and often the largest—jurisdictions. In Part II, we provide a description of our survey and statistical methods. Part III sets out our findings from the survey and discusses their implications. We

22. *See* St. Louis et al., *supra* note 5, at 308.
23. *Id.* at 309.

conclude by calling for more empirical and theoretical investigations of body camera and cellphone location technologies given their wide usage across police departments.

I. WHAT WE KNOW ABOUT POLICE SURVEILLANCE CAPABILITIES

To date, scholars have sought to examine the nature and scope of law enforcement surveillance capabilities by studying some of the largest police departments.[24] This evidence comes from both social science[25] and legal studies[26] that rely on surveys or case studies as their primary source of data. Case study evidence on body-worn cameras, for example, shows that most departments located in major American cities have or plan to acquire this technology.[27] As our review shows however, we do not know whether surveillance tools like body cameras, facial recognition, or Stingrays, to name just a few, are also a common feature of policing in small jurisdictions. This empirical gap limits our ability to discuss the implications of police surveillance for individual privacy and civil liberties more generally.

Below, we review the existing evidence on police surveillance inputs in greater detail. The literature review is organized by a general overview of the major surveillance technologies in use among police,[28] what the law currently says (or does not say) about each, and what we know about police departments' current use of these technologies. In total, we review nine types of distinct police surveillance tools, each of which we asked about in our national 2020 survey of police surveillance.

---

24. *See generally* sources cited *supra* notes 9–11.

25. *See generally* Brayne, *supra* note 7; Snyder, *supra* note 7; Adams & Mastracci, *supra* note 8; Lum et al., *supra* note 8.

26. *See* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 31 (2017). *See generally* Crump, *supra* note 7; Garvie & Moy, *supra* note 7.

27. Joh, *supra* note 26 (pointing to a 2015 survey showing high demand for body cameras among a majority of police and sheriff's departments in large U.S. cities).

28. Our selection of surveillance technologies was informed by a combination of existing literature on the categorization of and primary use of surveillance tools by police. See *infra* Part II for further discussion.

A. Cellphone-Related Monitoring

1. Cellphone Location Technology

Modern cellphones regularly convey location information to the cellphone's service provider.[29] Cellphone towers in proximity to a cellphone pick up the phone's cell-site location information at various time points, and wireless cellphone carriers then store this data for their records.[30] Law enforcement officials can obtain this data from cellphone providers.[31] We know that there are tens of thousands of such requests per year.[32] What we do not know is which, or how many, departments are submitting these requests.

Cellphone location tracking is unusual within our list of surveillance tools in that it is not a device law enforcement owns but instead a trove of data it seeks to access. Though normally the Fourth Amendment does not extend to protect individuals' personal information stored in a third-party's business records, such as a cellphone company, the Supreme Court held in 2018 that cell-site location information is different.[33] In *Carpenter v. United States*, the Court recognized individuals did have a Fourth Amendment privacy interest in seven days-worth of historic cell-site location information.[34] There is therefore some legal cost to acquiring this information, even though there is no particular piece of technology that a department must buy in order to use it.

Despite *Carpenter*'s holding regarding historic cell-site location information, there is much less protection for other cellphone location data. It is quite common for cellphone companies to receive emergency requests

---

29. Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).

30. *Id.*; *see also* Emma W. Marshall et al., *Police Surveillance of Cell Phone Location Data: Supreme Court Versus Public Opinion*, 37 BEHAV. SCIS. & L. 751, 754 (2019).

31. *See* Dennis H. Braithwaite & Allison L. Eiselen, *Nowhere To Hide? An Approach To Protecting Reasonable Expectations of Privacy in Cell Phone Location Data Through the Warrant Requirement*, 38 AM. J. TRIAL ADVOC. 287, 289 (2014) (providing an example of police contacting a cellphone carrier to obtain the real-time location of a defendant).

32. *See* VERIZON, VERIZON'S TRANSPARENCY REPORT FOR THE 2ND HALF OF 2020 (2020), https://www.verizon.com/about/sites/default/files/US-Transparency-Report-2H-2020.pdf [https://perma.cc/ZEU7-YU69]. In the second half of 2020, Verizon reported 15,061 warrants or court orders specifically for location information. *Id.* at 1. It is unclear how many of the 37,760 emergency requests during that period were for location data. *See id.* at 3–4.

33. *Carpenter*, 138 S. Ct. at 2216–18 (distinguishing past business record cases and creating a new rule for cellphone location data).

34. *Id.* at 2217 & n.3.

for real-time location information.[35] One avenue for such requests is a provision of the Stored Communications Act that allows for providers to disclose non-content information to the government when there is an emergency involving a risk of "death or serious physical injury."[36] This represents a somewhat lower legal cost than, for example, that associated with historic cell-site information.

While empirical evidence on local law enforcement's use of cellphone location data remains lacking, we do know that police departments located in urban, and hence larger, jurisdictions are more likely to be able to pinpoint—with the aid of wireless companies—the exact location of a cellphone relative to departments in non-urban, smaller jurisdictions.[37] We also know from cellphone provider transparency reports that these location requests are fairly common. Verizon alone received over 13,000 warrants for cellphone location data in the second half of 2020.[38]

2. Stingray Devices

Another cellphone-related technology that our survey examined was cell-site simulators or international mobile subscriber identity catchers, also known as "Stingray" or "Triggerfish" devices.[39] A Stingray device works by imitating a cellphone tower and picking up signals from any nearby

35. *See, e.g.*, VERIZON, *supra* note 32 (showing between two and three times as many emergency requests as warrants for all information types).

36. 18 U.S.C. § 2702(c)(4). For examples of this post-*Carpenter*, see United States v. Saemisch, 371 F. Supp. 3d 37, 42–43 (D. Mass. 2019); United States v. Andrews, No. 18-CR-149 (SRN/DTS), 2019 WL 669808, at *7 (D. Minn. Feb. 19, 2019); United States v. McHenry, 849 F.3d 699, 705 (8th Cir. 2017) (decided pre-*Carpenter*).

37. *See* Marshall et al., *supra* note 30, at 754 (noting that urban areas tend to have a higher concentration of cellphone towers, thereby making it easier to pinpoint a more precise cellphone location).

38. *See, e.g.*, VERIZON, *supra* note 32 ("During the second half of 2020, we received 13,678 warrants based on probable cause for location data. In addition, we received 1,469 warrants or court orders for 'cell tower dumps' during the second half of 2020.").

39. *See* Nicole Valdes Hardin, *Uncovering the Secrecy of Stingrays: What Every Practitioner Needs To Know*, 32 CRIM. JUST. 20, 20–21 (2018); *see also* Manes, *supra* note 6, at 513.

cellphones to track the locations of the devices.[40] Stingray technology is not cheap—departments can pay upwards of $148,000 just for a basic package.[41]

In addition to the financial cost of acquiring a Stingray device, some courts have held that use of Stingray devices violates Fourth Amendment privacy expectations and therefore requires a warrant.[42] Though there are not many decisions on this point, and no intervention by the Supreme Court as yet, it has been Department of Justice policy to seek warrants for Stingray device use since 2015.[43] Several states also have statutes that require warrants for Stingray use.[44] As a result, the legal cost of Stingrays is relatively high compared to other surveillance technologies.

Given the secrecy surrounding law enforcement's use of Stingray devices,[45] it is hard to know exactly how common or prevalent this practice is. Legal case studies have suggested it is likely that police in St. Louis and Baltimore used Stingrays and kept this from the public.[46] In addition, a 2018 report from the ACLU shows that police departments in at least twenty-seven states are known to have or use Stingrays.[47] Of these departments, all are in larger jurisdictions. We know virtually nothing about their use in departments located in small jurisdictions.

---

40. Hardin, *supra* note 39, at 21.

41. Kim Zetter, *How Cops Can Secretly Track Your Phone*, INTERCEPT (July 31, 2020, 4:00 AM), https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ [https://perma.cc/2MYX-YUJQ].

42. *See, e.g.*, Jones v. United States, 168 A.3d 703, 714–15 (D.C. 2017); People v. Gordon, 68 N.Y.S.3d 306, 311 (N.Y. Sup. Ct. 2017).

43. DEP'T OF JUST., DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/VZ85-3G5R].

44. *See, e.g.*, WASH. REV. CODE § 9.73.260 (2022); *see also* Cyrus Farivar, *Judge Rules in Favor of "Likely Guilty" Murder Suspect Found via Stingray*, ARS TECHNICA (Apr. 26, 2016, 10:30 AM), https://arstechnica.com/tech-policy/2016/04/citing-unconstitutional-search-via-stingray-judge-suppresses-murder-evidence/ [https://perma.cc/2HQH-ZVMD] (citing laws in California, Virginia, Minnesota, and Utah).

45. *See* Spencer McCandless, Note, *Stingray Confidential*, 85 GEO. WASH. L. REV. 993, 998–99 (2017) (citing Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 13–14, 13 n.58 (2014)).

46. *See* Joh, *supra* note 26, at 25–26.

47. *Stingray Tracking Devices: Who's Got Them?*, ACLU (Nov. 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them [https://perma.cc/MZ6V-5V97].

B. Video and Visual Monitoring

Video monitoring surveillance has been defined as the "observation of people, places, and machines."[48] Here we consider both traditional stationary surveillance cameras as well as more recent innovations such as body-worn cameras, automatic license plate readers, drones, and Ring video doorbell systems. We also address the use of global positioning systems (GPS) devices to track vehicles on public roads.

1. Video Cameras (Closed-Circuit Television)

Police departments increasingly rely on stationary video cameras, or closed-circuit television, in public spaces for crime prevention and investigation purposes.[49] As with other types of surveillance technology, evidence of police acquisition of closed-circuit television systems has been limited to cities in larger jurisdictions.[50]

The use of public video cameras does not generally implicate the Fourth Amendment. By default, the police are free to observe whatever may be seen from a place where they are entitled to be,[51] and "[n]othing in the Fourth Amendment prohibit[s] the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afford[s] them."[52] Most courts have therefore held that even

---

48. *See* Samuel Nunn, *Police Technology in Cities: Changes and Challenges*, 23 TECH. SOC. 11, 14 (2001).

49. *See* Hyungjin Lim & Pamela Wilcox, *Crime-Reduction Effects of Open-Street CCTV: Conditionality Considerations*, 34 JUST. Q. 597, 598 (2017).

50. *See* NANCY G. LA VIGNE ET AL., URB. INST., EVALUATING THE USE OF PUBLIC SURVEILLANCE CAMERAS FOR CRIME CONTROL AND PREVENTION—A SUMMARY 1–3 (2011), https://www.urban.org/sites/default/files/publication/27546/412401-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention-A-Summary.PDF [https://perma.cc/9XVE-EEF6] (evaluating Baltimore, Chicago, and Washington, D.C.); Giovanni Circo & Edmund McGarrell, *Estimating the Impact of an Integrated CCTV Program on Crime*, 17 J. EXPERIMENTAL CRIMINOLOGY 129, 132 (2021) (studying CCTV use in Detroit); *see also* Megan Hickey, *19th Ward Gets Influx of Police Cameras, License Plate Readers, But Do Cameras Help Reduce Crime?*, CBS CHI. (Feb. 5, 2021, 6:16 PM), https://chicago.cbslocal.com/2021/02/05/south-side-chicago-police-cameras-crime/ (discussing surveillance cameras in Chicago).

51. *See* Florida v. Riley, 488 U.S. 445, 449–50 (1989); United States v. Knotts, 460 U.S. 276, 282 (1983).

52. *Knotts*, 460 U.S at 282. The Supreme Court goes on to quote *United States v. Lee*'s holding that the use of a search light or a telescope was not prohibited by the Fourth Amendment

prolonged video surveillance of private property is not a search under the Fourth Amendment.[53] Though there is some dispute over this,[54] the majority rule is that warrants are not required for video surveillance of private property. Cameras aimed at public streets are not problematic under current case law.[55] The legal cost of video surveillance is therefore quite low, as is the cost of any single or small number of cameras.

Police use closed-circuit video surveillance for purposes including police investigations, arrests, and observing individuals of interest to police.[56] Here also, existing studies have documented police use of video surveillance in medium and large jurisdictions, but not small ones.[57] Nationally, just under half of all local police departments in the United States have reported use of

---

to support technologically enhanced visual surveillance within the ambit of a reasonable expectation of privacy. *Id.* at 282–83 (quoting United States v. Lee, 274 U.S. 559, 563 (1927)).

53. United States v. Houston, 813 F.3d 282, 287–88 (6th Cir. 2016) ("[A]gents only observed what [the defendant] made public to any person traveling on the roads surrounding the farm."); *see also* United States v. Jackson, 213 F.3d 1269, 1281 (10th Cir. 2000) (holding that a pole camera is not a search even if it observes the curtilage of a property), *vacated on other grounds*, 531 U.S. 1033 (2000). *Jackson* is still the law of the 10th Circuit. *See* United States v. Cantu, 684 F. App'x 703, 703 (10th Cir. 2017); *see also* United States v. Brooks, 911 F. Supp. 2d 836, 843 (D. Ariz. 2012) (holding that law enforcement's use of a pole camera for long-term surveillance did not violate Fourth Amendment protections). *Contra* United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) (holding that such camera surveillance is a search given the fences erected by the defendant); *but see* State v. Jones, 903 N.W.2d 101, 113–14 (S.D. 2017).

54. For instance, the South Dakota Supreme Court recently held that pole camera surveillance of a front yard for two months was a Fourth Amendment violation. *Jones*, 903 N.W.2d at 113–14.

55. *Knotts*, 460 U.S. at 281.

56. Lim & Wilcox, *supra* note 49, at 598.

57. *Id.* at 599 (citing Jerry H. Ratcliffe et al., *The Crime Reduction Effects of Public CCTV Cameras: A Multi-Method Spatial Approach*, 26 JUST. Q. 746 (2009)) (focusing on Cincinnati); LA VIGNE ET AL., *supra* note 50, at 1–3 (focusing on Baltimore, Chicago, and Washington, D.C); *see also* JENNIFER KING ET AL., CITRIS REPORT: THE SAN FRANCISCO COMMUNITY SAFETY CAMERA PROGRAM: AN EVALUATION OF THE EFFECTIVENESS OF SAN FRANCISCO'S COMMUNITY SAFETY CAMERAS (2008), https://www.wired.com/images_blogs/threatlevel/files/sfsurveillancestudy.pdf [https://perma.cc/7QAA-7C6N] (focusing on San Francisco); Brandon C. Welsh & David P. Farrington, *Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis*, 26 JUST. Q. 716, 722–26 (2009) (focusing on New York City, Brooklyn, and Cincinnati, in addition to other areas in the UK); Sarah J. McLean et al., *Here's Looking at You: An Evaluation of Public CCTV Cameras and Their Effects on Crime and Disorder*, 38 CRIM. JUST. REV. 303, 323–26 (2013) (focusing on Schenectady); Joel M. Caplan et al., *Police-Monitored CCTV Cameras in Newark, NJ: A Quasi-Experimental Test of Crime Deterrence*, 7 J. EXPERIMENTAL CRIMINOLOGY 255, 264–69 (2011) (focusing on Newark).

video surveillance, a number that increases to almost 90% among police in large jurisdictions with 250,000 or more residents.[58]

2. Body-Worn Cameras

Body-worn cameras are both a tool for surveillance as well as a mechanism for police accountability.[59] These devices can be attached to an officer's person and allow the recording of a variety of officer interactions.[60] The main reasons departments will acquire body-worn cameras include judicial proceedings (e.g., video evidence in court), officer safety (the idea being that cameras deter violence), officer accountability, and other types of common officer interactions.[61]

There is no Fourth Amendment issue with use of body cameras. This is a fairly straightforward application of the principle that the police are free to observe, from a lawful location, anything that occurs in a public place.[62] Though many states have laws on body cameras, few have limitations on their use. Common provisions in existing laws include ones that exempt certain body-camera footage from open records requests,[63] require the development of written body-camera policies,[64] or regulate the interface of body cameras and anti-wiretapping laws.[65] Some states even specifically require the use of body cameras by some or all officers.[66]

---

58. Eric L. Piza et al., *CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis*, 18 CRIMINOLOGY & PUB. POL'Y 135, 136 (2019).

59. *See* Candice Norwood, *Body Cameras Are Seen as Key to Police Reform. But Do They Increase Accountability?*, PBS NEWS HOUR (June 25, 2020, 4:41 PM), https://www.pbs.org/newshour/politics/body-cameras-are-seen-as-key-to-police-reform-but-do-they-increase-accountability [https://perma.cc/NVW6-D54Z].

60. NAT'L INST. OF JUST., A PRIMER ON BODY-WORN CAMERAS FOR LAW ENFORCEMENT 5 (2012), https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/a-primer-on-body-worn-cameras-for-law-enforcement.pdf [https://perma.cc/L76Y-DENE].

61. *Id.* at 3–4.

62. *See supra* notes 51–52 and accompanying text.

63. *Body-Worn Camera Laws Database*, NCSL (Apr. 30, 2021), https://www.ncsl.org/research/civil-and-criminal-justice/body-worn-cameras-interactive-graphic.aspx#/ [https://perma.cc/Q47W-UTJS] (citing laws in Connecticut, Texas, Florida, and Oregon, among others, having a variety of disparate open records policies).

64. *Id.* (nineteen states and the District of Columbia).

65. *Id.* (seven states).

66. *Id.* (five states); *see also Illinois Legislature Passes Bill Mandating Body Cameras for All Officers*, POLICE: L. ENF'T SOLS. (Jan. 13, 2021), https://www.policemag.com/590595/illinois-legislature-passes-bill-mandating-body-cameras-for-all-officers [https://perma.cc/7V62-PLN8].

By 2015, the major seller of body cameras, Axon,[67] had secured contracts for body-worn cameras with prominent police departments located in some of the largest jurisdictions.[68] A 2016 Bureau of Justice survey of body cameras in law enforcement found that 47% of respondents reported having the technology.[69] The study, which tracked responses by type and size of agency,[70] showed that police acquisition of body-worn cameras has been associated with police departments located in larger jurisdictions.[71] The Bureau's study is especially notable in that it appears to be the only one of its kind, and because it focused on this particular surveillance technology rather than taking a more general approach to surveying police departments.

3. Drones

Unmanned aerial vehicles, more commonly known as drones, have become a feature of local policing, with police using drones to locate both suspects and missing persons, record video footage of an area, and for investigative purposes more generally.[72] The many available functions of drones, including cameras, remote operation, and facial recognition,[73] make these valuable tools from the perspective of law enforcement officers.

Aerial observation is generally permissible under the Fourth Amendment.[74] A court could, in theory, hold that drones are subject to a different standard than prior cases involving helicopters and fixed-wing

---

67. Formerly called TASER International. Stephen Nellis, *Taser Changes Name to Axon in Shift to Software Services*, REUTERS (Apr. 5, 2017, 9:07 AM), https://www.reuters.com/article/us-usa-taser/taser-changes-name-to-axon-in-shift-to-software-services-idUSKBN177265 [https://perma.cc/Y6FH-UUU2].

68. Akela Lacy, *Two Companies Fight to Corner the Police Body Camera Market*, INTERCEPT (Dec. 8, 2021, 11:26 AM), https://theintercept.com/2021/12/08/police-reform-body-cameras-axon-motorola/ [https://perma.cc/WXM5-QS4S].

69. *See* HYLAND, *supra* note 8, at 1.

70. *Id.* at 2 (note that smaller departments here are defined as those with only part-time sworn officers).

71. *Id.* at 2 tbl.1; *see also* Joh, *supra* note 26, at 31–32.

72. *See* Jessica Dwyer-Moss, *The Sky Police: Drones and the Fourth Amendment*, 81 ALB. L. REV. 1047, 1048–49 (2017).

73. *See* DÍAZ, *supra* note 7, at 9.

74. California v. Ciraolo, 476 U.S. 207, 213–14 (1986) ("[W]e readily conclude that respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor."); *see also* Florida v. Riley, 488 U.S. 445, 450–51 (1989) (finding no reasonable expectation that a partially open greenhouse was protected from helicopter surveillance).

aircrafts. The Court in *Florida v. Riley* stressed that it was legal for the helicopter to be flying where it was.[75] So a person in a state or locality that banned drone flight, or drone flight at a given altitude, might have a reasonable expectation of privacy against drone surveillance.[76] One Michigan appellate court has reached this result, but it is the only one of which we are aware.[77] Several states have passed laws specifically restricting the use of drones by law enforcement agencies, however. Florida, for instance, imposes a warrant requirement subject to narrow exceptions.[78] One agency counted seventeen other states with similar requirements as of 2019,[79] and there appears to be active legislative movement in this area.[80] In 2021, the Fourth Circuit held that Baltimore's program of constant aerial surveillance—aircraft recording the city during most daylight hours—violated the Fourth Amendment because it "'tracks every movement' of every person outside in Baltimore."[81] The legal cost of aerial surveillance therefore depends on both the jurisdiction and the degree of intrusiveness.

Much of what we know about police drone acquisition comes from the Center for the Study of the Drone at Bard College.[82] The latest figures from their database show that 559 municipal police departments had acquired drones as of 2020.[83] The Center predicts that police use of drones will only grow, and it is likely that their numbers under-represent the actual total given the practice among neighboring law enforcement agencies of sharing or

---

75. *Riley*, 488 U.S. at 451. *But see id.* at 455 (O'Connor, J., concurring) (rejecting that basis for the holding and instead suggesting that frequency of flight, rather than legality, should be the crucial test).

76. *See generally* Syracuse Univ., Inst. for Sec. Pol'y & L., *Local Regulation*, DOMESTICATING THE DRONE, http://uavs.insct.org/local-regulation [https://perma.cc/8RTJ-G3BB] (listing regulations by state and municipality).

77. Long Lake Twp. v. Maxon, No. 349230, 2021 WL 1047366, at *7 (Mich. Ct. App. Mar. 18, 2021).

78. FLA. STAT. § 934.50 (2022).

79. 911 SECURITY, U.S. DRONE LAWS: OVERVIEW OF DRONE RULES AND REGULATIONS IN USA BY STATE 2 (2019), https://www.utsystem.edu/sites/default/files/offices/police/policies/USDroneLaws.pdf [https://perma.cc/5H2X-6CFG].

80. *Current Unmanned Aircraft State Law Landscape*, NCSL (Aug. 3, 2021), https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx [https://perma.cc/4LLA-V5Q6] (noting eleven pieces of state legislation in 2020 concerning drones).

81. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 341 (4th Cir. 2021).

82. *See* GETTINGER, *supra* note 8, at 1.

83. *Id.* at 2.

contracting out drone services.[84] One limitation of this database is that it is not broken down by large versus small jurisdictions.[85] Interestingly, survey evidence from one 2018 study shows that municipal law enforcement agencies with fewer than 100 employees accounted for the largest share of agencies with drones.[86]

4. Amazon Ring

Developed by Amazon, Ring integrates internet-capable cameras into doorbells. Police departments can indirectly make use of this technology by requesting video footage from owners of the device,[87] or by requiring the production of footage via legal mechanisms such as search warrants, subpoenas, and court orders.[88] Partnerships between Ring and law enforcement agencies function as a mechanism to facilitate the consensual requesting of Ring video footage.

Searches conducted by private actors are not subject to the Fourth Amendment unless the private actors are working on behalf of the government.[89] Law enforcement can ask people to consensually turn over their video doorbell footage without running afoul of any constitutional provision. There also do not appear to be any state laws restricting their ability to do so. There therefore does not appear to be any financial or legal cost in these partnerships, beyond whatever coordination is necessary to initially establish them.

There is little empirical documentation of how widespread Ring partnerships are among local police departments. An accurate assessment of this may be difficult in part due to the fact that law enforcement can request video footage directly from home or business owners. Nevertheless, we do

---

84. *Id.* at 1.

85. *See id.* at 2–9.

86. DAN GETTINGER, CTR. FOR THE STUDY OF THE DRONE AT BARD COLL., PUBLIC SAFETY DRONES: AN UPDATE 5 (2018), https://dronecenter.bard.edu/files/2018/05/CSD-Public-Safety-Drones-Update-1.pdf [https://perma.cc/P2AS-W8AU].

87. Matthew Guariglia, *Ring Changed How Police Request Door Camera Footage: What It Means and Doesn't Mean*, EFF (June 7, 2021), https://www.eff.org/deeplinks/2021/06/ring-changed-how-police-request-door-camera-footage-what-it-means-and-doesnt-mean [https://perma.cc/ZD2W-YWUX].

88. *See Law Enforcement Information Requests in 2020*, RING (Jan. 20, 2021), https://blog.ring.com/2021/01/20/law-enforcement-information-requests-in-2020/ [https://perma.cc/U37X-85CQ].

89. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

know that the number of departments using Amazon's Ring security cameras has risen sharply in just two years.[90] There is evidence suggesting a large number of police departments have joined Amazon's Ring network, but this study included both police and fire departments and did not differentiate between the two.[91] There does not appear to be data on what kinds of departments are represented within this figure.

5. Automatic License Plate Readers

Automatic license plate readers are "high-speed camera and information systems" that police use to record vehicle license plates and to photograph cars and the people within them.[92] Police can place automatic license plate readers onto their patrol cars as well as onto fixed structures such as street poles.[93]

Courts specifically considering whether the use of automatic license plate readers implicates the Fourth Amendment have generally rejected the claim.[94] The views of courts may shift on this in light of the recent holding in *Carpenter v. United States*,[95] however. For example, the Massachusetts Supreme Judicial Court suggested that a sufficiently comprehensive system of automatic license plate readers would constitute a search for constitutional purposes given cases like *Carpenter*.[96] Even in that case, however, the court

---

90. Kim Lyons, *Amazon's Ring Now Reportedly Partners with More than 2,000 US Police and Fire Departments*, THE VERGE (Jan. 31, 2021, 11:26 AM) https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras [https://perma.cc/6CRS-EBAB].

91. *Id.*

92. *See* Christopher S. Koper & Cynthia Lum, *The Impacts of Large-Scale License Plate Reader Deployment on Criminal Investigations*, 22 POLICE Q. 305, 306 (2019).

93. DÍAZ, *supra* note 7, at 8.

94. United States v. Diaz-Castaneda, 494 F.3d 1146, 1150–51 (9th Cir. 2007) (collecting cases) ("[E]very circuit that has considered the issue in a precedential opinion has held that license plate checks do not count as searches under the Fourth Amendment."); United States v. Ellison, 462 F.3d 557, 561 (6th Cir. 2006) ("No argument can be made that a motorist seeks to keep the information on his license plate private. . . . [A] motorist can have no reasonable expectation of privacy in the information contained on it.").

95. Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018).

96. Commonwealth v. McCarthy, 142 N.E.3d 1090, 1104 (Mass. 2020) ("With enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes.").

held against the defendant on the grounds that the system it was evaluating was not so large and advanced.[97]

Several states have statutes regulating the use of automatic license plate readers. Minnesota, for instance, requires a warrant to use automatic license plate readers' data in criminal investigations.[98] But this level of protection is rare. Nebraska, in contrast, merely requires that government records of automatic license plate readers' data not be retained for longer than 180 days without cause.[99] The National Conference of State Legislatures counts only sixteen states with laws that expressly mention automatic license plate readers as of the spring of 2021,[100] meaning that thirty-four states do not have such statutes.

Within just the past decade, automatic license plate readers have become an increasingly common policing tool.[101] Recent survey research suggests that almost two-thirds of larger police agencies—those with one hundred or more officers—have automatic license plate readers.[102] However, we know little about use of this technology in smaller police jurisdictions.

6. Vehicle Tracking Devices

The physical devices police use to track the movement of vehicles and their passengers rely on global positioning system ("GPS") technology.[103] These devices can be attached to the vehicles of both surveillance suspects and also officers themselves; there is great utility in a police force having real-time information on the location of its own vehicles.[104] In addition to

---

97. *Id.* at 1106.

98. MINN. STAT. § 13.824(2)(d) (2015).

99. NEB. REV. STAT. § 60-3204 (2022). The list of permissible uses is extensive. *Id.* § 60-3203.

100. *Automated License Plate Readers: State Statutes*, NCSL (Apr. 9, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx [https://perma.cc/RVJ9-M7PW].

101. Koper & Lum, *supra* note 92, at 306.

102. *Id.* (defining "large" police agencies as those with 100 or more officers).

103. *See* Tom Hughes & Corey Burton, *Police GPS Surveillance on Vehicles and the Warrant Requirement: "For a While I've Been Watching You Steady"*, 38 AM. J. CRIM. JUST. 535, 535 (2012); *see also* Nunn, *supra* note 48, at 17.

104. *See, e.g.*, Brian Dziuk, *Police GPS Tracking: Your Go-To Guide*, RASTRAC (Oct. 19, 2020, 2:50 PM), https://info.rastrac.com/blog/police-gps-tracking [https://perma.cc/S273-L9NP] (discussing the benefits of tracking police fleets).

being an effective detection system, the global positioning technology that vehicle tracking devices rely on is relatively cheap and easy to use.[105]

In general, people do not have a strong expectation of privacy in their movements on public roads.[106] Cases from the 1980s held that the use of tracking devices was permissible if, one, they only observed a person in their movements in public and, two, the tracking device was planted in property prior to it coming into the possession of the suspect.[107] Installation of a physical tracking device on a vehicle is a search under the Fourth Amendment, however, because such installation involves an intrusion into the private property of the suspect.[108] Similarly, requiring a person to carry or wear a tracking device is a search under the Fourth Amendment.[109]

Use of the global positioning system embedded in vehicle tracking devices has become increasingly common among police.[110] There is evidence that both small and large police departments use this technology.[111] However, aside from what we know from litigation involving police use of vehicle tracking devices,[112] there is little empirical evidence differentiating use across jurisdiction type.

7. Facial Recognition Technology

Facial recognition technology is a system for identifying or verifying individuals by scanning faces in existing databases or from a video feed.[113] For law enforcement, facial recognition technology can serve a range of investigative and crime-prevention functions.[114]

---

105. *See id.*; Hughes & Burton, *supra* note 103, at 536.

106. United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

107. *See* United States v. Jones, 565 U.S. 400, 408–10 (2012) (discussing *Knotts* and United States v. Karo, 468 U.S. 705 (1984)).

108. *Id.* at 404 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

109. Grady v. North Carolina, 575 U.S. 306, 310 (2015).

110. Hughes & Burton, *supra* note 103, at 536.

111. *Id.*

112. *See, e.g.*, John S. Ganz, *It's Already Public: Why Federal Officers Should Not Need Warrants To Use GPS Vehicle Tracking Devices*, 95 J. CRIM. L. & CRIMINOLOGY 1325, 1325–26 (2005).

113. *See* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, 34 CRIM. JUST. 9, 9 (2019).

114. *Id.*

Use of facial recognition by law enforcement is generally permissible under the Fourth Amendment despite the policy concerns raised by some scholars.[115] The problem under most conventional Fourth Amendment analyses is that one's face is not generally considered private.[116] Though a few states and localities have banned or severely restricted law enforcement's use of facial recognition,[117] this is a rare response. Moreover, these types of bans may be evaded through partnerships with neighboring agencies.[118] For instance, the Federal Bureau of Investigation has an extensive facial recognition database and sometimes queries it at the request of local agencies.[119]

---

115. *See, e.g.*, Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1210 (2021) (arguing for limited Fourth Amendment protection supplemented by statutory privacy laws given the strong policy case in favor of limiting facial recognition use).

116. United States v. Dionisio, 410 U.S. 1, 14 (1973) ("No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.").

117. *See State Facial Recognition Policy*, EPIC.ORG, https://epic.org/state-policy/facialrecognition/ [https://perma.cc/NM8N-56TZ] (stating that California has enacted a three-year moratorium on the technology and noting a few municipalities have taken action); Rebecca Ellis, *Portland Passes Nation's Toughest Restriction on Facial Recognition Technology*, OPB (Sept. 9, 2020, 5:47 PM), https://www.opb.org/article/2020/09/09/portland-passes-nations-toughest-restriction-on-facial-recognition-technology/ [https://perma.cc/GZ9L-RWWP] (describing Portland's facial recognition ban which "prohibits city agencies from using facial recognition technology" and bans businesses "from using facial recognition technology in public areas within Portland city limits"); Jim Halpert, *In Washington State's Landmark Facial Recognition Law, Public Sector Practices Come Under Scrutiny and Regulation*, DLA PIPER (Apr. 22, 2020), https://www.dlapiper.com/en/us/insights/publications/2020/04/in-washington-states-landmark-facial-recognition-law-public-sector-practices-come-under-scrutiny/ [https://perma.cc/4ABC-3A45] (describing the severe restrictions imposed by Washington State starting in the summer of 2021).

118. Alfred Ng, *Police Say They Can Use Facial Recognition, Despite Bans*, THE MARKUP (Jan. 28, 2021, 8:00 AM), https://themarkup.org/news/2021/01/28/police-say-they-can-use-facial-recognition-despite-bans [https://perma.cc/V2BU-3PER].

119. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-518, FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD BETTER ASSESS PRIVACY AND OTHER RISKS 43 (2021), https://www.gao.gov/assets/gao-21-518.pdf [https://perma.cc/T3BG-9QL5]; *The Use of Facial Recognition Technology by Government Entities and the Need for Oversight of Government Use of This Technology Upon Civilians: Hearing Before the H. Oversight & Reform Comm.*, 116th Cong. 2 (2019) [hereinafter *Facial Recognition Technology Hearing*] (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation).

Despite widespread concerns about facial recognition and debates over the accuracy of facial recognition software,[120] we lack evidence as to how many local police departments have access to this high-tech tool. Efforts have been made to compile such a list but have largely been limited to small samples.[121] Therefore, we lack national evidence drawing from a larger and broader sample size of the state of facial recognition acquisition among local police departments.

II. SURVEY OF LAW ENFORCEMENT TECHNOLOGY USE

In collaboration with CivicPulse, we conducted a survey of local police departments in June and July of 2020.[122] The survey questions were developed based on consultation with law enforcement experts, examination of the Bureau of Justice Statistics' survey of law enforcement agencies, and the researchers' own expertise. It asked about the inputs in police surveillance capacities, focusing on the different types of technologies that departments might seek to acquire. We drew on existing scholarship of police surveillance inputs to inform our own categorization of the nine surveillance technologies that appear in our survey.[123] These categories appear in our results as "cellphone-related monitoring" and "video monitoring."

Participants were randomly chosen from a universe consisting of the heads of law enforcement of U.S. local governments with populations of over 1,000

120. *See generally* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/TPA3-95E9].

121. *See* Interactive Map, BAN FACIAL RECOGNITION, https://www.banfacialrecognition.com/map/ [https://perma.cc/YH63-6SR3]; *see also* Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/J9NH-T27J] (using a sample size of fifty-two state and local agencies confirmed to use or have used face recognition); Crump, *supra* note 7, at 1629 (focusing on one local police department, San Diego's, use of face recognition).

122. CivicPulse is the research organization that fielded the survey on our behalf. *See generally* Home Page, CIVICPULSE, https://www.civicpulse.org/ [https://perma.cc/L3RE-KTLY]. The organization's expertise is conducting surveys of government officials at all levels. *About Us*, CIVICPULSE, https://www.civicpulse.org/about [https://perma.cc/YD6R-2AYX]. The survey was fielded from June 16, 2020, to July 3, 2020. The survey asked about law enforcement technology use generally before focusing specifically on the issue of COVID-19 enforcement.

123. *See* Nunn, *supra* note 48, at 14 (arguing that law enforcement technologies can broadly be broken into seven distinct categories).

residents plus an existing police department.[124] Because law enforcement is notoriously secretive about its surveillance practices,[125] we could not easily calculate a desired sample size; base rates on key measures were unclear. Our aim therefore was to collect as many responses as possible within a given timeframe. With the exception of the Bureau of Justice Statistic's Law Enforcement Management and Administrative Statistics (LEMAS) survey that has been conducted periodically since 1987,[126] our survey contains the largest national sample of local law enforcement agencies and their access to various surveillance technologies that we know of.

The recruitment email specified that heads of departments should take the online survey themselves, or, if appropriate, they should forward it to another agency official more knowledgeable about the issues addressed by the survey. We had 88.9% of respondents identify themselves as head of their departments. Approximately 80% of the 460 respondents that started the survey completed it. Using partial data where available, there were responses from 432 departments to the key technology questions in the survey. Of these departments, 68 are located in jurisdictions with fewer than 2,600 people, 166 in jurisdictions of between 2,600 and 10,000 people, and 200 in jurisdictions of 10,000 or more.[127]

Compared to survey studies of the general population, our response rate was relatively low.[128] As with many studies, systematic non-response bias is certainly a possibility here; perhaps the departments that responded are

---

124. CivicPulse defines a jurisdiction as a county, municipality, or township. For context, "the average local jurisdiction population in the United States is 6,200" people. Wendell Cox, *America Is More Small Town than We Think*, NEW GEOGRAPHY (Sept. 10, 2008), https://www.newgeography.com/content/00242-america-more-small-town-we-think [https://perma.cc/B996-WUUH] (citing data from the 2002 Census of Governments).

125. *See generally* Manes, *supra* note 6.

126. *Law Enforcement Management and Administrative Statistics (LEMAS)*, BUREAU OF JUST. STATS. (May 18, 2009), https://www.bjs.gov/index.cfm?ty=dcdetail&iid=248 [https://perma.cc/X6U4-YBWP].

127. CivicPulse arrived at this estimate using the 2017 American Community Values Survey. We do not offer a comparison of our sample to the general population of local police departments because we do not believe this makes methodological sense. To the extent that we could even agree how to characterize an "average" police department in the U.S., it is unclear what such a description would mean or capture. Instead, we approximate a comparison of our sample with a general population by pointing to the average size of police departments. Beyond department size, it is hard to know the average characteristics of police departments.

128. Our response rate was 0.059 (434 responses from 7339 invited), compared to the average survey response rate of .033. Nigel Lindemann, *What's the Average Survey Response Rate?*, SURVEYANYPLACE BLOG (Aug. 9, 2021), https://surveyanyplace.com/blog/average-survey-response-rate/ [https://perma.cc/6L49-36JW].

different than those that did not. Despite these limitations however, we believe our study significantly adds to the conversation by being the first academic, non-governmental study to quantitatively describe the current state of policing and surveillance. Prior to this study, much of our knowledge on the extent of police surveillance capabilities came from case studies.[129] These examine only one or a few departments at a time. As reviewed in Part I, this case study evidence leaves open many questions. We received responses from hundreds of departments, and the demographics of the jurisdictions policed by those departments (reported in Appendix A) capture a broad cross-section of American communities. We are also unsure whether a privately-run study of law enforcement officials and agencies can expect a high response rate. Unlike the general population, law enforcement officials and agencies, including police departments, are a difficult-to-reach population. With this in mind, our survey response rate is consistent with other studies that have used CivicPulse's data on elected officials.[130]

To promote honest responding, departments were promised anonymity. No incentives were offered, however. Since jurisdiction-level variables could be highly identifiable, this led to the creation of "bins" for each of the key demographic variables. So, as shown below, population was classified as one of three bins (under 2,600 people, between 2,600 and 10,000, and over 10,000 people). Urbanicity was also classified into three bins (0%–12% urban, 12%–96% urban, or more than 96% urban), as was ethnicity (less than 82.7% non-Hispanic White, between 82.7% and 93.7% non-Hispanic White, or more than 93.7% non-Hispanic White). For more details on these classifications, please see Appendix A.

Jurisdiction size is strongly related to other jurisdiction demographics, such as police department size. Jurisdictions with populations of under 2,600 overwhelmingly had departments with under 15 officers, for example. This seems to be consistent with prior findings showing that, even for larger jurisdictions of over 25,000 residents, the median number of police officers is just 15.9 per 10,000 residents.[131] The smaller jurisdictions in our sample—those with fewer than 2,600 people—were also predominantly not

129. *See* sources cited *supra* note 7.

130. *See Academic Papers*, CIVICPULSE, https://www.civicpulse.org/academic-papers [https://perma.cc/Y88R-PQB4] (listing research and academic papers generated with CivicPulse data).

131. *See* Mike Maciag, *Police Employment, Officers Per Capita Rates for U.S. Cities*, GOVERNING (July 2, 2018), https://www.governing.com/archive/police-officers-per-capita-rates-employment-for-city-departments.html [https://perma.cc/U7HQ-EYAF] (reflecting 2016 data).

urban. Of these small jurisdictions, 67.6% fell into our most rural (hence, least urban) bin for the "urbanicity" measure.[132] In contrast, only 4.5% of jurisdictions with populations of over 10,000 fell into the least urban category, while 52.5% of such larger jurisdictions fell into the most urban category. Jurisdiction population was also related to jurisdiction ethnicity. Most (51.5%) of the smallest jurisdictions were in the more than 93.7% non-Hispanic White bin, while only 21.5% of the largest jurisdictions fell into that category. See Appendix A for the full interrelations of jurisdiction demographics.

We began by examining technological capacity generally. Two matrix table questions asked respondents to report which of a variety of technologies and tools were available to their departments.[133] As can be seen in Table 1, almost all departments reported that officers had high-speed internet, access to computers, and the ability to use department software. But even here some differences by jurisdiction size emerge. Fewer departments in the smallest jurisdictions have their own email servers or the ability to store records digitally. They are also less likely to have a designated technology officer. And many departments across all jurisdiction types report not having sufficient funding for their technological needs. This last finding may explain, at least partially, why we see relatively low rates of adoption for some of the most high-tech, and also more expensive, technologies such as facial recognition and Stingrays (see our discussion below for Table 3).

132. "Least urban" (most rural) refers to the <12% category in Appendix A. This measure indicates that less than 12% of a population in a jurisdiction was living in an urban area. See Appendix A for a more detailed breakdown and explanation of how the Census categorizes urban versus rural.

133. Both questions included "None of the above" options, but no participant selected these.

Table 1: Access to Basic Technology

		Jurisdiction Size		
Technology Practice	**Percentage Overall**	Under 2600	2600–10k	Over 10k
All officers have access to computers	99.8%	100.0%	100.0%	99.5%
All officers have access to smart phones	72.9%	76.5%	80.0%	65.8%
Dept. stores records digitally	81.3%	69.1%	83.0%	83.9%
Most of our officers can use our software	91.4%	88.2%	87.9%	95.5%
Most of our officers can do data analysis	26.9%	17.6%	29.1%	28.1%
We have enough funding to buy the technology we need	18.5%	14.7%	14.5%	23.1%
Dept. has agency-wide email server	90.1%	63.2%	92.7%	97.0%
Dept. has high-speed internet	96.8%	92.6%	98.8%	96.5%
Dept. has computerized case management system	90.5%	82.4%	90.3%	93.5%
Dept. has technology officer	34.1%	20.6%	24.7%	46.5%
Dept. has data chief[134]	12.9%	7.4%	7.2%	19.5%
Number of Departments		68	166	200

The remainder of the survey asked about access to and use of surveillance tools, the existence of departmental policies related to surveillance tools, and concerns related to surveillance practices. First, in the same matrix block as the above questions about computer technology access, we asked which of

134. For both the data chief and technology officer questions, respondents could select a "Don't Know" option. One participant did so for data chief, and they are counted as a "No" for this table.

five surveillance technologies the departments "currently use and have access to."

Table 2: Access to and Use of Various Types of Surveillance Equipment

		Jurisdiction Size		
Surveillance Technology	**Percentage Using**	Under 2600	2600–10k	Over 10k
Automatic license plate readers	23.8%	7.4%	15.8%	36.0%
Body cameras	61.0%	70.6%	53.9%	63.5%
Drones to use for general law enforcement purposes	26.8%	4.4%	13.9%	45.0%
Vehicle tracking devices	24.5%	4.4%	15.8%	38.5%
Video surveillance cameras on public ways (e.g., stop lights, parks, public transit, etc.)	32.3%	20.6%	30.9%	37.5%

Two important patterns emerge from this data. First, use of these technologies varies sharply by jurisdiction size. With the single exception of body cameras, all these technologies are more frequently used in larger jurisdictions. Second, again with the exception of body cameras, each of these technologies is used by only a minority of departments. Even automated license plate readers, which are increasingly common among departments with more than 100 officers,[135] are not used by most departments in jurisdictions with over 10,000 residents. Less than 10% of the smallest jurisdictions have these, and less than 5% of those smallest jurisdictions have drones or vehicle tracking devices. We see similar results as automated license plate readers for vehicle tracking/global positioning devices. This is somewhat surprising given prior work suggesting growing use of global positioning systems among both small and large police departments.[136] The major outlier to what Table 2 shows as an overall trend of generally low use is body cameras; we outline possible explanations for this in Part III.

135. Koper & Lum, *supra* note 92, at 306.
136. Hughes & Burton, *supra* note 103, at 536.

Following these questions, the survey continued with three question blocks, each of which asked more detailed questions about a particular technology or surveillance practice.[137] These technologies were facial recognition, cellphone location tracking, and surveillance cameras. We chose these three topics for in-depth analysis because facial recognition has been the subject of frequent public debate in the past year,[138] and the other two technologies were commonly mentioned in our discussions with law enforcement experts. Departments were first asked whether they used each of these technologies. If they did, they were asked how often they did. If they did not, they were asked to select why not from a list of possible reasons. They were also asked whether they had a policy on the use of that technology.

For Facial Recognition, participants were asked "Does your department currently use or have access to facial recognition technology of any kind?"[139] As can be seen in Table 3, use of facial recognition technology was rare: only about 10% of departments reported having it. Each department that reported using the technology was then asked how often they used it for both "emergency" and "investigatory" purposes. Departments generally reported "rare" use of facial recognition technology for investigations and "very rare" use of it in emergency circumstances. Perhaps relevant to the rare emergency use, 0% of departments reported having access to "live" facial recognition technology, which would scan an active camera feed for face matches.[140] This

137. These blocks were presented in a fixed order.

138. *See, e.g.*, Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It and 'Lead to a Dystopian Future*,*'* NEWS 18 (Jan. 19, 2020), https://www.news18.com/news/world/the-secretive-company-that-might-end-privacy-as-we-know-it-and-lead-to-a-dystopian-future-2464201.html [https://perma.cc/6EHW-Q9BS].

139. Departments were invited to name their facial recognition vendor. This question was marked "(optional)" because it was expected that departments might be reluctant to do so. Two departments named JNET, and one each named CLEMIS, FACES, Lumen, and Vigilant Solutions.

140. "An alternative to using facial recognition reactively is to use it live (in real time). This involves a police-operated camera system (e.g., body-worn, red light, public transit, etc.) that actively scans people's faces in public. The live facial recognition system then uses this data and searches for matches against an existing law enforcement database (e.g., outstanding warrants)." (Phrasing of a facial recognition question in our survey).

type of high-end facial recognition has been used by law enforcement in the UK,[141] and employed by some non-law enforcement actors in the U.S.[142]

A follow-up question unique to the facial recognition technology block asked whether respondents were concerned about false matches with facial recognition technology. A minority (37.1%) of respondents said they were not at all concerned, most (57.1%) were somewhat concerned, and few (5.7%) were very concerned.

Table 3: In-Depth Surveillance Questions

		Jurisdiction Size		
Surveillance Technology	**Percentage Using**	Under 2600	2600–10k	Over 10k
Facial Recognition	9.7%	7.4%	9.6%	10.6%
Cell location tracking (provider)	75.3%	59.7%	72.2%	83.7%
Cell simulator (Stingray)	5.7%	3.0%	4.5%	7.7%
Cameras in public spaces (parks, transit)	43.9%	35.4%	39.7%	50.9%
Partnership with Ring	14.4%	6.3%	8.4%	22.9%

For cellphone location technology, respondents were prompted: "Wireless cellphone companies can use the GPS technology built into smartphones and tower signals to track users' movements and locations. Law enforcement officials will sometimes ask companies to disclose the location information of certain individuals. Does your department use cellphone location information?" As can be seen in Table 3, the overwhelming majority of departments do use cellphone location tracking. This usage is highest among large departments (over 80%) but is also extremely common among smaller departments (approximately 60%). This technology is more often used for investigations ("Often" 47.1% of the time) than for emergency situations

141. *Police To Roll Out Live Facial Recognition Cameras in London*, CNBC, (Jan. 24, 2020, 9:03 AM), https://www.cnbc.com/2020/01/24/police-to-roll-out-live-facial-recognition-cameras-in-london.html [https://perma.cc/TR82-RHC2].

142. *See* Tim Simonite & Gregory Barber, *The Delicate Ethics of Using Facial Recognition in Schools*, WIRED (Oct. 17, 2019, 6:00 AM), https://www.wired.com/story/delicate-ethics-facial-recognition-schools/ [https://perma.cc/7F9Q-FLMK]; *Products*, SN TECH, http://www.sntechnologies.ca/product/ [https://perma.cc/B89A-H5VT].

("Often" 26.5% of the time). Nevertheless, use of cellphone location far outpaces use of facial recognition. Also important in this context is the legal difference between investigative and emergency uses. As mentioned above, investigatory use of cellphone location data will often require a warrant, but there are established procedures for its warrantless use in emergency circumstances.[143]

In the cellphone block, participants were also asked whether they had cell simulator technology (Stingray or Triggerfish devices).[144] Use of these devices appeared to be rare in our sample. Less than 10% of even jurisdictions above 10,000 report having them, and only 3% of the smallest jurisdictions report the same.

The final block asked participants about their department's use of surveillance cameras: "Law enforcement departments often place surveillance cameras in any number of public spaces, including streets, parks, and transit systems. Is this something your department does?" More departments responded affirmatively to this question (43.9%) than to the similar one about surveillance cameras reported in Table 2 (32.3%). This may be due to this second question being asked in isolation instead of as part of a block, or to the question's wording.[145] Nevertheless, surveillance cameras are reported as being used by fewer departments than cellphone location data.

As a follow-up to the questions about surveillance cameras, participants were also asked whether their department had a partnership with Ring, the doorbell camera company (Table 3). A small minority of departments (14.4%) reported having such a partnership, with partnerships being more common among larger departments (22.9%).

---

143. *See supra* Section I.A.1 (discussing use of cellphone location information in different situations).

144. "Cell site simulator technologies (e.g., 'stingray' or 'triggerfish' devices) allow law enforcement officials to mimic a cell tower and force nearby cellphones to connect. This allows officials to locate a phone or identify a phone number. Does your department use cell site simulator technologies?" (Phrasing of Stingray question in our survey).

145. In retrospect, it is clear that this question is somewhat suggestively worded ("departments often place") and prompts additional contexts ("transit systems").

Table 4: Surveillance Uses and Policies (Percentages)

		Percent of those using:			Have Policy			
Technology		Never	Rarely	Often	Yes	D/K	In progress	No
Cell location	**For Emergency**	1.0	63.2	35.8	16.5	11.1	10.9	61.5
	For Investigation	1.6	56.7	41.7				
Cell simulator (Stingray)	**For Emergency**	4.3	69.6	26.1				
	For Investigation	8.7	69.6	21.7				
Cameras in public spaces	**For Emergency**	4.1	69.4	26.5	17.0	7.3	10.2	65.5
	For Investigation	0.0	52.9	47.1				
Facial recognition	**For Emergency**	18.4	78.9	2.6	15.8	7.9	18.4	57.9
	For Investigation	7.9	73.7	18.4				

Despite the common use of cellphone location technology, and the occasional use of video cameras and facial recognition, the majority of departments using each did not have policies in place governing use of each. This may be less problematic in the cellphone context, as there are substantial statutory and constitutional restrictions on both cellphone location data and Stingray devices. But camera and facial recognition use are, as noted above,

generally not regulated by the constitution or statute.[146] If departments also do not regulate them by policy, then they exist in a regulatory void. Further, it appears that a meaningful number of police officers are using facial recognition services without the knowledge of even their own departments.[147] Their departments presumably have no policies in place to regulate or advise this unofficial activity.

For each of these key technologies that involved purchasing and procurement, we further asked departments that did not have the technologies why they did not have them (Table 5). The results were fairly consistent across technologies. The two most frequently cited were "never seriously considered it" and "too expensive." Privacy concerns were only cited by approximately 20% of departments across all technologies.

Table 5: Reasons Why Technologies Were Forgone

Rationale	Facial Recognition	Cell Simulator	Surveillance Cameras
Never seriously considered it	49.6%	56.7%	28.5%
Too expensive	55.6%	33.1%	68.4%
The technology is not reliable	0.0%	0.0%	0.0%
Not sure how the technology will benefit the department	24.4%	22.7%	10.4%
Not sure how to get the technology	12.7%	17.0%	0.0%
Privacy concerns	20.3%	15.0%	19.7%
Not enough political support	16.3%	7.9%	20.2%
Other	0.0%	6.8%	0.0%
None of the above	7.0%	9.3%	0.0%
Number selecting any reasons	369	353	193

146. *Supra* Parts I.B.1, I.B.2, I.B.7.

147. Ryan Mac et al., *Surveillance Nation*, BUZZFEED NEWS (Apr. 9, 2021, 7:52 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition [https://perma.cc/XK98-C6EK] (highlighting a recent investigation tracking use of Clearview AI's facial recognition software. The report found that officials within law enforcement agencies often use facial recognition software without prior approval from or knowledge of agency leaders).

Following these questions, the survey asked whether departments were legally prohibited from using a range of surveillance technologies. This question was included to see whether departments felt they were restricted from using facial recognition or automated license plate readers given that, as explained above, these technologies are heavily regulated in some jurisdictions.[148] This question asked about eight different technologies: automatic license plate readers, cellphone location information, drones, facial recognition technology, home security footage acquired from private companies (e.g., Ring), surveillance cameras on public ways, vehicle telematics information, and vehicle tracking devices. Of our sample, 4.8% reported they were prohibited from using vehicle tracking devices. All other respondents selected "None of the above." This suggests that legal prohibitions are sufficiently rare so as to not be detectable in our sample.

III. DISCUSSION

On its own, the existing police and surveillance literature evidence lead one to conclude that most police departments in the United States have access to all kinds of high-tech surveillance gadgets. But our survey results, which allow for a broad look across jurisdictions of differing sizes, show a different picture. In reality, most police departments have few sophisticated surveillance options other than body-worn cameras and cellphone location information. Police departments located in small jurisdictions, in particular, have very little by way of sophisticated surveillance inputs. This suggests that there should be a renewed focus on jurisdiction size in this domain. Further, our results also suggest that political barriers are not the primary factor preventing departments from acquiring these technologies. Rather, the primary barriers our survey participants cited were cost and insufficient funding.[149]

Our results show that larger jurisdictions have a greater range of police surveillance technologies. These results are consistent with prior literature suggesting that larger jurisdictions tend to invest more heavily in surveillance equipment.[150] We should note, however, that our study does not distinguish jurisdiction size at a more granular level. Specifically, we cannot distinguish

148. *See supra* Sections I.B.5, I.B.7 (discussing legal restraints on use of automatic license plate readers and facial recognition).

149. *See supra* Table 5.

150. See our review of existing studies in Part I (emphasizing existing evidence of police surveillance access in larger jurisdictions).

between police departments in large jurisdictions versus the top ten largest jurisdictions.[151] For that, we must look to insights from case studies on police surveillance, such as Sarah Brayne's study of the Los Angeles Police Department's surveillance practices or Catherine Crump's assessment of police surveillance practices in Seattle, Oakland, and San Diego.[152] Nevertheless, our data confirms that, compared to larger jurisdictions, smaller jurisdictions are not subject to the same levels of police surveillance. This finding is important because, to our knowledge, this is the first quantitative evidence of surveillance differences by jurisdiction type.

Though we report our findings by jurisdiction size, this factor is confounded with urbanicity and the ethnicity of the population. The smallest jurisdictions are the whitest and least urban. In Appendix B, we report the equivalent of Tables 2 and 3 using urbanicity and ethnic composition as the independent factor. Those data show very similar patterns to what was observed regarding jurisdiction size. The most urban jurisdictions are more likely to be subject to each kind of surveillance technology than the least urban jurisdictions, excepting only body cameras. The jurisdictions with the greatest proportion of non-Hispanic white residents are in contrast less surveilled by every technology than their counterparts with the smallest proportion of that group.

That the smallest jurisdictions—those with fewer than 2,600 people—are the most likely in our sample to have departments with body cameras is interesting from a policy perspective. These findings provide support for prior work pointing to growing interest in and acquisition of body-camera technology.[153] That smaller jurisdictions have such a high concentration of police departments with body cameras suggests that police budgets are not determinative of certain surveillance capacities. One possible explanation for body cameras as an outlier may lie with federal funding. Despite their smaller budgets, police departments in small jurisdictions may have received federal funding from a 2015 body camera program.[154]

The prevalence of body cameras among small departments also suggests that pressures for greater police transparency and accountability may not be

---

151. This limitation is due to the fact that survey respondents were promised anonymity. More fine-grained population data would make it easier to match responses to individual departments, thereby breaching confidentiality.

152. *See generally* Brayne, *supra* note 7; Crump, *supra* note 7.

153. Joh, *supra* note 26, at 30–31, 33–34. *See generally* St. Louis et al., *supra* note 5, at 308 (discussing the background and developments of body cameras as a tool for police legitimacy).

154. St. Louis et al., *supra* note 5, at 308.

unique to police departments located in larger jurisdictions. As noted earlier, civil rights groups have pushed for departments to adopt and use body cameras as a way of ensuring greater accountability to the public.[155] It may be the case that police departments located in small jurisdictions want body cameras as a means to either preempt legal challenges or to protect their officers through video evidence of an encounter. Whatever the motivation for acquiring the technology, pressure to use body cameras as tools of police transparency appears to be growing. In 2021, Illinois passed a sweeping criminal justice reform bill stipulating that "[a]ll law enforcement agencies must employ the use of officer-worn body cameras."[156]

In addition to body cameras, our survey results suggest that the policing and surveillance conversations need to be focusing more on use of cellphone location tracking and video surveillance. A majority of departments in our sample reported using cellphone location tracking and body cameras, while fewer than 10% reported using Stingrays or facial recognition. In constitutional terms, this would support treating Stingrays and facial recognition as "not in general public use" and therefore presumptively unreasonable without a warrant.[157] We also find reported high use of video surveillance. Consistent with prior findings on police video surveillance, departments located in larger jurisdictions accounted for the highest percent of video surveillance use.[158]

Many factors may discourage police departments from investing in a wider range of technology. In the case of Stingrays, one may be financial. Only 18.5% of police departments reported having sufficient funding for their technology needs,[159] and tools such as Stingray devices are fairly expensive.[160] In contrast, obtaining cellphone location data is free, apart from the necessities of the legal process. For facial recognition, the relatively low access rates we find may have to do with skills and systems gaps within police departments. Only about 12.9% of departments in our sample reported having

---

155. *Id.*

156. H.R. 3653, 101st Gen. Assemb., Reg. Sess. (Ill. 2021) (amending 50 ILL. COMP. STAT. 706/10-15 (2016)).

157. Kyllo v. United States, 533 U.S. 27, 40 (2001).

158. *See generally, e.g.*, Caplan et al., *supra* note 57 (studying police use of video monitoring in Newark, New Jersey); Circo & McGarrell, *supra* note 50 (studying police use of video monitoring in Detroit, Michigan); Lim & Wilcox, *supra* note 49 (studying police use of video monitoring in Cincinnati, Ohio); McLean et al., *supra* note 57 (studying police use of video monitoring in Schenectady, New York).

159. *See supra* Table 1.

160. Zetter, *supra* note 41.

a data chief, and even those departments that do have facial recognition acknowledge that using it effectively is challenging.[161] Departments need people who know how to effectively use and assess the complicated algorithms involved in facial recognition systems. Additionally, the software and technologies that departments buy from private vendors do not easily synch or integrate with departments' existing systems.[162] This might deter departments, especially smaller departments with fewer human and technological resources, from paying for expensive products if there is no guarantee that these products can be easily integrated. More generally, the low access rates for Stingrays and facial recognition may be due in part to real or perceived threats of public backlash. Public distrust of police practices has resulted in some cities banning or restricting police use of surveillance equipment.[163] Fearing similar backlash and restrictions, police departments may be wary to adopt certain surveillance technologies, or, alternatively, may opt to use them without disclosing these practices.[164]

Our finding suggesting high use of cellphone location information among police departments may seem surprising considering the Supreme Court's recent ruling in *Carpenter v. United States*.[165] In *Carpenter*, the Court ruled that, given the highly invasive and personal nature of historical cellphone location data, a government actor seeking long-term cell-site location data from a third-party cellphone provider must, generally, first obtain a warrant.[166] This ruling applies to police who seek to obtain cellphone location records from a private company like Verizon or T-Mobile[167] Despite the Court's clear message that police do not have unlimited or unfettered access to historic cell-site location data,[168] the Court's ruling left open many

161. *See supra* Table 1.

162. With approval from Northwestern University's Institutional Review Board, we conducted an anonymous interview with an official affiliated with Chicago Police Department in 2019. This official noted that one of the biggest challenges the department faces is with seamless integration of vendor products with the department's existing operating systems. Interview with Chi. Police Dep't, in Chi., Ill. (Oct. 2019).

163. *E.g.*, Crump, *supra* note 7, at 1613 (noting that Seattle's city council passed an ordinance requiring city agencies to get approval before purchasing any surveillance equipment).

164. *See* Mac et al., *supra* note 147.

165. 138 S. Ct. 2206 (2018).

166. *Id.* at 2211 (holding that the government must generally obtain a warrant for cell phone location information data, unless an exception applies).

167. *Id.* at 2220.

168. *Id.* at 2221–23 (concluding that because the Government's action constituted a search, the Government needed a warrant to obtain those cellphone records).

questions.[169] Under *Carpenter*, police might bypass the warrant requirement in certain emergency situations, or if they are collecting cell-site information for short periods of time.[170] It also may not be that difficult to get a warrant, as providers report fulfilling tens of thousands of police requests in a year.[171] This may be why our results show such high use of cellphone location surveillance despite *Carpenter*.

The relative rarity of the use of facial recognition is also not a reason to discount concerns over it. First, there is some evidence suggesting that individuals within law enforcement agencies are using facial recognition without the knowledge or approval of their superiors.[172] This would result in undercounting on our survey. Second, a small number of large departments police a huge number of Americans. Though we believe there is value in understanding small-scale policing, it would be a misreading of our results to discount the experiences of those in the largest cities where this form of surveillance may be much more common. Finally, the general lack of policies guiding surveillance use within law enforcement raises concerns at every level of technology deployment. Of those departments reporting having facial recognition, almost 58% said they do not have any policies guiding use of that technology.[173] Privacy scholars and civil rights groups have warned of the privacy risks associated with biometric surveillance[174] for reasons including public mistrust,[175] racially biased engineering,[176] and a high rate of false-positive matches.[177] Given that reliability issues related to facial recognition have yet to be fully addressed and resolved, the lack of departmental guidelines exacerbate potential privacy risks to individuals. Further, there are better and worse ways to use facial recognition. Using a facial recognition match as an investigative lead, requiring external

169. *Id.* at 2220 (noting that the Court's decision does not apply to real-time cellphone location gathering, tower dumps, or conventional modes of surveillance).

170. *See id.* at 2222–23.

171. *See* VERIZON, *supra* note 32.

172. *See* Mac et al., *supra* note 147.

173. *See supra* Table 4.

174. *See, e.g.*, Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 108 (2019); *see also* Crump, *supra* note 7, at 1638; Manes, *supra* note 6, at 506; St. Louis et al., *supra* note 5, at 311; ACLU, COMMUNITY CONTROL OVER POLICE SURVEILLANCE: TECHNOLOGY 101, at 2, 5 (2016), https://www.aclu.org/sites/default/files/field_document/tc2-technology101-primer-v02.pdf [https://perma.cc/7X9F-ZVXU].

175. Kugler, *supra* note 174, at 111–12.

176. ACLU, *supra* note 174, at 5.

177. *Id.*

verification, poses different and lesser problems than using it as an independent basis to make an arrest. Treating potential matches as mere leads is, for instance, Federal Bureau of Investigation policy.[178] The low current usage of facial recognition may highlight an opportunity: the best time for an agency to consider restrictions, like that one, is before a practice becomes firmly entrenched.

One limitation of this study is that it did not ask many questions about backend data processing. There is a vast difference between merely having surveillance cameras and having both the cameras as well as the skills and infrastructure to sort and examine large amounts of video footage at a low cost. Based on the authors' conversations with police officials, we did not expect that many smaller departments would have such sophisticated backend operations. We know that developing an effective RMS (Records Management System) has been a major challenge for one of the largest police departments in the country,[179] and likely others too. That comparatively few departments reported even having designated technology or data officers supports this expectation. Nevertheless, the ability of departments to cheaply and efficiently process the information they collect is likely to be a consideration going forward, especially in the largest jurisdictions, as to whether or not to invest in surveillance technologies.

IV. CONCLUSION

Our results from a 2020 national survey of local police departments in the United States show that police departments located in small jurisdictions have very little by way of surveillance tools compared to those in larger jurisdictions. Moreover, it is not political factors that appear to be the main barriers to enhanced police surveillance capabilities, but rather bureaucratic reasons including cost and funding. Finally, our results show which surveillance technologies have become fully integrated with American policing, particularly use of cellphone location data, and which are still much

178. *Facial Recognition Technology Hearing*, *supra* note 119; *see also* KRISTIN FINKLEA ET AL., CONG. RSCH. SERV., R46586, FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY 4–5 (2020), https://fas.org/sgp/crs/misc/R46586.pdf [https://perma.cc/X8HK-7LNY].

179. *See* Matt Masterson, *Police Department Hasn't Taken Steps To Improve Record Management: Watchdog Report*, WTWW (Sept. 16, 2021, 12:12 PM), https://news.wttw.com/2021/09/16/police-department-hasn-t-taken-steps-improve-record-management-watchdog-report [https://perma.cc/C7F8-LB6L].

more in the early stages of use, particularly Stingray devices and facial recognition We believe that these developing surveillance technologies present an opportunity for early reform and policy intervention.

Appendix A: Jurisdiction Demographics

		Jurisdiction Size		
		Under 2600	2600–10k	Over 10k
Trump Vote Share	<51%	25.0%	42.2%	43.5%
	51-65%	22.1%	32.5%	29.5%
	>65%	52.9%	25.3%	27.0%
Urbanicity	<12%	67.6%	8.4%	4.5%
	12-96%	14.7%	34.3%	43.0%
	>96%	17.6%	57.2%	52.5%
Region	Midwest	39.7%	42.8%	38.5%
	Northeast	14.7%	24.7%	18.0%
	South	33.8%	19.9%	27.0%
	West	11.8%	12.7%	16.5%
Local government spending on policing	>1,340,000	5.9%	42.8%	92.5%
	38,700-1,340,000	89.7%	54.2%	6.5%
	<38,700	4.4%	3.0%	1.0%
College	<17.1%	51.5%	21.7%	20.0%
	17.1-27.4%	32.4%	38.0%	37.5%
	>27.4%	16.2%	40.4%	42.5%
Non-Hispanic White	<82.7%	16.2%	21.7%	34.0%
	82.7-93.7%	32.4%	42.2%	44.5%
	>93.7%	51.5%	36.1%	21.5%
Chief elected	No	91.2%	88.6%	66.0%
	Yes	8.8%	11.4%	34.0%
Dept. size	<15	95.5%	63.9%	5.5%
	15-49	4.5%	35.5%	56.0%
	50-99	0.0%	0.6%	20.5%
	100-199	0.0%	0.0%	12.5%
	200-300	0.0%	0.0%	3.0%
	>300	0.0%	0.0%	2.5%
Total jurisdictions		68	166	200

Note: CivicPulse, the company that conducted the police survey on our behalf, downloaded a set of Census measures used to merge onto the existing police survey dataset. The measures for jurisdiction size, percentage over 25 who completed 4-year college degrees ("College"), and proportion of people identifying as non-minority White ("Non-Hispanic White") were taken from the 2017 American Community Survey.[180] The "Urbanicity" measure was derived using the 2010 Census' classification of urban and rural areas.[181] The measure "local spending on policing" was taken from the U.S. Census of Governments (2017).[182] Number of officers ("Dept. size") and whether the chief was elected ("Chief elected") were both asked as questions in the survey.

180. For the 2017 ACS data, see *American Community Survey (ACS): Data Profiles*, U.S. Census Bureau, https://www.census.gov/acs/www/data/data-tables-and-tools/data-profiles/2017/ (last visited Feb. 24, 2022).

181. *2010 Census Urban and Rural Classification and Urban Area Criteria*, U.S. CENSUS BUREAU (Oct. 8, 2021), https://www.census.gov/programs-surveys/geography/guidance/geo-areas/urban-rural/2010-urban-rural.html [https://perma.cc/JR7M-VM88].

182. For data on local spending on policing, see *2017 State & Local Government Finance Historical Datasets and Tables*, U.S. Census Bureau (Oct. 8, 2021), https://www.census.gov/data/datasets/2017/econ/local/public-use-datasets.html [https://perma.cc/6XVN-7F9Z].

Appendix B: Urbanicity and Ethnicity Related to Surveillance Technology

Technology	**Urbanicity**		
	<12%	12-96%	>96%
Automatic license plate readers	2.9%	14.4%	37.4%
Body cameras	72.5%	61.4%	56.9%
Drones to use for general law enforcement purposes	11.6%	32.0%	28.0%
Vehicle tracking devices	7.2%	22.2%	31.8%
Video surveillance cameras on public ways (e.g., stop lights, parks, public transit, etc.)	20.3%	22.9%	43.1%
Facial Recognition	4.4%	2.6%	16.5%
Cell location tracking (provider)	69.1%	77.4%	75.9%
Cell simulator (stingray)	2.9%	2.8%	8.8%
Cameras in public spaces (parks, transit)	29.9%	36.4%	54.6%
Partnership with Ring	6.2%	9.6%	20.9%

Technology	**Non-Hispanic-White**		
	<82.7%	82.7-93.7%	>93.7%
Automatic license plate readers	34.8%	27.6%	9.5%
Body cameras	73.0%	58.0%	54.7%
Drones to use for general law enforcement purposes	33.0%	28.2%	19.7%
Vehicle tracking devices	27.0%	27.6%	18.2%
Video surveillance cameras on public ways (e.g., stop lights, parks, public transit, etc.)	40.0%	33.1%	24.8%
Facial Recognition	12.2%	10.5%	6.6%
Cell location tracking (provider)	74.0%	77.2%	73.9%
Cell simulator (stingray)	8.7%	6.5%	2.3%
Cameras in public spaces (parks, transit)	52.0%	46.4%	34.4%
Partnership with Ring	21.9%	16.8%	5.6%