

# THE UNDUE INFLUENCE OF SURVEILLANCE TECHNOLOGY COMPANIES ON POLICING

ELIZABETH E. JOH\*

*Conventional wisdom assumes that the police are in control of their investigative tools. But with surveillance technologies, this is not always the case. Increasingly, police departments are consumers of surveillance technologies that are created, sold, and controlled by private companies. These surveillance technology companies exercise an undue influence over the police today in ways that aren't widely acknowledged, but that have enormous consequences for civil liberties and police oversight. Three seemingly unrelated examples—stingray cellphone surveillance, body cameras, and big data software—demonstrate varieties of this undue influence. The companies which provide these technologies act out of private self-interest, but their decisions have considerable public impact. The harms of this private influence include the distortion of Fourth Amendment law, the undermining of accountability by design, and the erosion of transparency norms. This Essay demonstrates the increasing degree to which surveillance technology vendors can guide, shape, and limit policing in ways that are not widely recognized. Any vision of increased police accountability today cannot be complete without consideration of the role surveillance technology companies play.*

INTRODUCTION.....	102
I. EXAMPLES OF UNDUE INFLUENCE.....	104
A. <i>Stingray Cellphone Surveillance and Nondisclosure Agreements</i> .....	104
1. <i>Nondisclosure Agreements</i> .....	105
2. <i>Stingrays and the Fourth Amendment</i> .....	108
3. <i>Secret Stingray Use</i> .....	111
B. <i>Cornering the Market on Police Body Cameras</i> .....	112
1. <i>When Product Design Is Policy</i> .....	113
2. <i>Market Dominance</i> .....	114
C. <i>Big Data Software and Proprietary Information</i> .....	117
II. THE HARMS OF UNDUE INFLUENCE.....	120
A. <i>Fourth Amendment Distortion</i> .....	120
B. <i>Accountability by Design</i> .....	123
C. <i>Outsourcing Suspicion and Obscuring Transparency</i> .....	125
III. MINIMIZING UNDUE INFLUENCE.....	126

---

\* Copyright © 2017 by Elizabeth E. Joh, Professor of Law, U.C. Davis School of Law. Thanks to Kyle Edgerton, Barry Friedman, Jonathan Mayer, Bryce Newell, Charles Reichmann, Andrew Selbst, Nate Freed Wessler, participants in the 2017 Privacy Law Scholars Conference workshop, and the librarians of the Mabie Law Library. Thanks also to the U.C. Davis School of Law for research and institutional support and to the staff of the *New York University Law Review* for their fine editorial work.

A. <i>Local Surveillance Oversight</i> .....	127
B. <i>Public Records Requests as Oversight</i> .....	128
CONCLUSION .....	129

## INTRODUCTION

Conventional wisdom assumes that police are in charge of their investigative tools. However, the fact that police are now consumers of new surveillance technologies created and sold by private companies calls this assumption into question.<sup>1</sup> Through different mechanisms intended to promote their own interests and profits, these companies exert control over the police long after their products have been adopted. Private surveillance technology companies wield an undue influence over public police today in ways that aren't widely acknowledged, but have enormous consequences for civil liberties and police oversight.

This undue influence can take many forms. The police may be prevented by contract from disclosing information they are supposed to and otherwise would disclose to criminal defendants, judges, journalists, and the public. In addition, a monopoly (or near monopoly) in the market for a particular technology means that a local police department often must accept the design choices and costs of a single company when it acquires and uses a surveillance product. Finally, aggressive assertions of secrecy about proprietary information may mean that the press, the courts, and the public have no access to the technology shaping substantive decisions about who should be subjected to police attention.

The relationships between surveillance technology vendors and police departments show the increasing degree to which private companies can guide, shape, and limit what the public police do. That police rely on private vendors is unremarkable as a general proposition. The police, like other complex organizations, necessarily rely on vendors for everything from uniforms to bulletproof vests. This consumer-vendor relationship, however, poses greater concerns when the product itself is central to the development of the governmental suspicion that underlies so many enforcement decisions. While scholars have recognized the role of federal funding in local police surveillance programs,<sup>2</sup> the role of private

---

<sup>1</sup> Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 38 (2016) (“[B]ig data tools are often private market products; police departments are just another group of customers.”).

<sup>2</sup> See, e.g., Rachel A. Harmon, *Federal Programs and the Real Costs of Policing*, 90 N.Y.U. L. REV. 870, 872 (2015) (observing that federal funding for local policing “is far more extensive than its civil rights enforcement and has an enormous and understudied impact on policing”); see also Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1598 (2016) (arguing that federal funding of surveillance technologies can “short-circuit” involvement of local officials).

technology vendors has gone largely unnoticed. Yet any vision of increased police accountability today cannot be complete without consideration of the role the surveillance technology produced by these companies plays in policing, and whether the policing decisions embedded in such technology are also subject to public accountability.

The typical approach to the use of new police technologies involves the oversight of courts, legislatures, and local government bodies through judicial opinions, statutes, and local ordinances. The Supreme Court has weighed in, for example, on the police use of manned overhead surveillance,<sup>3</sup> thermal imaging devices,<sup>4</sup> and GPS trackers.<sup>5</sup> Congress and state legislatures have created legal standards for investigative techniques like electronic eavesdropping.<sup>6</sup> Cities and counties can oversee local law enforcement agencies through budgetary decisions.<sup>7</sup> When private companies influence policing through their role as vendors, however, the usual mechanisms of oversight do not easily apply; they have little obligation to permit public access, and the usual constitutional constraints over the police do not regulate them at all.<sup>8</sup>

In this Essay, I identify three recent examples in which surveillance technology companies have exercised undue influence over policing: stingray cellphone surveillance, body cameras, and big data programs. By undue influence I mean the commercial self-interest of surveillance technology vendors that overrides principles of accountability and transparency normally governing the police. I then examine the harms that ensue when this influence goes unchecked, and suggest some means by which oversight can be imposed on these relationships.

<sup>3</sup> Florida v. Riley, 488 U.S. 445 (1989).

<sup>4</sup> Kyllo v. United States, 533 U.S. 27 (2001).

<sup>5</sup> United States v. Jones, 565 U.S. 400 (2012).

<sup>6</sup> See, e.g., GINA STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., R98-326, PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 1–2 (2012), <https://fas.org/sgp/crs/intel/98-326.pdf>; KRISTEN RASMUSSEN ET AL., REPORTERS COMM. FOR FREEDOM OF THE PRESS, REPORTER'S RECORDING GUIDE: A STATE-BY-STATE GUIDE TO TAPING PHONE CALLS AND IN-PERSON CONVERSATIONS 2 (2012), <http://www.rcfp.org/rcfp/orders/docs/RECORDING.pdf>.

<sup>7</sup> See, e.g., JOE DEVRIES, AGENDA REPORT ON SURVEILLANCE ORDINANCE FOR CITY OF OAKLAND, CALIFORNIA 2 (Apr. 17, 2017), <https://oakland.legistar.com/View.ashx?M=F&ID=5137099&GUID=E2F31ED8-CC84-4540-9C16-2B6E84DB73BD> (proposing requirement of city council approval before any city entity acceptance of funds, acquisition, use, or contract regarding new surveillance technologies); see also ACLU, *An Act to Promote Transparency and Protect Civil Rights and Civil Liberties with Respect to Surveillance Technology* (Jan. 2017), <https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf> (requiring any “municipal entity” to obtain city approval before seeking, acquiring, or borrowing new surveillance technology).

<sup>8</sup> See *infra* Section II.

## I

## EXAMPLES OF UNDUE INFLUENCE

*A. Stingray Cellphone Surveillance and Nondisclosure Agreements*

Stingrays, as they are commonly known, refer to cell-site simulators,<sup>9</sup> a type of surveillance equipment that had been used by dozens of police departments—until recently—with little public knowledge. The secrecy surrounding police use of stingrays is attributable largely to the Harris Corporation. Harris dominates the market for stingrays used by the police, so much so that one of its products, the Stingray, has become eponymous with the technology itself.<sup>10</sup>

Stingray devices work by behaving as fake cellphone towers.<sup>11</sup> About the size of a suitcase, the devices are mobile and can be operated from a police car, carried by hand, or even mounted on airplanes.<sup>12</sup> Stingrays collect information by exploiting cellphone vulnerabilities. Cellphones send out signals seeking the closest cell site—usually located on a tower—approximately every seven seconds, whether the user is making a call or not.<sup>13</sup> Because a stingray mimics a legitimate cellphone tower antenna, it forces all nearby phones within its range to provide it with identifying information.<sup>14</sup> Depending on the individual model, a stingray device can

---

<sup>9</sup> They are also called International Mobile Subscriber Identity (IMSI) catchers. See, e.g., Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED (Apr. 9, 2013, 6:30 AM), <https://www.wired.com/2013/04/verizon-rigmaiden-aircard/>.

<sup>10</sup> Harris is also the manufacturer of other cell-site simulator models like TriggerFish, KingFish, and Hailstorm, but the term “stingray” has become a standard term in journalism and scholarship. See Ryan Gallagher, *Meet the Machines That Steal Your Phone’s Data*, ARS TECHNICA (Sept. 25, 2013, 1:00 PM), <https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/>.

<sup>11</sup> See, e.g., Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, WIRED (Mar. 1, 2015, 4:55 PM), <https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/> (“Stingrays are mobile surveillance systems the size of a small briefcase that impersonate a legitimate cell phone tower in order to trick mobile phones and other mobile devices in their vicinity into connecting to them and revealing their unique ID and location.”). Stingrays can be used either to identify 1) the hardware numbers of cellphones in a particular location or 2) the precise location of a cellphone associated with a number the police already know. See Jennifer Valentino-Devries, *How ‘Stingray’ Devices Work*, WALL ST. J.: DIGITS (Sept. 21, 2011, 10:33 PM), <http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/>.

<sup>12</sup> See Devlin Barrett, *Americans’ Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014, 8:22 PM), <https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533> (describing stingrays as small devices with the capability to gather data from tens of thousands of cellphones from an airplane).

<sup>13</sup> See Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 188–90 (2014) (describing cellular technology).

<sup>14</sup> See Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH 134, 145–46 (2014)

identify in real time all nearby phones, pinpoint their location with a high degree of accuracy, and even block service to nearby devices.<sup>15</sup> In cases where stingray use has been revealed, the police have sought either the unique serial numbers associated with all of the cellphones in a particular location, or the location of a phone whose serial number the officers already knew.<sup>16</sup>

These cases of cellphone surveillance are different from instances in which the police have asked wireless carriers like Sprint or Verizon for an individual's historical cell site information. In recent appellate decisions like *United States v. Graham* and *United States v. Davis*, the police sought historical records from cellphone service providers about the connections—sometimes thousands of data points—individual subscribers had made with cellphone towers. In those cases, courts—relying on the Fourth Amendment's third-party doctrine—have largely ruled in favor of the government's ability to request that information without a warrant.<sup>17</sup> By contrast, a stingray device allows the police to collect real time, not historical, cell-site location information on their own, without relying on help from wireless carrier companies.<sup>18</sup>

### 1. Nondisclosure Agreements

Dozens of local police departments as well as the FBI have drawn criticism because of the intense secrecy surrounding their use of stingrays.<sup>19</sup> Beginning in 2011, journalists, civil liberties groups, and defense attorneys uncovered numerous examples in which police departments in the United States used stingray devices in criminal investigations.<sup>20</sup> In many cases, no

(describing operation of a stingray and its capabilities).

<sup>15</sup> Zetter, *supra* note 11.

<sup>16</sup> Valentino-Devries, *supra* note 11.

<sup>17</sup> See *United States v. Graham*, 824 F.3d 421, 424 (4th Cir. 2016) (“Government’s acquisition of historical [data] from Defendants’ cell phone provider did not violate the Fourth Amendment.”); *United States v. Davis*, 785 F.3d 498, 518 (11th Cir. 2015) (“[G]overnment access to MetroPCS’s records comports with applicable Fourth Amendment principles . . .”). On June 5, 2017, the U.S. Supreme Court granted certiorari in *United States v. Carpenter*, a case raising the question of whether warrants are required for the collection of historical cell phone location information. 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017); Adam Liptak, *Justices Act on Voting Rights and Cellphone Privacy*, N.Y. TIMES (June 5, 2017), <https://nyti.ms/2rLnNJL> (noting that “the justices agreed to decide a major case on the privacy of cellphone records”).

<sup>18</sup> The police use of historical cell site location information has been subjected to a number of challenges. See *infra* Section I.A.2.

<sup>19</sup> Stingrays have also been reportedly used by law enforcement agencies outside the United States. See, e.g., Ashifa Kassam, *Vancouver Police Confirm Use of ‘Stingray’ Surveillance Technology*, GUARDIAN (Aug. 10, 2016, 5:05 PM), <https://www.theguardian.com/world/2016/aug/10/vancouver-police-confirm-stingray-surveillance-technology>.

<sup>20</sup> See Jennifer Valentino-DeVries, “Stingray” Phone Tracker Fuels Constitutional Clash,

one outside of the police departments involved was officially notified that the police were intercepting information with stingrays.<sup>21</sup>

The Harris Corporation, the primary manufacturer of stingray devices,<sup>22</sup> has played a large role in this secrecy. In order to provide its stingray devices to local police departments, Harris needed regulatory approval of its products from the Federal Communications Commission (FCC).<sup>23</sup> When Harris applied to the FCC for certification of its stingray devices in 2010, it requested that all information about stingrays be treated “as confidential and be withheld from public inspection.”<sup>24</sup> To justify its request for confidentiality, Harris cited both its need to protect its proprietary information from competitors, and the alleged need to prevent criminals from learning about and circumventing law enforcement surveillance technology.<sup>25</sup> The FCC ultimately granted two specific conditions requested by Harris for its equipment authorization grant:

1) “The marketing and sale of these devices shall be limited to federal, state, local public safety and law enforcement officials only;” and

2) “State and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization.”<sup>26</sup>

In practice, these conditions have meant that local law enforcement agencies must abide by nondisclosure agreements, often overseen by the FBI, to use or acquire stingray equipment.<sup>27</sup> The results of numerous public records requests filed by journalists and others confirm that police departments around the country have entered into similarly worded

---

WALL ST. J. (Sept. 22, 2011) (describing stingray as “one of several *new* technologies used by law enforcement to track people’s locations, often without a search warrant”) (emphasis added).

<sup>21</sup> See *infra* Section I.A.3.

<sup>22</sup> See Valentino-DeVries, *supra* note 20 (noting that the “best known stingray maker is Florida-based defense contractor Harris Corp”).

<sup>23</sup> See Robert Patrick, *Controversial Secret Phone Tracker Figured in Dropped St. Louis Case*, ST. LOUIS POST-DISPATCH (Apr. 19, 2015), [http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article\\_fbb82630-aa7f-5200-b221-a7f90252b2d0.html](http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html).

<sup>24</sup> Letter from Tania W. Hanna, Dir., Gov’t Relations, Harris Corp. & Evan S. Morris, Legal Analyst, Gov’t Relations, Harris Corp., to Marlene H. Dortch, Sec’y, FCC 4 (Oct. 12, 2010), [https://d3gn0r3afghp.cloudfront.net/foia\\_files/10-8-14\\_MR13549\\_RES\\_ID2014-668.pdf](https://d3gn0r3afghp.cloudfront.net/foia_files/10-8-14_MR13549_RES_ID2014-668.pdf).

<sup>25</sup> *Id.* at 2–3.

<sup>26</sup> FCC, Certification of Grant of Equipment Authorization to Harris Corp. (Mar. 2, 2012), <http://bit.ly/2suz6nq>.

<sup>27</sup> See, e.g., Timothy Williams, *Covert Electronic Surveillance Prompts Calls for Transparency*, N.Y. TIMES (Sept. 28, 2015), <https://www.nytimes.com/2015/09/29/us/stingray-covert-electronic-surveillance-prompts-calls-for-transparency.html> (“The F.B.I., which helps manage the distribution of the devices to police departments, requires agencies to sign nondisclosure agreements prohibiting them from discussing their use of the technology.”). In other cases, Harris has required nondisclosure agreements directly from local law enforcement agencies before permitting them to use their equipment. See, e.g., *infra* notes 30–31 and accompanying text.

nondisclosure agreements about stingrays.<sup>28</sup>

These nondisclosure agreements impose strict conditions of secrecy on law enforcement agencies that intend to use stingrays.<sup>29</sup> For example, the nondisclosure agreement agreed to by the Baltimore Police Department in 2011 to use a Harris Stingray imposed the following conditions:<sup>30</sup>

An agreement not to “distribute, disseminate, or otherwise disclose any information” regarding stingray technology “without the prior written approval of the FBI.”

An agreement not to, “in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology” without “prior written approval of the FBI.”

An agreement to, “at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation” stingray technology.

Similarly, in the 2010 nondisclosure agreement the city of Tucson, Arizona, signed with Harris, the city agreed not to “discuss, publish, release or disclose any information pertaining [to stingrays] . . . without the prior written consent of Harris.”<sup>31</sup> The nondisclosure agreements of Tucson and Baltimore are representative of others entered into by police departments around the country.<sup>32</sup>

Requests by courts and journalists to determine whether police departments have acquired or used stingray technology have frequently met resistance from police departments relying on the terms of these nondisclosure agreements. For instance, police investigating a 2013 string of robberies in St. Louis identified three suspects by locating a victim’s

---

<sup>28</sup> See, e.g., *Non-Disclosure Agreements Between FBI and Local Law Enforcement for StingRay*, CTR. FOR HUM. RTS. & PRIVACY, <https://www.cehrp.org/non-disclosure-agreements-between-fbi-and-local-law-enforcement/> (last visited June 5, 2017) (collecting various stingray nondisclosure agreements); JPat Brown & Shawn Musgrave, *The Spy in Your Pocket*, MUCKROCK, <https://www.muckrock.com/project/the-spy-in-your-pocket-14/> (last visited June 4, 2017) (same).

<sup>29</sup> See Robert Patrick, *St. Louis Police: We Track Cellphones, But Won’t Tell You How*, ST. LOUIS POST-DISPATCH (May 25, 2015), [http://www.stltoday.com/news/local/crime-and-courts/st-louis-police-we-track-cellphones-but-won-t-tell/article\\_8041339d-e80d-558f-9bc7-46ba943391eb.html](http://www.stltoday.com/news/local/crime-and-courts/st-louis-police-we-track-cellphones-but-won-t-tell/article_8041339d-e80d-558f-9bc7-46ba943391eb.html) (stating that the strict secrecy of the nondisclosure agreements has led to prosecutors dropping cases rather than explaining how stingrays were used).

<sup>30</sup> Letter from Ernest Reith, Acting Assistant Dir., FBI, to Frederick H. Bealefeld, III, Police Comm’r, Balt. Police Dep’t, & Gregg L. Bernstein, Esq., State’s Att’y, Office of the State’s Att’y for Balt. City (July 13, 2011), available at <http://www.baltimoresun.com/bal-police-stingray-nondisclosure-agreement-20150408-htlmlstory.html>.

<sup>31</sup> Kim Zetter, *Police Contract with Spy Tool Maker Prohibits Talking About Device’s Use*, WIRED (Mar. 4, 2014, 4:34 PM), <https://www.wired.com/2014/03/harris-stingray-nda/> (quoting Tucson-Harris nondisclosure agreement).

<sup>32</sup> See *supra* note 28 (collecting examples).

cellphone in a motel room.<sup>33</sup> One defense attorney noted that the police report in the case referred only to a “proven law enforcement technique” that had located the precise location of the phone.<sup>34</sup> One day before a police intelligence officer was scheduled to be deposed about the department’s stingray use, the pending criminal charges against the robbery defendants were dismissed.<sup>35</sup> While the prosecutors in the case denied any connection between the dismissal of charges and the potential disclosure of information, a police detective had stated in a prior deposition that he could not comment upon any possible stingray use in the case because of an existing nondisclosure agreement.<sup>36</sup> Similar stories about dropped charges have been reported in Baltimore and in other cities.<sup>37</sup>

## 2. *Stingrays and the Fourth Amendment*

Defense attorneys, civil liberties groups, journalists, and, most recently, judges have expressed alarm at this secrecy because stingray devices could be considered searches under the Fourth Amendment. If so, warrantless use of stingrays could constitute a violation of the Fourth Amendment. Whether or not the government engages in a Fourth Amendment search depends on the interference with a person’s reasonable expectation of privacy.<sup>38</sup>

Police use of stingray devices to locate cellphones (and their owners) might implicate Fourth Amendment interests in at least two ways. First, if a surveillance technology permits the police to obtain information they otherwise would not be able to collect without physical intrusion into a space protected by the Fourth Amendment, then the use of that technology is generally considered a search. For instance, in *Kyllo v. United States*, the U.S. Supreme Court considered whether police use of a thermal imaging device used to determine whether Danny Kyllo’s home was emitting an unusually high amount of heat suggestive of illegal marijuana cultivation violated the Fourth Amendment.<sup>39</sup> Noting that the thermal imaging device obtained information that would otherwise have been obtained only by a

---

<sup>33</sup> Robert Patrick, *St. Charles Woman Withdraws Guilty Plea in Case Linked to Secret FBI Cellphone Tracker*, ST. LOUIS POST-DISPATCH (Apr. 27, 2015), [http://www.stltoday.com/news/local/crime-and-courts/st-charles-woman-withdraws-guilty-plea-in-case-linked-to/article\\_70d5ae28-e819-59d8-a391-78fdd4602d9f.html](http://www.stltoday.com/news/local/crime-and-courts/st-charles-woman-withdraws-guilty-plea-in-case-linked-to/article_70d5ae28-e819-59d8-a391-78fdd4602d9f.html).

<sup>34</sup> *Id.*

<sup>35</sup> When charges were dropped against her three co-defendants, Wilqueda Lillard withdrew her guilty plea on the basis that the use of stingray surveillance had not been disclosed in her case. Prosecutors dismissed the case. *Id.*

<sup>36</sup> *See id.*; Patrick, *supra* note 29.

<sup>37</sup> *See infra* Section II.A for examples.

<sup>38</sup> *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (establishing reasonable expectation of privacy test).

<sup>39</sup> 533 U.S. 27, 29 (2001).



physical entry of a home, the Court held that the warrantless use of such a device violated *Kyllo's* Fourth Amendment rights.<sup>40</sup> Similarly, police use of a stingray device aimed at a home or apartment building in order to determine whether a particular user's cellphone (and the user) was inside may be a Fourth Amendment search requiring a warrant and probable cause.

Second, the use of a device to force a person's cellphone to provide the police with precise locational data—in some cases within two meters of the cellphone—echoes similar legal debates about whether the Fourth Amendment governs the government's collection of vast amounts of locational data, even in public spaces. That issue was raised, but not decided, in the U.S. Supreme Court's 2012 decision in *Jones v. United States*. In *Jones*, the Court considered whether the government's warrantless collection of twenty-eight days' worth of GPS locational data amounted to a Fourth Amendment search.<sup>41</sup> The majority in *Jones* concluded that it did, but reached this conclusion in a way that did not directly address the collection of the data itself. Rather, the majority focused on the warrantless physical installation of the GPS receiver on the defendant's car and found that this interference with Jones's property rights amounted to a Fourth Amendment search.<sup>42</sup>

Five justices, however, in concurring opinions, seem to have approved of what has sometimes been called the "mosaic theory" of the Fourth Amendment.<sup>43</sup> The mosaic theory argues that while any one governmental act of information collection may not be a search under the Fourth Amendment, the totality of these actions might be. Thus, while the observation of a single trip may not be regulated by the Fourth Amendment, prolonged government observation of a person's movements would reveal much more information about a person and ought to be considered a search. The D.C. Circuit, in deciding Jones's case before it reached the Supreme Court, explicitly embraced the mosaic theory in holding the GPS monitoring was a search.<sup>44</sup>

---

<sup>40</sup> *Id.* at 40 (holding that when the Government uses a device to explore details of a home that are otherwise unknowable in the absence of physical intrusion, the surveillance constitutes a search); *see also* *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of a beeper taken into a private residence was a Fourth Amendment search).

<sup>41</sup> 565 U.S. 400, 402–03 (2012).

<sup>42</sup> *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.'").

<sup>43</sup> *See*, Orin Kerr, *What's the Status of the Mosaic Theory After Jones?*, VOLOKH CONSPIRACY, (Jan. 23, 2012, 1:59 PM), <http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/> ("And perhaps the most fascinating aspect of the *Jones* opinions is that there appears to be a majority ready to embrace the mosaic theory, at least in some form.")

<sup>44</sup> *See* *United States v. Maynard*, 615 F.3d 544, 558 (D.C. Cir. 2010), *rev'd sub nom.* *United States v. Jones*, 565 U.S. 400 (2012) ("[T]he whole of one's movements is not exposed

Justice Alito's concurring opinion in *Jones*, joined by Justices Ginsburg, Breyer, and Kagan, does not refer explicitly to the mosaic theory, but it does state that "use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."<sup>45</sup> Justice Sotomayor, in a separate concurrence, agreed that Jones's case could be resolved by the majority's trespass-based focus, yet she also agreed with Justice Alito that "at the very least" long term GPS monitoring would impinge on reasonable expectations of privacy.<sup>46</sup> Justice Sotomayor went on to explain that she would "take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements."<sup>47</sup>

Similar concerns about how to view the aggregation of data collected by the government have been raised in cases of historical cell-site location data.<sup>48</sup> In these cases, the government, in trying to trace a person's whereabouts, has obtained from wireless carrier companies the information that shows where and when the person's cellphone was in contact with cellphone tower antennae. The resulting data constitutes a time machine of sorts that traces the person's location over a period of time. From the government's perspective, the Fourth Amendment's third-party doctrine provides no Fourth Amendment protection to such data held by wireless carriers;<sup>49</sup> the only legal requirement is a showing that the data would be "relevant" under the Federal Stored Communications Act.<sup>50</sup>

---

*constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts."

<sup>45</sup> 565 U.S. at 430 (Alito, J., concurring).

<sup>46</sup> *Id.* at 415 (Sotomayor, J., concurring).

<sup>47</sup> *Id.* at 416 (Sotomayor, J., concurring).

<sup>48</sup> See, e.g., *United States v. Graham*, 824 F.3d 421, 447 (4th Cir. 2016) (Wynn, J., dissenting in part and concurring in the judgment) ("And in my view, the sheer volume of data the government acquired here decides this case."); *United States v. Davis*, 785 F.3d 498, 533 (11th Cir. 2015) (Martin, J., dissenting) ("The judiciary must not allow the ubiquity of technology—which threatens to cause greater and greater intrusions into our private lives—to erode our constitutional protections."); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 164 (2012) ("[S]ome judges who have considered cases involving law enforcement access to location data posit that the persistent gaze of government may itself represent an objective harm to the public.").

<sup>49</sup> See *Graham*, 824 F.3d 421 (holding that the government's use of historical cell-site location information without a warrant did not violate the Fourth Amendment). Notably, however, Justice Sotomayor's concurrence in *United States v. Jones* called for a reexamination of the third-party doctrine. See 565 U.S. at 416 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."). On June 5, 2017, the Supreme Court granted certiorari in *Carpenter v. United States*, a case raising the question of whether warrants are required for the collection of historical cell phone location information. 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017); Liptak, *supra* note 17.

<sup>50</sup> 18 U.S.C. § 2703(d) (2012).

### 3. *Secret Stingray Use*

Whether or not police use of stingrays are Fourth Amendment searches requiring warrants and probable cause is impossible to determine if judges and defense attorneys are unaware of their use. In many criminal proceedings in which stingray use was suspected or later confirmed, police did not seek warrants for their use.<sup>51</sup> In some cases, police applied for a pen register order, without disclosing that the police had used a stingray device.<sup>52</sup> Orders granted under the Federal Pen Register Act are not warrants. Under that law, a court “shall” grant an application for an order if the government has demonstrated that “the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”<sup>53</sup>

In at least one other instance, police maintained secrecy about stingray use through misleading description. In 2014, the American Civil Liberties Union (ACLU) of Florida uncovered an email exchange between two local police departments suggesting a policy of describing stingrays as confidential informants. An exchange between the Sarasota and North Point, Florida, police departments showed that the departments had borrowed a stingray device from the U.S. Marshals Service, which requested secrecy about the use of the device. The email instructed that in reports, “we simply refer to the assistance as ‘received information from a confidential source regarding the location of the suspect.’”<sup>54</sup>

At the federal level, widespread attention and criticism of stingray secrecy ultimately resulted in a change in FBI policy. In September 2015, the Department of Justice announced new guidelines for FBI use of stingrays.<sup>55</sup> The guidelines specify that law enforcement agencies must seek a warrant based upon probable cause as required by Rule 41 of the Federal Rules of Procedure, with exceptions for exigent circumstances where seeking a warrant is not practicable.<sup>56</sup> The policy also applies in

---

<sup>51</sup> See, e.g., *Thomas v. State*, 127 So. 3d 658, 660 (Fla. Dist. Ct. App. 2013) (observing that the police “did not want to obtain a search warrant because they did not want to reveal information about the technology they used to track the cell phone signal”).

<sup>52</sup> See, for example, *infra* Section II.A for a discussion of *State v. Andrews*, 134 A.3d 324 (Md. Ct. Spec. App. 2016).

<sup>53</sup> 18 U.S.C. § 3123(a) (2012).

<sup>54</sup> Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, ACLU (June 19, 2014), <https://www.aclu.org/blog/internal-police-emails-show-efforts-hide-use-cell-phone-tracking>.

<sup>55</sup> See Kim Zetter, *The Feds Need a Warrant to Spy with Stingrays from Now On*, WIRED (Sept. 3, 2015, 5:31 PM), <https://www.wired.com/2015/09/feds-need-warrant-spy-stingrays-now/> (“The new policy forces prosecutors and investigators not only to obtain a warrant but also to disclose to judges that the specific technology they plan to use is a stingray, as opposed to another surveillance tool.”).

<sup>56</sup> Press Release, Office of Pub. Affairs, U.S. Dep’t of Justice, Justice Department

circumstances where the Department uses stingrays “in support of other Federal agencies and/or State and Local law enforcement agencies.”<sup>57</sup> Several states also have proposed bills requiring warrants for police stingray use, while others, including California, Virginia, Minnesota, Washington, and Utah, have already enacted such laws.<sup>58</sup>

### B. *Cornering the Market on Police Body Cameras*

As consumers of surveillance products, police departments choose from what the market has to offer. When one or two companies dominate a surveillance technology market, their product-design choices can determine how police departments use the technology.

Body cameras are a perfect example. When the 2014 fatal shooting of an unarmed African-American teenager by a police officer in Ferguson, Missouri, drew widespread protests and nationwide attention to fatal encounters with the police, public attention focused on the use of police body cameras as a means of promoting police accountability.<sup>59</sup> After a grand jury declined to indict officer Darren Wilson for Michael Brown’s death, Brown’s family called for “every police officer working the streets in this country” to wear a body camera.<sup>60</sup>

While body cameras had been used by some departments prior to 2014,<sup>61</sup> police departments around the country struggling to respond to concerns about transparency and accountability rushed to purchase them

---

Announces Enhanced Policy for Use of Cell-Site Simulators (Sept. 3, 2015), <https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators>.

<sup>57</sup> *Id.*

<sup>58</sup> See Cyrus Farivar, *California Cops, Want to Use a Stingray? Get a Warrant, Governor Says*, ARS TECHNICA (Oct. 8, 2015, 7:32 PM), <https://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/>; Erin Kelly, *Bipartisan Bill Seeks Warrants for Police Use of ‘Stingray’ Cell Trackers*, USA TODAY (Feb. 15, 2017, 4:08 PM), <http://www.usatoday.com/story/news/politics/onpolitics/2017/02/15/bipartisan-bill-seeks-warrants-police-use-stingray-cell-trackers/97954214/> (referring to congressional proposals of Geolocation Privacy and Surveillance (GPS) Act which “would require a warrant for all domestic law enforcement agencies to track the location and movements of individual Americans . . . without their knowledge”).

<sup>59</sup> See, e.g., Zusha Elinson, *Post-Ferguson Legislative Push Mostly Fizzled*, WALL ST. J. (Aug. 6, 2016, 5:30 AM), <http://www.wsj.com/articles/post-ferguson-legislative-push-mostly-fizzled-1438853400>. Whether or not body cameras will actually promote these values is unclear. Their role in police accountability will depend in part on what policies individual police departments adopt.

<sup>60</sup> Elisha Fieldstadt, *Should Every Police Officer Be Outfitted with a Body Camera?*, NBC NEWS (Nov. 26, 2014, 3:30 PM), <http://www.nbcnews.com/storyline/michael-brown-shooting/should-every-police-officer-be-outfitted-body-camera-n256881>.

<sup>61</sup> See Randall Stross, *Wearing a Badge, and a Video Camera*, N.Y. TIMES (Apr. 6, 2013), <http://www.nytimes.com/2013/04/07/business/wearable-video-cameras-for-police-officers.html>.

after the events of Ferguson.<sup>62</sup> To further encourage police body camera adoption at the state and local level, the Department of Justice in 2015 made \$20 million dollars in grant funding available for body camera purchases.<sup>63</sup> According to a 2015 survey, almost ninety-five percent of police and sheriff's departments in major American cities and counties had plans to adopt or had adopted body cameras.<sup>64</sup>

The basics of a body camera appear simple enough: It is worn by a police officer, and it records video. In practice, however, police departments that adopt body cameras must address complex issues about data production, storage, and access.<sup>65</sup> The data production questions, for instance, involve when and in what circumstances body cameras can or must be turned on or off. For instance, should police officers turn on their body cameras in every interaction with the public? Should an officer accede to a request to turn a camera off? Should police have individual discretion to turn their body cameras off—such as when informants or sexual assault victims are involved—and if so, when? The answers to these questions determine not only how the resulting video is produced, but whether it is produced at all.

### 1. *When Product Design Is Policy*

Questions that appear to be about policy are also often questions of design. A camera that alerts the public when it records incorporates a form of visceral notice;<sup>66</sup> a camera with a “stealth mode” permits surreptitious recording by the police.<sup>67</sup> If a camera can be controlled remotely, then the

---

<sup>62</sup> See, e.g., Max Ehrenfreund, *Body Cameras for Cops Could Be the Biggest Change to Come Out of the Ferguson Protests*, WASH. POST (Dec. 2, 2014), [https://www.washingtonpost.com/news/wonk/wp/2014/12/02/body-cameras-for-cops-could-be-the-biggest-change-to-come-out-of-the-ferguson-protests/?utm\\_term=.ac1b585fec69](https://www.washingtonpost.com/news/wonk/wp/2014/12/02/body-cameras-for-cops-could-be-the-biggest-change-to-come-out-of-the-ferguson-protests/?utm_term=.ac1b585fec69) (quoting president of the Police Foundation as saying that “[w]ithin the next five years or so, body-worn cameras will be as ubiquitous in the world of policing as handcuffs, the police radio, [and] the gun”).

<sup>63</sup> Mark Berman, *Justice Dept. Will Spend \$20 Million on Police Body Cameras Nationwide*, WASH. POST (May 1, 2015), <https://www.washingtonpost.com/news/post-nation/wp/2015/05/01/justice-dept-to-help-police-agencies-across-the-country-get-body-cameras/>.

<sup>64</sup> See LAFAYETTE GRP., MAJOR CITIES CHIEFS AND MAJOR COUNTY SHERIFFS: SURVEY OF TECHNOLOGY NEEDS—BODY WORN CAMERAS ii (2015), <https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rvnT.EAJQwK4/v0>.

<sup>65</sup> See Elizabeth E. Joh, *Beyond Surveillance: Data Control and Body Cameras*, 14 SURVEILLANCE & SOC’Y 133, 134–35 (2016) (discussing these issues).

<sup>66</sup> See M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1033 (2012) (describing visceral notice as “changing the consumers [sic] understanding by leveraging the very experience of a product or service”).

<sup>67</sup> See, e.g., Martin Kaste, *Stealth Mode? Built-In Monitor? Not All Body Cameras Are Created Equal*, NPR (Oct. 30, 2015, 5:48 PM), <http://www.npr.org/sections/alltechconsidered/2015/10/30/453210272/stealth-mode-built-in-monitor-not-all-body-cameras-are-created-equal> (noting that camera variations “can have a

decision to record can be left to a supervisor,<sup>68</sup> a choice which may preserve more data but increase resentment by line officers. If a camera has a “buffer” that has several seconds of recording preserved *before* an officer turns the camera on, then that design choice might assuage concerns about police discretion, mistakes, and dishonesty. Video data, once recorded, also needs to be stored in a way that complies with standards of evidence preservation and data security.

## 2. *Market Dominance*

In the marketplace for body cameras, most of these choices are left to one company, Taser International. Previously associated with electronic stun guns, Taser has become the dominant company in police body camera manufacturing, responsible for three-quarters of the body camera market in the United States.<sup>69</sup> Many of the largest police departments around the country, including those in Chicago, Los Angeles, Philadelphia, Washington, D.C., Dallas, Baltimore, and Las Vegas, have signed contracts with Taser.<sup>70</sup> Through its Axon brand, Taser sells several different types of cameras, including the Axon Flex, which is designed to attach to glasses or a shirt collar and records an officer’s eye-level view.<sup>71</sup>

Taser’s market dominance can be attributed to two factors. First, it is Taser’s cloud-management service, rather than its body cameras, that ensures long-term contracts with police departments. Body cameras generate a huge quantity of data that must be stored somewhere. Many police departments lack the technical capacity or skills to store data securely themselves. Taser offers police departments subscriptions to its cloud storage service for body-camera video with its subsidiary, Evidence.com.<sup>72</sup>

For the police, Taser offers a full-service system: both cameras and

---

profound effect on how the cameras are used and who benefits from them”).

<sup>68</sup> See Shirley Li, *The Big Picture: How Do Police Body Cameras Work?*, ATLANTIC (Aug. 25, 2014), <https://www.theatlantic.com/national/archive/2014/08/how-do-police-body-camera-work/378940/> (describing a body camera made by Vidcie that livestreams video to the precinct).

<sup>69</sup> David Gelles, *Taser International Dominates the Police Body Camera Market*, N.Y. TIMES (July 12, 2016), <https://nyti.ms/2kG49LY>.

<sup>70</sup> Zusha Elinson & Dan Frosch, *In Body-Camera Push, Taser Schools Cities on No-Bid Deals; Police-Equipment Maker Offers Local Officials Guidance on Contracts and Trips to Conferences*, WALL ST. J. (Apr. 19, 2016, 7:11 PM), <http://www.wsj.com/articles/in-body-camera-push-taser-schools-cities-on-no-bid-deals-1461092807>.

<sup>71</sup> Karen Weise, *Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So*, BLOOMBERG BUSINESSWEEK (July 12, 2016, 5:00 AM), <http://www.bloomberg.com/news/articles/2016-07-12/will-a-camera-on-every-cop-make-everyone-safer-taser-thinks-so>.

<sup>72</sup> See, e.g., Jimmy Jenkins, *Taser International Sees Future in Data Storage*, MARKETPLACE (Nov. 3, 2015, 5:00 AM), <https://www.marketplace.org/2015/11/03/tech/taser-international-sees-future-data-storage>.

data storage. As one investor stated, “Taser wants to be the Tesla or Apple of law enforcement.”<sup>73</sup> Indeed, the data storage service has proven far more profitable for Taser than the cameras themselves, “low-margin hunks of plastic designed to get police departments using the real moneymaker.”<sup>74</sup> While police departments do not buy new body cameras every year, cloud services have recurring charges.<sup>75</sup> For instance, Taser’s cameras purchased by the Birmingham, Alabama, police in 2015 cost about \$180,000, but the department’s entire five-year contract, including data storage and management, is \$889,000.<sup>76</sup>

Second, Taser holds a distinct advantage over other body-camera companies because of its existing dominance in the electric stun-gun market. When police departments purchase electric stun guns, they are almost always Taser brand products. Until 2014, stun guns were the main source of Taser’s profitability.<sup>77</sup> By 2015, year-over-year revenue from Taser’s Axon unit nearly doubled compared to the previous year.<sup>78</sup> Because of its stun-gun business, Taser claims to have relationships with 17,000 of the 18,000 law enforcement agencies in the United States.<sup>79</sup>

Those relationships also make it easier for Taser to persuade police departments to avoid competitive bidding processes and choose Axon cameras. Taser representatives emailed police officials in Richmond, Virginia, for example, and urged them to rely upon exemptions to the state’s procurement bidding process. One Taser representative wrote, “I’ve recently read through the State’s Procurement Guide relating to non-competitive purchases . . . . I see this can be used for a purchase when ‘there is only one source practicably available for the goods or services required.’”<sup>80</sup> In December 2015, the Richmond Police Department signed a no-bid contract worth \$2.4 million with Taser.<sup>81</sup> Reporters have uncovered similar instances of Taser actively courting police departments to sign no-bid contracts.<sup>82</sup>

Taser intends to influence the future design and use of police body

---

<sup>73</sup> See Weise, *supra* note 71.

<sup>74</sup> *Id.*

<sup>75</sup> See Lucas Mearian, *As Police Move to Adopt Body Cams, Storage Costs Set to Skyrocket*, COMPUTERWORLD (Sept. 3, 2015, 2:45 AM), <http://www.computerworld.com/article/2979627/cloud-storage/as-police-move-to-adopt-body-cams-storage-costs-set-to-skyrocket.html>.

<sup>76</sup> *Id.*

<sup>77</sup> Weise, *supra* note 71.

<sup>78</sup> Elinson & Frosch, *supra* note 70.

<sup>79</sup> Weise, *supra* note 71.

<sup>80</sup> Elinson & Frosch, *supra* note 70.

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*

cameras as well.<sup>83</sup> The company's CEO and co-founder, Rick Smith, expects Taser's body cameras will incorporate facial-recognition technology so officers can "query police records or social networks in real time."<sup>84</sup> While other smaller companies continue to develop alternative products and win contracts—most notably with the NYPD, the nation's largest police force<sup>85</sup>—the body-camera company most police departments will rely upon is Taser.

Taser will likely only strengthen its position in the body camera market after announcing in April 2017 that it would offer every police department in the country free body cameras, support software, and data storage for one year.<sup>86</sup> In addition, the company announced it would change its corporate name from Taser to Axon to reflect its emphasis on body cameras and their related technologies.<sup>87</sup>

Finally, the promise of body cameras—to increase police accountability and to deter misconduct—has only been partially realized. A technology by itself does not provide accountability; the policies behind it do.<sup>88</sup> Around the country, police have rushed to adopt body cameras, sometimes with few guidelines in place regarding issues such as when cameras should be used, when they can be turned off, how long data can be retained, and who may have access to it. Likewise, state legislatures have

---

<sup>83</sup> See, e.g., Weise, *supra* note 71 ("Cop cams are inextricably tied to Taser, by far the dominant supplier, and the company will likely shape whatever the devices evolve into.")

<sup>84</sup> *Id.*

<sup>85</sup> When the NYPD selected Viewu, Taser responded by lodging a formal complaint with the Police Commissioner. Pervaiz Shallwani, *NYPD's Contract for Body Cameras Will Face Scrutiny*, WALL ST. J. (Oct. 12, 2016, 9:30 PM) <https://www.wsj.com/articles/nypds-body-camera-contract-faces-scrutiny-1476318351> (noting that the NYPD chose Viewu over Taser in part because of cost); see also Mark Morales, *Taser Questions NYPD's Body-Camera Contract Award*, WALL ST. J. (Oct. 13, 2016), <https://www.wsj.com/articles/taser-questions-nypds-body-camera-contract-award-1476399883> (same).

<sup>86</sup> See, e.g., Mark Berman, *Taser Changes Its Name, Says It Will Give Every Police Officer in the U.S. a Free Body Camera for a Year*, WASH. POST (Apr. 5, 2017), <https://www.washingtonpost.com/news/post-nation/wp/2017/04/05/taser-changes-its-name-says-it-will-give-every-police-officer-in-the-u-s-a-free-body-camera-for-a-year/> ("After that [one year] trial period, the police departments would either send back the cameras or buy them."); Alfred Ng, *Police Hear a Pitch for Free Body Cameras, with a Side of AI*, CNET (Apr. 5, 2017, 9:00 AM), <https://www.cnet.com/news/police-free-body-cameras-artificial-intelligence-taser-axon-viewu/> (noting that the offer includes "body cameras for up to one year, along with software, storage, training and tech support for the equipment").

<sup>87</sup> Karen Weise, *Taser Is Giving Body Cameras to Any Cops Who Want Them*, BLOOMBERG BUSINESSWEEK (Apr. 5, 2017, 12:22 PM), <https://www.bloomberg.com/news/articles/2017-04-05/taser-is-giving-body-cameras-to-any-cops-who-want-them>.

<sup>88</sup> Elizabeth Joh, *Five Lessons from the Rise of Bodycams*, SLATE (Nov. 28, 2016, 11:41 AM), [http://www.slate.com/articles/technology/future\\_tense/2016/11/how\\_not\\_to\\_respond\\_to\\_the\\_next\\_police\\_surveillance\\_technology.html](http://www.slate.com/articles/technology/future_tense/2016/11/how_not_to_respond_to_the_next_police_surveillance_technology.html) (suggesting that the absence of clear guidelines in many jurisdictions has raised questions about public access, police officer discretion, and future technologies with respect to body cameras).



been slow to clarify how body camera video may be released under state public records laws. As a result, police body cameras have become poorly regulated all-purpose surveillance tools.<sup>89</sup>

### C. *Big Data Software and Proprietary Information*

Like companies selling stingrays and body cameras, vendors that sell police big data software can influence policing in ways that often go unnoticed. The term “big data” generally refers to the application of computer algorithms to very large sets of data,<sup>90</sup> such as the technology that drives predictions on Amazon, Tinder, and Netflix as well as decisions about credit card applications, loan approvals, financial fraud, and airport screening. For an increasing number of police departments, the tools of prediction are useful for helping the police identify suspicious persons and places.<sup>91</sup> Predictive policing programs suggest geographic areas where police should focus their enforcement attention.<sup>92</sup> Network analysis can help police identify which persons might be at heightened risk of violent victimization or aggression.<sup>93</sup> Threat analysis software can assign a score to warn a police officer of any potential danger posed in a street encounter or traffic stop.<sup>94</sup>

These algorithmically determined judgments about suspicion can be

---

<sup>89</sup> See, e.g., Jake Laperruque, *Should Police Bodycams Come with Facial Recognition Software?*, SLATE (Nov. 22, 2016, 7:00 AM), [http://www.slate.com/articles/technology/future\\_tense/2016/11/should\\_police\\_bodycams\\_come\\_with\\_facial\\_recognition\\_software.html](http://www.slate.com/articles/technology/future_tense/2016/11/should_police_bodycams_come_with_facial_recognition_software.html) (discussing near future likelihood of incorporating facial recognition technology into police body cameras).

<sup>90</sup> See, e.g., Steve Lohr, *How Big Data Became So Big*, N.Y. TIMES (Aug. 11, 2012), <https://nyti.ms/2jNgVr1> (describing big data as a “shorthand label that typically means applying the tools of artificial intelligence, like machine learning, to vast new troves of data beyond that captured in standard databases”).

<sup>91</sup> See generally Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014) (explaining how predictive policing, mass surveillance systems, and DNA databases are changing policing).

<sup>92</sup> See, e.g., Erica Goode, *Sending the Police Before There’s a Crime*, N.Y. TIMES (Aug. 15, 2011), <https://nyti.ms/2rNpMK1> (noting that the predictive policing program used in Santa Cruz, California, “generates projections about which areas and windows of time are at highest risk for future crimes by analyzing and detecting patterns in years of past crime data”).

<sup>93</sup> See, e.g., Monica Davey, *Chicago Police Try to Predict Who May Shoot or Be Shot*, N.Y. TIMES (May 23, 2016), <https://nyti.ms/1s4fQfh> (describing the use by Chicago police of its “heat list,” a computer algorithm that “assigns scores based on arrests, shootings, affiliations with gang members and other variables . . . to predict who is most likely to be shot soon or to shoot someone”).

<sup>94</sup> See, e.g., Conor Friedersdorf, *A Police Department’s Secret Formula for Judging Danger*, ATLANTIC (Jan. 13, 2016), <https://www.theatlantic.com/politics/archive/2016/01/a-police-departments-secret-formula-for-judging-danger/423642> (describing how with Intrado’s Beware software, “a city that gets a 911 call about a known individual or address can plug that information into a proprietary search function and get a ‘threat assessment’ based on publicly available data”).

biased or error-laden. In some cases, the raw inputs used by an algorithm can reflect biased human decisions that in turn help produce a biased result.<sup>95</sup> For instance, arrests—particularly for minor offenses—are the products of police discretion, which may in turn be influenced by legitimate determinations, like resource constraints, and illegitimate ones, like racial bias. If a predictive policing program relies heavily on past arrests as a factor in determining future suspicion, then any resulting prediction about where police should go in the future may be nothing more than a reflection of where they have been in the past.<sup>96</sup>

Similar questions might be raised about programs that sift through social media posts. Threat assessments may take into account inputs of dubious value—like posts critical of the police—that then produce results that themselves merit skepticism.<sup>97</sup> In addition, legal scholars have raised questions about whether the existing legal system—traditionally premised upon humans making the judgments—can adapt to automated decision making.<sup>98</sup>

The good news is that many computer scientists and legal scholars recognize both the value and feasibility of making “black box”<sup>99</sup> algorithms used in legal decisions more accountable.<sup>100</sup> The automated decision making of algorithms can be assessed beforehand to see if their processes are consistent, fair, and adequate. Alternatively, we might examine these processes afterwards to see if their results comport with legal and policy norms. In theory, algorithms in policing, sentencing, bail, and other criminal justice areas may represent an improvement on traditional methods of assessment: human beings alone.

The bad news is that the information necessary to make these

---

<sup>95</sup> See Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 674 (2016) (“Approached without care, data mining can reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society.”).

<sup>96</sup> See Joh, *supra* note 91, at 58 (discussing the problem of using human discretionary judgments as inputs in big data programs).

<sup>97</sup> See Kristian Lum & William Issac, *To Predict and Serve?*, SIGNIFICANCE, Oct. 2016, at 14, 16 (“[E]ven the best machine learning algorithms trained on police data will reproduce the patterns and unknown biases in police data.”). Both authors are data scientists. *Id.* at 15.

<sup>98</sup> See, e.g., Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 18 (2014) (“Meaningful accountability is essential for predictive systems that sort people into ‘wheat’ and ‘chaff,’ ‘employable’ and ‘unemployable,’ ‘poor candidates’ and ‘hire away,’ and ‘prime’ and ‘subprime’ borrowers.”).

<sup>99</sup> See generally FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* 8 (2015) (arguing that big data is a “black box” which must be made more intelligible to society).

<sup>100</sup> See, e.g., Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 636 (2017) (observing that “accountability mechanisms and legal standards that govern decision processes have not kept pace with technology” and arguing that “[c]itizens, and society as a whole, have an interest in making these processes more accountable”).

evaluations is often locked behind private doors. Though police departments may rely increasingly on big data tools, they do not create them. The police are customers who contract with private vendors. A police department looking for big data tools to predict crime or assess threats will turn to products like PredPol, Beware, Geofeedia, or DigitalStakeout. When police departments agree to purchase or contract for big data tools, they typically bargain for the results, but not the proprietary algorithms that produce them. PredPol, whose software relies upon inputted data to produce 500-foot square boxes on a map of a city to direct police where future crime is likely to occur, is well known for keeping its algorithm a “closely guarded” secret.<sup>101</sup>

The same is true of Intrado’s Beware, the software that analyzes billions of data points, including property records, commercial databases, recent purchases, and social media posts, to assign threat scores for people in a matter of seconds.<sup>102</sup> A person encountered in a traffic stop or service call and assigned a high threat score by the software will warrant extra caution on the part of the police. How the software arrives at any particular score, however, is not known to the public or even to the police because Intrado considers its algorithms a trade secret.<sup>103</sup>

In other cases, surveillance technology vendors may ban access to the *data* they produce for the police. The technology used in ShotSpotter, employed in at least ninety cities,<sup>104</sup> is able to identify the location of a gunshot within eighty feet of its discharge and report that data to the police.<sup>105</sup> The ShotSpotter company, however, considers the resulting data proprietary information that is unavailable to the public.<sup>106</sup> The company’s CEO described distribution of its data through public records requests as akin to “taking someone else’s Netflix subscription.”<sup>107</sup> While ShotSpotter

<sup>101</sup> Ali Winston, *Arizona Bill Would Fund Predictive Policing Technology*, *CTR. FOR INVESTIGATIVE REPORTING: REVEAL* (Mar. 25, 2015), <https://www.revealnews.org/article/arizona-bill-would-fund-predictive-policing-technology>.

<sup>102</sup> Brent Skorup, *Cops Scan Social Media to Help Assess Your ‘Threat Rating.’* *REUTERS: THE GREAT DEBATE* (Dec. 12, 2014), <http://reut.rs/13fIDBJ>. Local police departments “craft specific standards for what information is available and relevant in a threat score.” *Id.*

<sup>103</sup> See Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat ‘Score.’* *WASH. POST* (Jan. 10, 2016), [http://wapo.st/1OcTX3K?tid=ss\\_tw&utm\\_term=.f02f3c190f6f](http://wapo.st/1OcTX3K?tid=ss_tw&utm_term=.f02f3c190f6f); see also Skorup, *supra* note 102.

<sup>104</sup> Matt Drange, *We’re Spending Millions on This High-Tech System Designed to Reduce Gun Violence. Is It Making a Difference?*, *FORBES* (Nov. 17, 2016), <https://www.forbes.com/sites/mattdrange/2016/11/17/shotspotter-struggles-to-prove-impact-as-silicon-valley-answer-to-gun-violence>.

<sup>105</sup> Cara Buckley, *High-Tech ‘Ears’ Listen for Shots*, *N.Y. TIMES* (Nov. 20, 2009), <https://nyti.ms/2qPmJ6Q> (describing the operation of ShotSpotter technology).

<sup>106</sup> Jason Tashea, *Should the Public Have Access to Data Police Acquire Through Private Companies?*, *A.B.A. J.* (Dec. 1, 2016), [http://www.abajournal.com/magazine/article/public\\_access\\_police\\_data\\_private\\_company](http://www.abajournal.com/magazine/article/public_access_police_data_private_company).

<sup>107</sup> *Id.*

offers gunshot data for sale to its government customers, few cities have chosen that option. That choice may be attributable in part to confusion on the part of police departments as to what data they do and do not own in their ShotSpotter contract.<sup>108</sup>

These private lock-in effects may linger even after a police department terminates a contract with a vendor. Since at least 2012, Palantir has provided the NYPD with software that analyzes criminal justice data and highlights connections between people and crimes. When the NYPD decided to cancel its contract with Palantir in 2017 and requested a copy of Palantir's analysis to transfer to its new software system, Palantir provided the information—but without a translation key. Giving NYPD the means to translate Palantir's earlier software analysis, the company argued, would compromise its intellectual property rights.<sup>109</sup>

## II

### THE HARMS OF UNDUE INFLUENCE

The use of nondisclosure agreements, the ability to dominate a particular market, and the shielding of proprietary information all share a common feature: They exert an undue influence by private companies on public police practices. That influence can and has resulted in real harms that affect legal change, police oversight, and police accountability.

#### A. *Fourth Amendment Distortion*

First, the undue influence of surveillance technology companies can distort or hinder the development of Fourth Amendment law. When new surveillance technologies are kept secret because of nondisclosure agreements, they cannot be challenged by criminal defendants and those challenges can't be decided by judges—whatever the merits of the defendants' claims. The use of a new surveillance technology may or may not be considered a Fourth Amendment search, but a private company's insistence on secrecy removes the legal issue from judicial review.

That pattern fits the secrecy around the use of stingray devices and the subsequent discovery by reporters and civil liberties groups that these devices were being used by police. In a number of recent cases, police departments used stingrays and either did not seek any judicial authorization at all, or chose not to seek a warrant and applied for a “trap and trace” order with no indication that a new technology would be

---

<sup>108</sup> *See id.*

<sup>109</sup> The cancellation of the Palantir contract is discussed in William Alden, *There's a Fight Brewing Between the NYPD and Silicon Valley's Palantir*, BUZZFEED NEWS (June 28, 2017, 3:23 PM), [https://www.buzzfeed.com/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley?utm\\_term=.ioa3rVeLW8#.lyWx9BmDR0](https://www.buzzfeed.com/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley?utm_term=.ioa3rVeLW8#.lyWx9BmDR0).

employed.

The 2016 opinion in *State v. Andrews*,<sup>110</sup> from the Maryland Court of Special Appeals, illustrates how deliberate secrecy about a surveillance technology can hinder Fourth Amendment law. In 2014, Baltimore police used Hailstorm, a cell-site simulator also sold by the Harris Corporation, to locate Kerron Andrews, a suspect in an attempted murder. By forcing Andrews's phone to connect with their stingray, the Baltimore police located Andrews, who was sitting inside a residence in Baltimore City.<sup>111</sup> Andrews argued that the evidence later found at the apartment should be suppressed because it was discovered as a result of police use of a stingray without a warrant.<sup>112</sup>

The *Andrews* court ultimately decided that the police should have obtained a warrant for their stingray use because it intruded upon Andrews's reasonable expectation of privacy under the Fourth Amendment.<sup>113</sup> In trying to locate Andrews, the police did not apply for a warrant, but they did apply for and were granted a pen register/trap and trace order.<sup>114</sup> By deciding that individuals have Fourth Amendment privacy rights in their real-time cellphone location information, the *Andrews* court held that the evidence found because of the Hailstorm's use had to be suppressed.

In deciding in Andrews's favor, the Maryland Court of Special Appeals heavily criticized the Baltimore Police Department (BPD) for its secret stingray use. The BPD application for the pen register order nowhere specified that the police would be using a stingray. Indeed, such a disclosure was prohibited by the nondisclosure agreement entered into by the Baltimore State's Attorney and the FBI as a condition imposed on the BPD in order to purchase Harris Corporation stingrays. The terms of the Baltimore nondisclosure agreement prohibited the police from revealing information about their stingray in any "press release, in court documents, during judicial hearings, or during other public forums or proceedings."<sup>115</sup>

Such secrecy, according to the *Andrews* court, "obstructs the court's ability to make the necessary constitutional appraisal."<sup>116</sup> In determining whether a search under the Fourth Amendment has occurred, a "court must understand why and *how* the search is to be conducted," including "the functionality of the surveillance device and the range of information

---

<sup>110</sup> 134 A.3d 324 (Md. Ct. Spec. App. 2016).

<sup>111</sup> *Id.* at 328–29.

<sup>112</sup> *Id.* at 330.

<sup>113</sup> *Id.* at 327.

<sup>114</sup> *Id.* (citing MD. CODE ANN., CTS. & JUD. PROC. § 10–4B–01 to 05 (West)).

<sup>115</sup> *Id.* at 338.

<sup>116</sup> *Id.* at 339.

potentially revealed by its use.”<sup>117</sup> By choosing compliance with the Harris nondisclosure agreement over its obligations to the court, the BPD took actions “detrimental to its position and inimical to the constitutional principles we revere.”<sup>118</sup>

The *Andrews* court at least had the opportunity to review the applicability of the Fourth Amendment’s search and seizure doctrine to the use of stingray surveillance. In other cases, prosecutors have dropped cases rather than be forced to divulge any possible stingray use. In a 2014 case, prosecutors withdrew evidence in the robbery prosecution of Shemar Taylor rather than disclose information about how the BPD was able to gather information about the defendant’s cellphone location.<sup>119</sup> And cases like *Andrews*’s and Taylor’s are not unique. Baltimore detective Emmanuel Cabreja testified in April 2015 that the department had used stingray surveillance 4300 times since 2007. Cabreja said that he personally had used a stingray device between 600 to 800 times in less than two years.<sup>120</sup>

Other police departments have gone to similar lengths to avoid disclosing any information about possible stingray use. In 2014, Tallahassee police admitted to a judge that the department had used stingrays at least 200 times without informing the courts and without obtaining a warrant.<sup>121</sup> In 2015, prosecutors dropped more than a dozen charges against three defendants in a series of robberies in St. Louis, Missouri, the day before a St. Louis police officer was scheduled to testify about the suspected use of a stingray in the case.<sup>122</sup> In a similar case, a detective declined to specify how one of the defendants had been located and cited a nondisclosure agreement that bound the department.<sup>123</sup>

While courts and lawmakers have begun to pay much more attention to police use of stingrays, that attention was made possible through investigative journalism, fortuitous circumstances, and defense attorneys’ skepticism regarding vague references to tracking locations. In what may

---

<sup>117</sup> *Id.* at 338.

<sup>118</sup> *Id.* at 339.

<sup>119</sup> Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, BALT. SUN (Nov. 17, 2014), <http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html>. Detective John Haley, when asked by Taylor’s defense attorney about the technique used to track him, responded: “I wouldn’t be able to get into that.” Haley cited the BPD’s nondisclosure agreement. Baltimore Circuit Judge Barry G. Williams replied: “You don’t have a nondisclosure agreement with the court.” *Id.*

<sup>120</sup> Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015), <http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html>.

<sup>121</sup> Zetter, *supra* note 31.

<sup>122</sup> Patrick, *supra* note 23.

<sup>123</sup> Patrick, *supra* note 29.

be dozens or even hundreds of instances around the country, criminal defendants lost opportunities to present Fourth Amendment claims about the warrantless use of cellphone surveillance tools in their cases. In turn, courts lagged even further behind in assessing the Fourth Amendment's application to stingray use. The one party most responsible for this doctrinal slowdown is a private company, the Harris Corporation.

### B. *Accountability by Design*

Police body camera video will only be useful if it exists in the first place. In a number of recent examples, body cameras failed to record shootings by the police because the officers involved failed to turn them on,<sup>124</sup> the cameras fell off,<sup>125</sup> or because the camera recorded images but no sound.<sup>126</sup> While these problems at first may seem to be matters of user error, they also illustrate how accountability can be embedded in surveillance technology design.

Consider the September 2016 fatal police shooting of Keith Scott, who was confronted by police officers in Charlotte, North Carolina. While the plainclothes officer who fatally shot Scott was not wearing a body camera, the uniformed officer who arrived at the scene was. Policies of the Charlotte-Mecklenburg Police Department required uniformed officers to turn on their body cameras "prior to" any investigative contact with civilians, but the uniformed officer did not turn his own on until some forty-five seconds after he arrived at the scene.<sup>127</sup> Right before the officer turned on his camera, its buffer mode recorded thirty seconds of video, but without any sound.<sup>128</sup> That video could not then confirm whether and how the officers on the scene had spoken to Scott, nor what they said, in the moments before shooting him.

In the Scott shooting, the failure to record was an accountability problem that was as much a design issue as it was human error. A differently designed camera might record a buffer with audio and video, or

---

<sup>124</sup> E.g., Kate Mather, *Two LAPD Officers Who Fatally Shot a Boyle Heights Teen Didn't Have Their Body Cameras On*, L.A. TIMES (Jan. 12, 2017), <http://www.latimes.com/local/lanow/la-me-ln-lapd-shooting-20170111-story.html>.

<sup>125</sup> E.g., Andrea Gallo, *End of Federal Alton Sterling Investigation Puts Spotlight Back on Body Cameras*, ADVOCATE (May 5, 2017), [http://www.theadvocate.com/baton\\_rouge/news/alton\\_sterling/article\\_815cec3a-31d6-11e7-a9dd-1b789f73ec80.html](http://www.theadvocate.com/baton_rouge/news/alton_sterling/article_815cec3a-31d6-11e7-a9dd-1b789f73ec80.html) (recounting the fatal shooting of Alton Sterling by Baton Rouge police officers whose body cameras "fell off at some point during their scuffle with Sterling").

<sup>126</sup> See *infra* notes 127–28 and accompanying text (discussing the shooting of Keith Scott).

<sup>127</sup> Wesley Lowery, *Charlotte Officer Did Not Activate Body Camera Until After Keith Scott Had Been Shot*, WASH. POST (Sept. 26, 2016), [http://wapo.st/2cwPtXn?tid=ss\\_tw&utm\\_term=.c9b26c12fbd7](http://wapo.st/2cwPtXn?tid=ss_tw&utm_term=.c9b26c12fbd7).

<sup>128</sup> See *id.*

be activated when cruiser lights are on,<sup>129</sup> or even be turned on remotely. Yet when one company dominates the market for a surveillance technology, police department choices are constrained by a dominant company's choices.

Many law enforcement agencies are well aware that they lack control over basic issues like body camera design and features. A common complaint noted in a 2015 survey of seventy large law enforcement agencies on body cameras stated that “[m]any technology decisions are largely being driven by *vendor selection*, rather than being driven by identified and articulated technical requirements.”<sup>130</sup>

When one company dominates the market for a surveillance technology, its choices about product design make important decisions about policing before the police themselves have an opportunity to do so. A police department considering a policy of surreptitious body camera recording in some instances may be pushed to adopt the tactic if the cameras they use incorporate stealth by design. Furthermore, if police departments, city councils, and state legislatures are slow to adopt regulations for body camera use—as is the case in many states<sup>131</sup>—then a dominant vendor's product design choices become the *de facto* policies for the police.

The largest vendor of police body cameras continues to make choices that influence policing and the legal limits of information collection. In February 2017, Taser acquired two companies that develop artificial intelligence to analyze stored video data.<sup>132</sup> By allowing the police to review stored data to look for objects, places, and actions, these tools encourage long-term rather than short-term data storage of body camera video, an issue that many police departments have not yet resolved. Finally, the prediction by Taser's CEO that its cameras will soon incorporate facial-recognition technology will mean that this policy decision—to match faces captured from a bodycam with an existing database—will likely be embedded in a surveillance technology before police departments or

---

<sup>129</sup> Taser does offer a body camera that turns on whenever an officer turns on a Taser stun gun. See Michael Fleeman, *L.A. Police to Get Tasers That Activate Body Cameras When Used*, REUTERS (Jan. 6, 2015), <http://reut.rs/1xPDACa>.

<sup>130</sup> LAFAYETTE GRP., *supra* note 64, at 5 (emphasis added). The Department of Homeland Security provided funding for the report. *Id.* at i.

<sup>131</sup> See, e.g., Liam Dillon, *All Police Body Camera Bills Have Failed This Year in California*, L.A. TIMES (Aug. 23, 2016), <http://www.latimes.com/politics/essential/la-pol-sac-essential-politics-updates-all-the-police-body-camera-bills-now-1471995313-htlmlstory.html> (noting that “[f]or the second straight year, California lawmakers have failed to pass any major legislation regulating police body cameras”).

<sup>132</sup> Aaron Tilley, *Artificial Intelligence Is Coming to Police Bodycams, Raising Privacy Concerns*, FORBES (Feb. 9, 2017), <http://www.forbes.com/sites/aarontilley/2017/02/09/artificial-intelligence-is-coming-to-police-bodycams-raising-privacy-concerns>.



legislatures decide formally whether or not to permit this capability. Hardly any police department in the United States has made policy decisions about incorporating biometrics into bodycams thus far.<sup>133</sup>

### C. Outsourcing Suspicion and Obscuring Transparency

Police that rely on big data tools to identify those people and places that deserve attention are using these programs to help develop their own assessments about suspicion. These assessments in turn can help develop the legal suspicion necessary to conduct stops, frisks, and arrests. At some point in the near future, courts will have to determine whether an algorithm's determination can form the basis, at least in part, of Fourth Amendment suspicion. If informants and tips can help develop reasonable suspicion, it is likely that courts will accept big data analysis as another source of information for the police as well.<sup>134</sup>

The problem for courts and defendants hoping to find out how a big data program has arrived at its conclusions is that the suspicion itself has been outsourced, at least in part. How an algorithm recommended police attention to one person or city block rather than another may be guarded as a "trade secret" that the algorithm's creators are unwilling to reveal.

While not a tool for developing police suspicion, defendants' experiences with TrueAllele software provide an instructive example. The software, developed by the Cybergenetics Corporation, promises to help identify suspects in cases where crime scene evidence commingles the DNA of multiple people, a situation that is often too difficult for conventional crime labs to resolve.<sup>135</sup> Courts in several states have admitted TrueAllele results in criminal cases, while not requiring Cybergenetics to reveal its source code to defense attorneys or their experts. Mark Perlin, Cybergenetics's founder, has cited the protection of the company's trade secrets as the reason why he has denied access to how TrueAllele arrives at its results.<sup>136</sup> At least one state court has concluded that disclosure of TrueAllele's source code could "'cause great harm' to the company."<sup>137</sup> As

---

<sup>133</sup> See LEADERSHIP CONFERENCE ON CIVIL & HUMAN RIGHTS & UPTURN, POLICE BODY WORN CAMERAS: A POLICY SCORECARD (2016), [https://www.bwvscorecard.org/static/pdfs/LCCHR\\_Upturn-BWC\\_Scorecard-v2.03.pdf](https://www.bwvscorecard.org/static/pdfs/LCCHR_Upturn-BWC_Scorecard-v2.03.pdf) (noting only six of fifty surveyed departments have policies on biometrics).

<sup>134</sup> See Joh, *supra* note 91, at 55–58 (making and developing this observation); see also Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 312 (2012) ("While never enough alone, with some relevant corroboration, a predictive tip will serve as the basis of a constitutional stop.").

<sup>135</sup> Joe Palazzolo, *Defense Attorneys Demand Closer Look at Software Used to Detect Crime-Scene DNA*, WALL ST. J. (Nov. 18, 2015), <https://www.wsj.com/articles/defense-attorneys-demand-closer-look-at-software-used-to-detect-crime-scene-dna-1447842603>.

<sup>136</sup> *Id.*

<sup>137</sup> Joe Palazzolo, *Judge Denies Access to Source Code for DNA Software Used in Criminal*

a result, defendants have been unable to verify TrueAllele's claims regarding the accuracy of its software's identification methods.

That same pattern will likely repeat itself with suspicion algorithms.<sup>138</sup> Big data software companies, like PredPol and Beware, believe their products contain proprietary information that cannot be shared with criminal defendants, journalists, or other interested parties. Thus, there is no mechanism for a person to see, for instance, what their threat rating is, how that score was developed, and how to challenge a potentially erroneous score.<sup>139</sup>

But an officer may unholster a firearm because of a black box score. By outsourcing the development of suspicion in part to surveillance-technology vendors, police departments that contract for these services obscure the means by which they develop suspicion to investigate, make decisions about whether and how they might deploy limited resources, and influence individual officers in how they approach the public.

### III

#### MINIMIZING UNDUE INFLUENCE

New surveillance technology products are eroding traditional limits on policing like resource constraints and public visibility.<sup>140</sup> Stingrays, body cameras, and big data software vastly increase investigative powers for the police at low cost and in secret. The continuing influence of surveillance companies even after police have purchased their services further removes policing from traditional mechanisms of oversight.

There are few conventional means to address the influence of surveillance technology vendors on the police. As private companies, they are not subject to the same constitutional restraints imposed upon the police. Nor are they subject to federal or state records-request laws. Any proposals to address this undue influence, then, are not likely to look like the traditional means by which the police themselves are regulated. Instead, we can look at recent examples to identify some means that can increase

---

*Cases*, WALL ST. J.: L. BLOG (Feb. 5, 2016, 10:56 AM), <http://on.wsj.com/1L3a0xN> (quoting Memorandum Order at 3, *Commonwealth v. Robinson*, No. CP-02-CR-0007777-2013 (Pa. Ct. Com. Pl. Feb. 5, 2016)).

<sup>138</sup> Rebecca Wexler argues further that the spread of automation and outsourcing of criminal justice data creates the erroneous impression that “the adversarial process is itself a business competition.” See Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System* 61 (Apr. 14, 2017) (unpublished manuscript), <https://ssrn.com/abstract=2920883>.

<sup>139</sup> See Skorup, *supra* note 102 (“[T]here is no mechanism for people to see their threat ‘ratings’—much less why the algorithm scored it.”).

<sup>140</sup> *Cf.* *United States v. Jones*, 565 U.S. 400, 429 (2012) (Alito, J., concurring in the judgment) (“In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.”).

transparency in these vendor-customer (i.e., company-police) relationships.

### A. Local Surveillance Oversight

In many cases, surveillance technology companies fail to provide basic information about their products. While local communities are unlikely to be able to force private companies to disclose information, let alone discover the existence of such information, they can put pressure on local government to participate in the process through which their police departments acquire new surveillance technologies.

Some cities have begun this process. In 2013, Seattle became the first city to adopt a local ordinance requiring city departments to seek approval before the purchase of surveillance equipment.<sup>141</sup> The ordinance prohibits any department from installing or using surveillance equipment until the city council provides guidance on its use. That guidance must include an assessment of the technology's impacts on anonymity and privacy and propose steps to be taken to mitigate those impacts. The ordinance arose out of controversies in which the Seattle Police Department had acquired a drone and proposed using federal funds to establish a surveillance camera network.<sup>142</sup>

In 2016, the County of Santa Clara, California, became the first in the nation to enact a similar ordinance that requires the sheriff and district attorney to seek approval from the county board of supervisors before obtaining new surveillance technology.<sup>143</sup> Law enforcement agencies are also required to provide the Santa Clara County Board of Supervisors with an annual surveillance report which describes "how the surveillance technology was used, including whether it captured images, sound, or information regarding members of the public who are not suspected of engaging in unlawful conduct."<sup>144</sup>

Also in 2016, the City of Oakland, California, created a nine-member Privacy Advisory Commission to guide the city's police on surveillance technology policies.<sup>145</sup> Public support for the commission arose out of the controversy surrounding a federal grant to develop a Domain Awareness

---

<sup>141</sup> SEATTLE, WASH., MUN. CODE § 14.18.20 (2013). Catherine Crump explains the background of the ordinance in a detailed case study. *See Crump, supra* note 2, at 1605–16.

<sup>142</sup> *See Crump, supra* note 2, at 1607–10 (noting the public backlash after the police department's failure to notify the city council of its drone acquisition).

<sup>143</sup> SANTA CLARA COUNTY, CAL., ORDINANCE CODE § A40-2 (2017); *see also* Cyrus Farivar, *Silicon Valley County Passes New Law Requiring Approval Before Cops Buy Spy Kit*, ARS TECHNICA (June 8, 2016, 5:00 AM), <https://arstechnica.com/tech-policy/2016/06/silicon-valley-county-passes-new-law-requiring-approval-before-cops-buy-spy-kit>.

<sup>144</sup> SANTA CLARA COUNTY, CAL., ORDINANCE CODE §§ A40-3, A40-7(a)(1) (2017).

<sup>145</sup> *Privacy Advisory Commission, CITY OF OAKLAND, CAL.*, <http://www2.oaklandnet.com/government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm> (last visited July 6, 2017).

Center (DAC) at the Port of Oakland. The DAC was intended to be a surveillance hub collecting and analyzing data from a variety of sources including license plate readers, cameras, and gunshot detectors that would collect data not just from the port but the city as well.<sup>146</sup> Oakland residents concerned about privacy organized resistance to the DAC, and in response the city council voted in 2014 to scale back plans for the center.<sup>147</sup>

City or county ordinances that require the police to inform them about and seek approval for the surveillance technologies they want to purchase are a promising first step. Oversight does not have to end at procurement. Local officials can require that their police departments develop guidelines for how the technology will be used and how the resulting data will be stored, analyzed, and shared. City councils and boards of supervisors can continue to oversee the use of those technologies through a variety of mechanisms, such as annual reporting requirements.<sup>148</sup> Some cities might also decide to limit corporate secrecy directly. In April 2017, for instance, Oakland's Privacy Advisory Commission proposed an ordinance that would render "any surveillance-related contract" with the city, including "nondisclosure agreements," to "be deemed void and legally unenforceable."<sup>149</sup>

### B. Public Records Requests as Oversight

While not usually considered a police-oversight mechanism, in the case of new surveillance technologies, the use of the federal Freedom of Information Act and state public records laws have played a central role in uncovering details about technologies kept secret in part because of the influence of vendors. Responses to public records act requests by civil liberties groups,<sup>150</sup> journalists,<sup>151</sup> and private citizens<sup>152</sup> have uncovered the

---

<sup>146</sup> See Darwin BondGraham & Ali Winston, *The Real Purpose of Oakland's Surveillance Center*, EAST BAY EXPRESS (Dec. 18, 2013), <http://www.eastbayexpress.com/oakland/the-real-purpose-of-oaklands-surveillance-center/Content?oid=3789230> (reporting that "the [DAC] is an open-ended project that would create a surveillance system that could watch the entire city and is designed to easily incorporate new high-tech features in the future"); Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES (Oct. 13, 2013), <https://nyti.ms/19EsPar> ("The new system . . . is the latest example of how cities are compiling and processing large amounts of information, known as big data, for routine law enforcement.").

<sup>147</sup> See Brian Wheeler, *Police Surveillance: The US City That Beat Big Brother*, BBC NEWS (Sept. 29, 2016), <http://www.bbc.com/news/magazine-37411250>.

<sup>148</sup> The ACLU has developed and distributed a model ordinance for community control over police surveillance. See Act to Promote Transparency, *supra* note 7.

<sup>149</sup> City of Oakland, Cal., Proposed Oakland Municipal Code § 9.64.060 (filed Apr. 28, 2017) (on file with author).

<sup>150</sup> See, e.g., Rachel Cohn & Angie Liao, *Mapping Reveals Rising Use of Social Media Monitoring Tools by Cities Nationwide*, BRENNAN CTR. FOR JUST. (Nov. 16, 2016), <https://www.brennancenter.org/blog/mapping-reveals-rising-use-social-media-monitoring-tools-cities-nationwide> (producing a map of police department acquisition of social media monitoring

existence of stingray nondisclosure agreements.

Collecting and sharing the results of these records requests have spurred further investigation and interest in uncovering new forms and sources of police surveillance technologies. Organizations like MuckRock<sup>153</sup> and the ACLU,<sup>154</sup> for example, have collected and posted investigative reporting that documents stingray use and the release of stingray nondisclosure agreements entered into by local police departments. When collected and posted together, these nondisclosure agreements are strikingly similar.

Prolonged media interest in the existence of stingrays uncovered in part by these tactics has prompted lawmakers to investigate. In 2014 and 2015, Senators Chuck Grassley and Patrick Leahy, both on the Senate Judiciary Committee, repeatedly asked the Department of Justice (DOJ) to disclose its policies and practices regarding stingray cellphone surveillance.<sup>155</sup> In their letters to the DOJ, Senators Grassley and Leahy cited media reports on the use of stingrays by federal, state, and local law enforcement agencies.<sup>156</sup>

## CONCLUSION

Stingrays, body cameras, and big data tools are likely to become as ubiquitous in policing as firearms, stun guns, and truncheons. As

software through public reports, a government procurement database, and public records requests); *Stingray Tracking Devices: Who's Got Them?*, ACLU, <https://www.aclu.org/map/stingray-tracking-devices-whos-got-them> (last visited Aug. 21, 2017) (identifying “72 agencies in 24 states and the District of Columbia that own stingrays” but noting that “because many agencies continue to shroud their purchase and use of stingrays in secrecy, this map dramatically underrepresents the actual use of stingrays by law enforcement agencies nationwide”).

<sup>151</sup> There are numerous examples of specific stingray nondisclosure agreements becoming known as a result of records requests by journalists. For instance, the Harris nondisclosure agreement with the Tucson Police Department was revealed pursuant to a records request made by journalist Mohamad Ali “Beau” Hodai. Zetter, *supra* note 31.

<sup>152</sup> Mike Katz-Lacabe, a private citizen, used state records requests to uncover the existence of stingrays in a number of Northern California law enforcement agencies. He subsequently created the Center for Human Rights and Privacy to collect and share information on surveillance technologies. See *About CeHRP*, CTR. FOR HUM. RTS. & PRIVACY, <https://www.cehrp.org/about-cehrp> (last visited May 25, 2017); see also CTR. FOR HUM. RTS. & PRIVACY, *supra* note 28 (collecting StingRay non-disclosure agreements).

<sup>153</sup> Brown & Musgrave, *supra* note 28 (collecting Stingray nondisclosure agreements).

<sup>154</sup> See *Stingray Tracking Devices: Who's Got Them?*, *supra* note 150 (tracking use of stingray devices).

<sup>155</sup> See Letter from Charles E. Grassley, Chairman, & Patrick Leahy, Ranking Member, U.S. Senate Comm. on the Judiciary, to Loretta Lynch, Attorney Gen., U.S. Dep’t of Justice (June 24, 2015), [https://www.judiciary.senate.gov/imo/media/doc/2015-06-24%20CEG%20and%20PJJ%20to%20DOJ%20\(Cell-site%20simulators\).pdf](https://www.judiciary.senate.gov/imo/media/doc/2015-06-24%20CEG%20and%20PJJ%20to%20DOJ%20(Cell-site%20simulators).pdf) (requesting written answers to questions regarding FBI use of cell site simulators).

<sup>156</sup> *E.g.*, *id.*

increasingly sophisticated surveillance technologies roll out at an ever-faster pace, we should expect police departments to be eager to adopt them. The problem, however, is that as consumers in the surveillance technology marketplace, police departments are often at the mercy of surveillance technology vendors. This means that police are limited by whatever the surveillance technology market provides for them. Moreover, the interests of technology vendors in protecting their products add a layer of secrecy that is at odds with conventional norms of transparency and accountability in policing—at a time in which the public has become especially aware of the need for reinforcing these norms.