THE UNDUE INFLUENCE OF SURVEILLANCE TECHNOLOGY COMPANIES ON POLICING

Elizabeth E. Joh*

ABSTRACT

Conventional wisdom assumes that the police are in control of their investigative tools. But in the case of 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. These companies 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.

* Professor of Law, U.C. Davis School of Law. Thanks to the librarians of the Mabie Law Library, and to the U.C. Davis School of law for research and institutional support.

INTRODUCTION

Conventional wisdom assumes that police are in charge of their investigative tools. The companies that create new surveillance technologies, however, are upending this assumption. Here, the police are consumers of surveillance technologies created and sold by private companies.[1] Through different mechanisms intended to promote their own interests and profits, these companies continue to exert control over the police long after their products have been adopted. Private surveillance technologies 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 technology shaping substantive decisions by the police about stops, frisks, and arrests.

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,[2] the role of private technology vendors has gone largely unnoticed. Yet

---

[1] 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.").

[2] *See, e.g.,* Rachel 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

any vision of increased police accountability today cannot be complete without consideration of the role surveillance technology companies play.

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, thermal imaging devices, and GPS trackers.[3] Congress and state legislatures have created legal standards for investigative techniques like electronic eavesdropping. Cities and counties can oversee local law enforcement agencies through budgetary decisions. When private companies influence policing through their role as vendors, 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.

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. 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.

I. EXAMPLES OF UNDUE INFLUENCE

A. STINGRAY CELLPHONE SURVEILLANCE AND NON-DISCLOSURE AGREEMENTS

Stingrays, as they are commonly known, refer to cell-site simulators:[4] 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

extensive than its civil rights enforcement and has an enormous and understudied impact on policing"); Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016) (arguing that federal funding of surveillance technologies can "short-circuit" involvement of local officials).

[3] *See* Kyllo v. United States, 533 U.S. 27 (2001); Jones v. United States, 132 S.Ct. 945 (2012).

[4] They are also called IMSI devices. *See, e.g.,* Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED, Apr. 9, 2013, at https://www.wired.com/2013/04/verizon-rigmaiden-aircard/.

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.[5]

Stingray devices work by behaving as fake cellphone towers.[6] 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.[7] Stingrays collect information by exploiting cellphone vulnerabilities. Our cellphones constantly try and connect to nearby cellphone towers in order to connect to our wireless carriers. Because a stingray mimics a legitimate cellphone tower antennae, it forces all nearby phones within its range to provide it with identifying information.[8] Depending on the individual model, a stingray device can identify in real time all nearby phones, pinpoint their location with a high degree of accuracy, and even block service to nearby devices.[9] In cases where stingray use has been revealed, the police seek either the unique serial numbers associated with all of the cellphones in a particular location, or to find the location of a phone where the officers

---

[5] Harris is also the manufacturer of other cellsite 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, at https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

[6] *See, e.g.,* Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders,* WIRED, Mar. 1, 2015, at 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 1) identify the hardware numbers of cellphones in a particular location or 2) to identify the precise location of a cellphone associated with a number the police already know. Jennifer Valentino-Devries, *How Stingray Devices Work,* WALL ST. J., Sept. 21, 2011, at http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/.

[7] Devlin Barrett, Americans' Cellphones Targets in Secret U.S. Spy Program, Wall St. J., Nov. 13, 2014, at https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

[8] *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 Authorities,* 16 YALE J.L. & TECH 134, 145-46 (2014).

[9] Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, WIRED, Mar. 1, 2015.

already know the numbers associated with it.[10]

These cases of cellphone surveillance are different from instances in which the police have asked wireless carriers like Sprint or Verizon for historical cell site information about a particular person. In recent appellate decisions like *United States v. Graham*[11] and *United States v. Davis,*[12] the police sought historical records from carrier companies about connections individual subscribers had made with a cellphone tower antennae. 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. 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.

1. Non-Disclosure Agreements

Dozens of local police departments as well as the FBI have drawn criticism because of the intense secrecy surrounding their use of stingrays.[13] In 2015 and 2016 journalists, civil liberties groups, and defense attorneys uncovered numerous examples in which police departments in the U.S. used stingray devices in criminal investigations. In many cases, no one outside of the police departments involved was officially notified that the police were intercepting information through the use of stingrays.

The Harris Corporation, the primary manufacturer of stingray devices, is responsible for most of this secrecy. To provide its stingray devices to local police departments, Harris needed regulatory approval of its products from the Federal Communications Commission.[14] When Harris applied to the Federal

---

[10] Jennifer Valentino-Devries, *How Stingray Devices Work*, Wall. St. J., Sept 21, 2011.
[11] 824 F.3d 421 (4th Cir. 2016).
[12] 785 F.3d 498 (11th Cir. 2015).
[13] Stingray have also been reportedly used by law enforcement agencies elsewhere. *See, e.g.,* Ashifa Kassam, *Vancouver Police Confirm Use of Stingray Surveillance Technology,* GUARDIAN, Aug. 10, 2016, at https://www.theguardian.com/world/2016/aug/10/vancouver-police-confirm-stingray-surveillance-technology.
[14] Robert Patrick, *Controversial secret phone tracker figured in dropped St. Louis case*, ST. LOUIS POST-DISPATCH, Apr. 19, 2015, at http://www.stltoday.com/news/local/crime-

Communications Commission for certification of its stingray devices in 2010, it requested that all information about stingrays "be treated as confidential and withheld from public inspection."[15] 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.[16] 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 enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization.[17]

In practice, these conditions have meant that local law enforcement agencies must abide by non-disclosure agreements, often overseen by the FBI, to use or acquire stingray equipment.[18] The results of numerous public records requests filed by journalists and others confirm that that police departments around the country have entered into similarly worded non-disclosure agreements about

---

and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html

[15] Letter from Tania W. Hanna & Evan S. Morris to Marlene H. Dortch, *Revised Request for Confidentiality of Harris Corporation*, Oct. 12, 2010, 4, at https://d3gn0r3afghep.cloudfront.net/foia_files/10-8-14_MR13549_RES_ID2014-668.pdf.

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

[17] FCC Grant of Equipment Authorization Certification, Mar. 2, 2012, at https://d3gn0r3afghep.cloudfront.net/foia_files/10-8-14_MR13549_RES_ID2014-668.pdf.

[18] *See, e.g.,* Timothy Williams, *Covert Electronic Surveillance Prompts Calls for Transparency,* N.Y. TIMES, Sept. 28, 2015, at https://www.nytimes.com/2015/09/29/us/stingray-covert-electronic-surveillance-prompts-calls-for-transparency.html ("The FBI, 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 non-disclosure agreements directly from local law enforcement agencies before permitting them to use their equipment.

stingrays.[19]

These non-disclosure agreements impose strict conditions of secrecy on law enforcement agencies that intend to use stingrays. [20] For example, the non-disclosure agreement agreed to by the Baltimore Police Department in 2011 in order to use a Harris Stingray, imposed the following conditions:[21]

- 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 non-disclosure agreement the City of Tucson 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."[22] The non-disclosure agreements of Tuscon and Baltimore are representative of others entered into by police departments around the country.

Requests by courts and journalists to determine whether police departments have acquired or used stingray technology have frequently met with resistance by

---

[19] Muckrock, Mike Lacabe's organization

[20] Robert Patrick, *St. Louis police: We track cellphones, but won't tell you how*, ST. LOUIS POST-DISPATCH, May 25, 2015, at http://www.stltoday.com/news/local/crime-and-courts/st-louis-police-we-track-cellphones-but-won-t-tell/article_80413390-e80d-558f-9bc7-46ba943391eb.html.

[21] *Baltimore Police Stingray non-disclosure agreement,* BALTIMORE SUN, Apr. 8 2015, at http://www.baltimoresun.com/bal-police-stingray-non-disclosure-agreement-20150408-htmlstory.html.

[22] Kim Zetter, *Police Contract With Spy Tool Maker Prohibits Talking About Device's Use*, WIRED, Mar. 4, 2014, at https://www.wired.com/2014/03/harris-stingray-nda/ (quoting Tucson-Harris non-disclosure agreement).

police departments relying on the terms of these non-disclosure agreements. For instance, police investigating a 2013 string of robberies in St. Louis identified three suspects by locating a victim's cellphone in a motel room.[23] 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. One day before a police intelligence officer was scheduled to be deposed about the department's Stingray use, pending criminal charges against the robbery defendants were dismissed.[24] 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 hearing that he could not comment upon any possible stingray use in the case because of an existing non-disclosure agreement.[25] Similar stories about dropped charges have been reported in Baltimore and in other cities.

2. Stingrays and the Fourth Amendment

Defense attorneys, civil liberties groups, journalists, and (eventually) 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 an interference with a person's reasonable expectation of privacy.[26]

---

[23] Robert Patrick, *Secret Service Agent's Testimony Shines Light on Use of Shadowy Cellphone Tracker in St. Louis*, ST. LOUIS POST-DISPATCH, Sept. 6, 2016, at http://www.stltoday.com/news/local/crime-and-courts/secret-service-agent-s-testimony-shines-light-on-use-of/article_f37e0c1d-824c-5fad-b630-48084553cdf2.html

[24] When charges were dropped against her three co-defendants, Wilqueda Lillard withdrew her guilty plea on basis that the use of stingray surveillance had not been disclosed in her case. Prosecutors dismissed the case. Robert Patrick, *St. Charles woman withdraws guilty plea in case linked to secret FBI cellphone tracker*, ST. LOUIS POST-DISPATCH, Apr. 27, 2015, at 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

[25] *See id.*

[26] 389 U.S. 347, 361 (1967)(Harlan, J., concurring)(establishing reasonable expectation of privacy test).

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, 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 unusually high amount of heat violated the Fourth Amendment.[27] Noting that the thermal imaging device obtained information that would otherwise have been obtained only by a physical entry of a home, the Court held that the warrantless use of such a device violated Kyllo's Fourth Amendment rights.[28] 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 should constitute 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 upon, in the U.S. Supreme Court's decision in *Jones v. United States*. In *Jones,* the Court considered whether the government's warrantless collection of 28 days' worth of GPS locational data amounted to a Fourth Amendment search.[29] The majority in *Jones* concluded that it did but in a way that did not directly address the collection of the data itself. Rather, the majority focused on the physical installation of the GPS receiver on the defendant's car, and found that this interference with Jones' property rights amounted to a Fourth Amendment search.

Five justices, however, writing in separate concurrences, seem to have approved of what has sometimes been called the "mosaic theory" of the Fourth Amendment. The mosaic theory argues that while any one governmental act of information collection may not be a search under the Fourth Amendment, the

---

[27] 633 U.S. 27 (2001).
[28] *See also* United States v. Karo, 468 U.S. 705, 715 (1984) (monitoring of beeper taking into a private residence was a Fourth Amendment search).
[29] 132 S.Ct. 945, 948 (2012).

totality of these actions might be. Thus, while one observation of a trip to the liquor store may not be regulated by the Fourth Amendment, that act repeated dozens of times would reveal much more information about a person and ought to be considered a search. The D.C. Circuit, in deciding Jones' case before it reached the Supreme Court, explicitly embraced the mosaic theory in holding the GPS monitoring was a search.[30]

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 "longer term use of GPS monitoring in investigations . . impinges on expectations of privacy."[31] Justice Sotomayor, in a separate concurrence, agreed that Jones' 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 violate reasonable expectations of privacy. Sotomayor goes on to explain that she would "take these attributes of GPS monitoring into account when considering the existence of a reasonable society expectation of privacy in the sum of one's public movements."[32]

Similar concerns about how to view the aggregation of data collected by the government have been raised in cases of historical cell site data. 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--sometimes tens of thousands of locational points--provide 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;[33] the only legal requirement is a showing that the data would be "relevant" under the

---

[30] *See* United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010), rev'd by United States v. Jones, 132 S.Ct. 945 (2012).

[31] 132 S. Ct. 945, 964 (2012)(Alito, J., concurring). Justice Sotomayor wrote in a separate concurrence that while she felt it unnecesary to resolve the case, she agreed with Justice Alito that long term GPS monitoring infringed Fourth Amendment expectations of privacy. 132 S.Ct. at 955 (Sotomayor, concurring).

[32] 132 S.Ct. At 956 (Sotomayor, J, concurring).

[33] *See* Smith v. Maryland, 442 U.S. 735 (1979). Justice Sotomayor's concurrence in United States v. Jones also called for a reexamination of the third party doctrine. *See* 132 S.Ct (Sotomayor, J., concurring).

Stored Communications Act.[34]

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 unware of their existence. In many criminal proceedings in which stingray use was suspected or later confirmed, prosecutors did not seek warrants for their use.[35] In some cases, prosecutors applied for a pen register order, without disclosing that the police had used a stingray device.[36] Orders granted under the federal Pen Register Act are not warrants. A court is required to 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."[37]

In at least one other instance, police maintained secrecy about stingray use by misleading description. In 2014, the 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 that "we simply refer to the assistance as 'received information from a confidential source regarding the location of the suspect."[38]

At the federal level, widespread attention and criticism of stingray secrecy resulted in a change in FBI policy. In September 2015, the Department of Justice

---

[34] 18 U.S.C. 2703(d).

[35] *See, e.g.,* Thomas v. State, No. 1Daa-6156 (Fl. Dist. Ct. App. 2013)(observing 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."), *available at* http://caselaw.findlaw.com/fl-district-court-of-appeal/1650231.html.

[36] *See, e.g.,* discussion of State v. Andrews, 227 Md. App. 350 (2016), *infra*.

[37] 18 U.S.C. 3123(a).

[38] ACLU of Florida, Sarasota Police Stingray Emails, June 19, 2014, at https://aclufl.org/resources/sarasota-police-stingray-emails/.

announced new guidelines for FBI use of stingrays.[39] 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.[40] The policy also applies in circumstances where the Department uses stingrays "in support of other Federal agencies and/or State and Local law enforcement agencies."[41] Several states also have bills requiring warrants for police stingray use under consideration, while others including California, Virginia, Minnesota, Washington, and Utah have already enacted such laws.[42]

B. CORNERING THE MARKET ON POLICE BODY CAMERAS

As consumers of surveillance products, police departments are limited by what the market has to offer. In a market dominated by one or two companies these companies' choices will shape not just what police departments purchase, but even how they use it - if they can afford the market price for the product at all.

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

---

[39] Kim Zetter, *The Feds Need a Warrant to Spy With Stingrays from Now on,* WIRED, Sept. 3, 2015, at https://www.wired.com/2015/09/feds-need-warrant-spy-stingrays-now/.

[40] U.S. Dep't of Justice, *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators,* Sept. 3, 2015, at https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.

[41] *See id.*

[42] *See* Cyrus Farivar, *California cops, want to use a stingray? Get a warrant, governor says,* ARS TECHNICA, Oct. 8, 2015, at 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, at http://www.usatoday.com/story/news/politics/onpolitics/2017/02/15/bipartisan-bill-seeks-warrants-police-use-stingray-cell-trackers/97954214/ (referring to proposals of Geolocation Privacy and Surveillance (GPS) Act which would require a warrant for all domestic law enforcement agencies to trak the location and movements of individual Americans without their knowledge).

police, public attention focused on the use of police body cameras as a means of promoting police accountability.[43] After a grand jury declined to indict officer Darren Wilson for shooting Michael Brown to death, Brown's family called for "every police officer working the streets in this country" to wear a body camera.[44]

While body cameras had been used by some departments prior to the protests prompted by Ferguson,[45] police departments around the country struggling to respond to concerns about transparency and accountability rushed to purchase them. 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.[46] According to a 2015 survey, almost 95 percent of police and sheriff's departments in major American cities and counties have plans to adopt or had adopted body cameras.[47]

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 several issues about data production, storage, and sharing.[48] 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

---

[43] *See, e.g.*, Elinson, Zusha, *Post-Ferguson Legislative Push Mostly Fizzed*, WALL ST. J., Aug. 6, 2016 at http://www.wsj.com/articles/post-ferguson-legislative-push-mostly-fizzled-1438853400 . Whether or not body cameras will actually promote this values is unclear. Their role in police accountability will depend in part on what polices individual departments adopt.

[44] Elisha Fieldstadt, *Should Every Police Officer be Outfitted With a Body Camera,* NBC NEWS, Nov. 26, 2014, at http://www.nbcnews.com/storyline/michael-brown-shooting/should-every-police-officer-be-outfitted-body-camera-n256881.

[45] Randall Stross, *Wearing a Badge, and a Video Camera*, N.Y. TIMES, Apr. 6,2013, at http://www.nytimes.com/2013/04/07/business/wearable-video-cameras-for-police-officers.html?rref=collection%2Ftimestopic%2FTASER%20International%20Inc

[46] Mark Berman, *Justice Department will spend $20 million on police body cameras nationwide,* Wash. Post, May 1, 2015, at https://www.washingtonpost.com/news/post-nation/wp/2015/05/01/justice-dept-to-help-police-agencies-across-the-country-get-body-cameras/

[47] Major Cities Chiefs Association and Major County Sheriffs' Association, *Technology Needs: Body Worn Cameras* ii (Dec. 2015), at https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rvnT.EAJQwK4/v0.

[48] *See* Elizabeth E. Joh, *Beyond Surveillance: Data Control and Body Cameras*, 14 SURVEILLANCE & SOC'Y 133, 134-135 (2016) (discussing these choices).

have individual discretion to turn their body cameras off—such as when informants or sexual assault victims are involved—and if so, when? 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;[49] a camera with a "stealth mode" permits surreptitious recording by the police. [50] If a camera can be controlled remotely, then the decision to record can be left to a supervisor[51]: a decision 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 dishonest mistakes. 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 U.S.[52] Many of the largest police departments around the country, including Chicago, Los Angeles, Philadelphia, Washington, D.C., Dallas, Baltimore, and Las Vegas have

---

[49] *See Ryan Calo, Against Notice Skepticism in Privacy (and Elsewhere),* 87 NOTRE DAME L. REV. 1027 (2012).

[50] *See, e.g.,* Martin Kaste, *Stealth Mode? Built-In Monitor? Not All Body Cameras Are Created Equal,* NPR, Oct. 30, 2015, at http://www.npr.org/sections/alltechconsidered/2015/10/30/453210272/stealth-mode-built-in-monitor-not-all-body-cameras-are-created-equal.

[51] Shirley Li, *The Big Picture: How Do Police Body Cameras Work?*, THE ATLANTIC, Aug. 25, 2014, at 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).

[52] David Gelles, *Taser International Dominates the Police Body Camera Market,* N.Y. TIMES, July 12, 2016, at https://nyti.ms/2kG49LY.

signed contracts with Taser.[53] 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.[54]

Taser's market dominance can be attributed to two factors. First, it is Taser's cloud management service rather than its body cameras that ensure long term contracts with police departments. Body cameras generate a huge quantity of data that has to 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 company Evidence.com.

For the police, Taser offers a full-service system: both cameras and data storage. As one investor in Taser stated, "Taser wants to be the Tesla or Apple of law enforcement."[55] 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.[56]" While police departments do not buy new body cameras every year, cloud services have recurring charges.[57] 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.[58]

Second, Taser also 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

---

[53] Ellinson & Frosch, supra note xx.

[54] Karen Weise, *Make Everyone Safer? Taser Thinks So*, BLOOMBERG BUSINESSWEEK, July 12, 2016, at http://www.bloomberg.com/news/articles/2016-07-12/will-a-camera-on-every-cop-make-everyone-safer-taser-thinks-so

[55] *See* Weise, *supra* note xx (reporting $127 million in stun gun revenue in 2013)

[56] *See id.*

[57] *See, e.g.*Andrew Kragie, *Houston police chief wants body cameras that automatically record,* HOUSTON CHRON., Dec. 15, 2016, at http://www.computerworld.com/article/2979627/cloud-storage/as-police-move-to-adopt-body-cams-storage-costs-set-to-skyrocket.html (observing that most of the Houston Police Department's body camera contract with Watchguard is for data storage).

[58] Lucas Mearian, *As police move to adopt body cams, storage costs set to skyrocket,* COMPUTERWORLD, Sep. 3, 2015, at http://www.computerworld.com/article/2979627/cloud-storage/as-police-move-to-adopt-body-cams-storage-costs-set-to-skyrocket.html.

Taser brand products. Until the fatal shooting of Michael Brown in Ferguson, Missouri sparked nationwide protests in 2014, stun guns were the main source of Taser's profitability.[59] By 2015, year over year revenue from its Axon unit nearly doubled compared to the previous year.[60] 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.[61]

Those relationships also make it easier for Taser to persuade police departments to avoid competitive bidding processes and chose 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 can see this can be used for a purchase when 'there is only once source practicably available for the goods or services required'.[62]" In December 2015, the Richmond police department signed a no-bid contract worth $2.4 million with Taser.[63] Reporters have uncovered similar instances of Taser's actively courting police departments to sign no-bid contracts.

Taser intends to influence the future design and use of police body cameras as well.[64] 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.[65]" While other smaller companies continue to develop alternative products and win contracts—most notably with the NYPD, the nation's largest police force—the body camera company most police departments will rely upon is Taser.

Finally, the promise of body cameras—to increase police accountability and to deter misconduct—has only been partially realized. A technology by itself doesn't

---

[59] *See* Weise, *supra* note xx.
[60] Ausha Elinson & Dan Frosch, In Body-Camera Push, Taser Schools Cities on No-bid Deals, Wall St. J., April 19, 2016, at http://www.wsj.com/articles/in-body-camera-push-taser-schools-cities-on-no-bid-deals-1461092807
[61] See Weise, supra note xx.
[62] Elinson & Frosch, *supra* note xx.
[63] Elinson & Frosch, *supra* note xx.
[64] See, e.g., Weise, supra note xx ("Cop cams are inextricably tied to Taser, by far the dominant supplier, and the company will likely shape whatever the devices evolve into.").
[65] Elinson & Frosch, supra note xx.

provide accountability; the policies behind it do.[66] 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 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.[67]

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.[68] Big data usually refers to 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.[69] Predictive policing programs suggest geographic areas where police should focus their enforcement attention.[70] Network analysis can help police identify which persons might be at heightened risk of violent victimization or aggression.[71] Threat analysis software

---

[66] Elizabeth Joh, *Five Lessons From the Rise of Bodycams,* SLATE, Nov. 28, 2016, at http://www.slate.com/articles/technology/future_tense/2016/11/how_not_to_respond_to_the_next_police_surveillance_technology.html.

[67] *See, e.g.,* Jake Laperruque, *Should Police Bodycams Come With Facial Recognition Software*? SLATE, Nov. 22, 2016, at http://www.slate.com/articles/technology/future_tense/2016/11/should_police_bodycams_come_with_facial_recognition_software.html.

[68] *See, e.g.,* Steve Lohr, *How Big Data Became So Big,* N.Y. TIMES, Aug. 12, 2012, at https://nyti.ms/2jNgVrl.

[69] *See generally* Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014).

[70] *See, e.g.,* Erica Good, *Sending the Police Before There's a Crime*, N.Y. TIMES, Aug. 15, 2011.

[71] *See, e.g.,* Monica Davey, *Chicago Police Try to Predict Who May Shoot or Be Shot*, N.Y.TIMES, May 23, 2016, at https://nyti.ms/2lmUbiV (describing use by Chicago police of its "heat list": a computer algorithm that "assigns scores based on arrests, shootings,

can assign a score to warn a police officer to any potential danger posed in a street encounter or traffic stop.

These algorithmically determined judgments about suspicion can be 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.[72] 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.[73] 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. In addition, legal scholars have raised questions about whether the existing legal system—traditionally premised upon humans making the judgments-can adapt to automated decisionmaking.

The good news is that many computer scientists and legal scholars recognize both the value and feasibility of making "black box"[74] algorithms used in legal decisions more accountable.[75] The automated decisionmaking 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,

affiliations with gang members and other variables" to "predict who is mostl like to be shot soon or to shoot someone").

[72] *See, e.g.,* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 CAL. L. REV. 671, 674 (2016) ("Approached without care, data mining can reproduce existing patterns of discrimination, inhere the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society.")

[73] *Cf.* Joh, *supra* note xx, at 58 (discussing the problem of inputs in big data programs).

[74] *See generally* Frank Pasquale, BLACK BOX SOCIETY: THE HIDDEN ALGORITHMS BEHIND MONEY AND INFORMATION (2015).

[75] *See e.g.,* Joshua Kroll, et al., *Accountable Algorithms,* 165 U. PENN. L. REV. ___ , 4 (2017) (observing that "accountability mechanisms and legal standards that govern decision processes have not kept pace with technology").

sentencing, bail, and in 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 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 themselves that produce them. Predpol, whose software relies upon inputted data to produce 500 by 500 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."[76]

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 matter of seconds.[77] 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.[78]

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, is able to identify the location of a gunshot within a ten foot radius of its discharge and report that data to the police. The Shotspotter

---

[76] Ali Winston, *Arizona Bill would fund predictive policing technology*, REVEAL, Mar. 25, 2015, at https://www.revealnews.org/article/arizona-bill-would-fund-predictive-policing-technology/.

[77] Local departments "craft individual standards for what information is available and relevant in a threat score." Brent Skorup, *Cops scan social media to help assess your 'threat rating,"* REUTERS, Dec. 12, 2014, at http://blogs.reuters.com/great-debate/2014/12/12/police-data-mining-looks-through-social-media-assigns-you-a-threat-level/.

[78] Justin Jouvenal, *The new way police are surveilling you: Calculating your threat "score,"* WASH. POST, Jan. 10, 2016, at https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.6c705fda87e9; *see also* Skorup, *supra* note xx.

company, however, considers the resulting data proprietary information that is unavailable to the public.[79] The company's CEO described distribution of its data through public records requests as akin to "taking someone else's Netflix subscription."[80] While Shotspotter 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.[81]

II. THE HARMS OF UNDUE INFLUENCE

The use of non-disclosure 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, they cannot be challenged by criminal defendants and those challenges can't be decided by judges—whatever the merits of a defendant's claims may be. 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

---

[79] Jason Tashea, *Should the public have access to data police acquire through private companies?*, ABA J., DEC. 1, 2016, at http://www.abajournal.com/magazine/article/public_access_police_data_private_company.

[80] *See id.*

[81] *See id.*

seek a warrant and applied for a "trap and trace" order that with no indication that a new technology would be chosen.

The 2016 opinion in *State v. Andrews,*[82] 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 were able to locate Andrews, who was sitting inside a residence in Baltimore City.[83] 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.

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.[84] 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. The term pen register originally referred to devices that records the outgoing numbers dialed by a telephone, although today it also can refer to other devices with similar functions. Police can obtain such orders without a warrant or probable cause, but rather on the lesser standard of "relevance."[85] By deciding that individuals have Fourth Amendment rights in their real-time cell phone location information, the *Andrews* court determined that the evidence found as a result of the Hailstorm's use had to be suppressed.

In deciding in Andrews's favor, however, the Maryland Court of Special Appeals heavily criticized the Baltimore police 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 non-disclosure agreement entered into by the Baltimore State's Attorney and the FBI as a condition imposed on the Baltimore police in order to purchase Harris Corporation stingrays. The terms of the Baltimore non-disclosure agreement

[82] 134 A.3d 324 (Md. App. 2016).
[83] *Id.* at 359.
[84] *Id.* at 327.
[85] *Id.* at 409 (citing MD CJP 10-4B-04(a)(1)).

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."[86]

Such secrecy, according to the *Andrews* court, "obstructs the court's ability to make the necessary constitutional appraisal."[87] 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 potentially revealed by its use."[88] By choosing compliance with the Harris non-disclosure agreement over its obligations to the court, the Baltimore police, in the *Andrews* court's view, took actions "detrimental to its position and inimical to the constitutional principles we revere."[89]

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 2014 case, prosecutors withdrew evidence in the prosecution of Shemar Taylor rather than disclose information of how the Baltimore police were able to gather information about the defendant's cellphone location.[90] And cases like Andrews's and Taylor's were not unique. Baltimore detective Emmanuel Cabreja testified in April 2015 that the department had used stingray surveillance 4,300 times since 2007. Cabreja said that he personally had used a stingray device between 600 to 800 times in less than two years.[91]

Other police departments have gone to similar lengths to avoid disclosing

---

[86] *Id.* at 374.
[87] *Id. at 375.*
[88] *Id.*
[89] *Id.*
[90] Justin Fenton, *Judge threatens detective with contempt for declining to reveal cellphone tracking methods,* BALTIMORE SUN, Nov. 17,. 2014, at http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html. In the robbery trial of Shemar Taylor, Detective John Haley, when asked by Taylor's defense attorney about the technique used to track him, Haley responded: "I wouldn't be able to get into that." Baltimore Circuit Judge Barry G. Williams replied: "You don't have a nondisclosure agreement with the court."
[91] *See id.*

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.[92] 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.[93] A detective had previously declined to specify how one of the defendants had been located and cited a non-disclosure agreement that bound the department.[94]

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 attorney skeptical of vague references to tracking location. In what are likely dozens or hundreds of instances around the country, criminal defendants lost opportunities to present their Fourth Amendment claims about the warrantless use cellphone surveillance tools in their cases. In turn, courts lagged even further behind in assessing the Fourth Amendment application to their 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,[95] the cameras fell off, or because the camera recorded images but no sound. While these problems at first

---

[92] *See* Kim Zetter, *Police Contract With Spy Tool Maker Prohibits Talking About Device's Use*, WIRED, Mar. 4, 2014, at https://www.wired.com/2014/03/harris-stingray-nda/.
[93] Robert Patrick, *Controversial secret phone tracker figured in dropped St. Louis case,* ST. LOUIS POST-DISPATCH, Apr. 19, 2015, at 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.
[94] Robert Patrick, *St. Louis police, We track cellphones, but won't tell you how,* ST. LOUIS POST-DISPATCH, May 25, 2015, at http://www.stltoday.com/news/local/crime-and-courts/st-louis-police-we-track-cellphones-but-won-t-tell/article_80413390-e80d-558f-9bc7-46ba943391eb.html.
[95] *See, e.g., Two LAPD officers who fatally shot a Boyle Heights teen didn't have their body cameras on,* L.A. TIMES, Jan. 12, 2017.

may see 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 Lamont Scott, who was confronted by police officers outside of an apartment complex 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. While policies of the Charlotte-Mecklenburg police department required uniformed officers to turn on their body cameras "prior to" any investigative contact with civilians, the officer in the Scott shooting did not turn his own on until some 45 seconds after he arrived at the scene.[96] Right before the officer turned on his camera, its buffer mode recorded 30 seconds of video, but without any sound.[97] That video could not then confirm how and whether 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 be activated when cruiser lights are on,[98] or even turned on remotely. Yet when one company dominates the market for a surveillance technology, police department choices are constrained by the dominant company's choices—in this case, Taser's.

Many law enforcement agencies are well aware that they lack control over the basic issues like body camera design and features. A common complaint noted in a 2015 survey of 70 large law enforcement agencies on body cameras stated that

---

[96] *See* Wesley Lowery, *Charlotte officer did not activate body camera until after Keith Scott had been shot,* WASH. POST, Sept. 26, 2016, at https://www.washingtonpost.com/news/post-nation/wp/2016/09/26/charlotte-officer-did-not-activate-body-camera-until-after-keith-scott-had-been-shot-2/?utm_term=.86cd2505f0bc.

[97] *See id.*

[98] 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, at http://www.reuters.com/article/us-usa-california-tasers-idUSKBN0KF26B20150106.

"Many technology decisions are largely being driven by *vendor selection*, rather than being driven by identified and articulated technical requirements."[99]

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 weighing surreptitious body camera recording in some instances may be pushed further 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[100]—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.[101] By allowing the police to review stored data to look for objects, places, and actions, these tools encourage long terms 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—matching faces captured from a bodycam with an existing database—will likely be embedded in a surveillance technology before police departments or legislatures decide independently formally to permit this capability or not.

---

[99] Major Cities Chiefs & Major County Sheriffs, *Technology Needs: Body Worn Cameras* 5 (Dec. 2015) at https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rvnT.EAJQwK4/v0. The Department of Homeland Security provided funding for the report. *See id. at i.*

[100] *See, e.g,* Liam Dillon, *All police body camera bills have failed this year in California,* L.A. TIMES, Aug. 23, 2016, at http://www.latimes.com/politics/essential/la-pol-sac-essential-politics-updates-all-the-police-body-camera-bills-now-1471995313-htmlstory.html (noting that "[f]or the second straight year, California lawmakers have failed to pass any major legislation regulating police body cameras").

[101] Aaron Tilley, *Artificial Intelligence is Coming to Police Bodycams, Raising Privacy Concerns,* FORBES, Feb. 9, 2017, at http://www.forbes.com/forbes/welcome/?toURL=http://www.forbes.com/sites/aarontilley/2017/02/09/artificial-intelligence-is-coming-to-police-bodycams-raising-privacy-concerns/&refURL=&referrer.

Hardly any department has made policies decisions about incorporating biometrics into bodycams thus far.[102]

C. Outsourcing suspicion and obscuring transparency

Police that rely on big data tools to identify those places and people 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.[103] 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.[104]

The problem that 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 will encounter a company reluctant to give up its trade secrets.

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 often too difficult for crime labs to figure out.[105] 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,

---

[102] Project Upturn, *Police Body Worn Cameras: A Policy Scorecard,* Aug. 2016, at https://www.bwcscorecard.org/static/pdfs/LCCHR_Upturn-BWC_Scorecard-v2.03.pdf.

[103]

[104] *See* Joh, *supra* note xx, at 57 (developing and making 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.").

[105] Joe Palazzolo, *Defense Attorney Demand Closer Look at Software Used to Detect Crime-Scene DNA,* WALL ST. J., Nov. 18, 2015, at https://www.wsj.com/articles/defense-attorneys-demand-closer-look-at-software-used-to-detect-crime-scene-dna-1447842603.

Cybergenetic's founder, has cited the protection of the company's trade secrets as the reason why he has denied access to how True Allele arrives at its results. At least one state court has concluded that disclosure of TrueAllele's source code would "cause irreparable harm to the company."[106] As a result, defendants have been unable to verify the claims of TrueAllele regarding the accuracy the method by which the software identified them as suspects.

That same pattern will likely repeat itself with suspicion algorithms. Big data software like PredPol and Beware consider their products as propriety 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.[107]

But an officer's firearm may be unholstered 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.[108] Stingrays, body cameras, and big data software vastly increase investigative powers for the police at low cost and in secret. The continuing influence played by surveillance

---

[106] *See* Joe Palazzolo, *Judge Denies Access to Source Code for DNA Software Used in Criminal Cases,* WALL ST. J., Feb. 5, 2016, at http://on.wsj.com/1L3a0xN; Commonwealth v. Robinson, Memorandum Order, CC 201307777 (PA Ct Common Pleas) Feb. 3, 2016, at http://online.wsj.com/public/resources/documents/Michael_Robinson_Opinion.pdf.

[107] *See* Skorup, *supra* note xx ("There is no mechanism for people to see their threat ratings much less how algorithm scored it.").

[108] United States v. Jones, 132 S. Ct. 945(2012)(Alito, J., concurring in the judgment)("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory but practical."

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 requests 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 might look at recent examples to identify some means that can increase transparency over these vendor (company)-customer (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 their existence on their own, they can put pressure on local government to participate in the process of how 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.[109] The ordinance prohibits any department from using or installing surveillance equipment until the city council provides guidance on its use. That guidance must include an assessment of the technology's impact on privacy and anonymity 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.[110]

In 2016, the county of Santa Clara, California became 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

[109] Seattle, WA Ordinance 12412 (2013), at http://clerk.seattle.gov/~scripts/nph-brs.exe?d=ORDF&s1=117730.cbn.&Sect6=HITOFF&l=20&p=1&u=/~public/cbor1.htm&r=1&f=G. Catherine Crump explains the background of the ordinance in a detailed case study. *See* Crump, *supra* note xx, at 1605-1616.

[110] *See id.*

technology.[111] Law enforcement agencies are also required to provide to Santa Clara Supervisors 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."[112]

That same year, the city of Oakland, California created a permanent nine member Privacy Advisory Commission to guide the city's policing on surveillance technology policies. Public support for the commission arose out of the controversy surrounding a federal grant to develop a Domain Awareness Center 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.[113] 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.[114]

City or county ordinances that require the police to inform them about and seek approval for the surveillance technologies they want to purchase is a promising first step. Oversight does not have to end at procurement. Local officials can require that their police departments develop guidelines about 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

---

[111] Santa Clara County, Ordinance Division A40-2 (2017), at https://www.municode.com/library/ca/santa_clara_county/codes/code_of_ordinances?nodeId=TITAGEAD_DIVA40SUECCOAF; Cyrus Farivar, *Silicon Valley county passes new law requiring approval before cops buy spy kit,* ARS TECHNICA, June 8, 2016, at https://arstechnica.com/tech-policy/2016/06/silicon-valley-county-passes-new-law-requiring-approval-before-cops-buy-spy-kit/.

[112] Santa Clara County, Ordinance Division A40-3, A40-7 (definitions) (2017).

[113] *See The Real Purpose of Oakland's Surveillance Center,* EAST BAY EXPRESS, Dec. 2013, at http://www.eastbayexpress.com/oakland/the-real-purpose-of-oaklands-surveillance-center/Content?oid=3789230; Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance,* N.Y. TIMES, Oct.13, 2013 at https://nyti.ms/2koivCu.

[114] *See* Bryan Wheeler, *Police surveillance: The US city that beat Big Brother*, BBC, Sept. 29, 2016, at http://www.bbc.com/news/magazine-37411250.

use of those technologies through a variety of mechanisms, such as annual reporting requirements.[115]

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,[116] journalists,[117] and private citizens[118] have uncovered the existence of stingray non-disclosure agreements.

Collecting and sharing the results of these records requests has spurred further investigation and interest in uncovering new forms and sources of police

---

[115] The ACLU has developed and distributed a model Community Control Over Police Surveillance model ordinance. *See* ACLU, CCOPS Model Bill (2016) at https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf.

[116] See, e.g., ACLU, *Stingray Tracking Devices: Who's Got Them?*, at https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (identifying 71 agencies in 24 states and the District of Columbia as owning 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."); Brennan Center for Justice (Rachel Cohn, Angie Liao), *Mapping Reveals Rising Use of Social Media Monitoring Tools By Cities Nationwide,* Nov. 16, 2016, at https://www.brennancenter.org/blog/mapping-reveals-rising-use-social-media-monitoring-tools-cities-nationwide (producing report on police department acquisition of social media monitoring software through public reports, procurement database, and public records requests).

[117] There are numerous examples of specific Stingray non-disclosure agreements becoming known as a result of records requests by journalists. For instance, the Harris NDA with the Tuscon Police Department was revealed pursuant to a records request made by journalist Mohamad Ali "Beau" Hodai. *See* Kim Zetter, *Police Contract With Spy Tool Maker Prohibits Talking About Device's Use*, WIRED, Mar. 4, 2014, at https://www.wired.com/2014/03/harris-stingray-nda/.

[118] 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* Center for Human Rights and Privacy, *Non-Disclosure Agreements Between FBI and Local Law Enforcement for StingRay*, at https://www.cehrp.org/non-disclosure-agreements-between-fbi-and-local-law-enforcement/.

surveillance technologies. Organizations like MuckRock[119] and the ACLU,[120] for example, have collected and posted stingray non-disclosure agreements imposed on local police departments for stingray use. When collected and posted together, these non-disclosure agreements are strikingly similar.

Prolonged media interest in the existence of stingrays uncovered in part by these tactics have 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 to disclose its policies and practices regarding stingray cellphone surveillance.[121] In their letters to DOJ, Senators Grassley and Leahy cited media reports on the use of stingrays by federal, state, and local law enforcement agencies.[122]

CONCLUSION

Stingrays, body cameras, and big data tools are likely to become as ubiquitous in policing as firearms, stun guns and truncheons. As 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 adds a layer of secrecy that is at odds with conventional norms of transparency and accountability in policing—at a time the public has become especially aware of the need for reinforcing these norms.

---

[119] Muckrock, *The Spy in Your Pocket* (2017), at https://www.muckrock.com/project/the-spy-in-your-pocket-14/ (collecting Stingray non-disclosure agreements).
[120] ACLU, *Stingray Tracking Devices* (2017), at https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices.
[121] *Judiciary Committee Seeks DOJ Policy on Cell Phone Monitoring Technology*, June 26, 2015, at http://www.grassley.senate.gov/news/news-releases/judiciary-committee-seeks-doj-policy-cell-phone-monitoring-technology.
[122] *Id.*