The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing

*Elizabeth E. Joh**

I. Introduction

In a crime analytics bureau, a police officer logs in to see what alerts have been posted by social media software designed to spot potential threats within the billions of daily online tweets, pins, likes, and posts. On the street, a police officer uses his body-worn camera to scan a crowd; the feed is sent in real time back to the department where facial recognition and movement analysis software alerts the patrol officer as to whether furtive movements or people on watch lists have been identified. Police follow up on these alerts to identify people who should be immediately investigated. Other people are dismissed as not posing an immediate threat but are logged on watch lists for future reference. No police department has all of this technological ability today, but some will one day soon.[1] There is no question that this version of big data policing is on the cusp of wider adoption,[2] and it raises key questions about fundamental issues of police discretion and accountability.

Whether the police identify a person and choose to investigate him for suspected criminal activity is a decision largely left up to the police. The decisional freedom[3] to focus police attention on a particular person or persons rather than others—what I'll call "surveillance discretion"[4]—is a widely accepted means of investigation. Law enforcement would be unimaginable without it. This task of filtering—identifying suspects from the general population—exemplifies traditional police work. Police officers usually generate leads by focusing their attention on particular suspects through observation, questioning, and information conveyed by witnesses, victims, or other third parties.

New technologies have altered surveillance discretion by lowering its costs and increasing the capabilities of the police to identify suspicious persons. Furthermore, soon it will be feasible and affordable for the government

* Professor of Law, University of California, Davis School of Law (eejoh@ucdavis.edu). Many thanks to Andrew Ferguson, Jane Bambauer, the participants of the 2015 Vanderbilt Criminal Justice Roundtable, and the participants of the 2015 Privacy Law Scholars Conference for valuable comments and suggestions.

[1] *See* Edwin Chan & Alex Dobuzinskis, *U.S. Police Struggle to Uncover Threats on Social Media*, Reuters (Dec. 26, 2014), http://www.reuters.com/article/2014/12/26/us-usa-police-socialmedia-idUSKBN0K40MD20141226 [http://perma.cc/UWA9-239V] (describing fact that fatal shooting of NYPD officers was preceded by Instagram post by shooter).

[2] *See, e.g.*, Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327, 410 (2015).

[3] Thanks to Jane Bambauer for this phrase.

[4] Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 U. Wash. L. Rev. 35, 61 (2014).

to record, store, and analyze nearly everything people do.[5] The police will rely on alerts generated by computer programs that sift through the massive quantities of available information for patterns of suspicious activity. The selection of investigative targets that emerge from big data rather than from traditional human investigation represents an important expansion in the powers of the police. That expansion, in turn, calls out for new tools of police accountability.

These "big data" tools produce dramatically different ways of identifying suspects. By applying computer analytics to very large collections of digitized data,[6] law enforcement agencies can identify suspicious persons and activities on a massive scale.[7] While these tools are useful in tracking down evidence of past crimes, big data also provides the police with new capabilities to identify ongoing and future threats. The Department of Homeland Security uses computer analytics to identify suspicious Twitter feeds that include words such as "bomb" or "listeria."[8] Police departments in Santa Cruz (CA), Seattle, and New York City are experimenting with predictive policing software to identify geographic places where crime is likely to take place.[9] One day the police nationwide may use location-based tweets to inform those same predictions.[10] The Chicago Police Department already

---

[5] *See* JOHN VILLASENOR, RECORDING EVERYTHING: DIGITAL STORAGE AS AN ENABLER OF AUTHORITARIAN GOVERNMENTS 1 (Dec. 14, 2011), http://www.brookings.edu/~/media/research/files/papers/2011/12/14-digital-storage-villasenor/1214_digital_storage_villasenor.pdf [http://perma.cc/U2TB-RYNW].

[6] *See, e.g.*, Steve Lohr, *How Big Data Became So Big*, N.Y. TIMES (Aug. 11, 2012), http://www.nytimes.com/2012/08/12/business/how-big-data-became-so-big-unboxed.html [http://perma.cc/B67F-CL9U] ("Big Data is 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.").

[7] Here big data refers to any application of any type of computer analytics to large sets of digitized data. Somewhat confusingly, the legal and popular scholarship interchangeably uses similar and overlapping terms in this area, such as datamining, databasing, machine learning, and artificial intelligence. *See* Michael Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, U. PA. L. REV. (forthcoming) (manuscript at 8), http://ssrn.com/abstract=2593795 [http://perma.cc/D8UA-ZFT3]. For instance, in his thorough analysis of how big data will change the reasonable suspicion calculus, Andrew Guthrie Ferguson uses big data to mean extremely large quantities of data, with or without data analytics. *See* Ferguson, *supra* note 2 ("Big data refers to the accumulation and analysis of unusually large data sets.").

[8] Somini Sengupta, *In Hot Pursuit of Numbers to Ward Off Crime*, N.Y. TIMES: BITS (June 19, 2013), http://bits.blogs.nytimes.com/2013/06/19/in-hot-pursuit-of-numbers-to-ward-off-crime/ [http://perma.cc/G2TJ-66EC].

[9] *See, e.g.*, Rich Calder, *NYPD Wants to Add Crime-Predicting Software to Arsenal*, N.Y. POST (July 8, 2015), http://nypost.com/2015/07/08/nypd-wants-to-add-crime-predicting-software-to-arsenal/ [http://perma.cc/6PR9-ZZDT]; Heather Kelly, *Police Embracing Tech That Predicts Crimes*, CNN (May 26, 2014), http://www.cnn.com/2012/07/09/tech/innovation/police-tech/ [http://perma.cc/NJB6-U2VE]; Bellamy Pailthorp, *Seattle, Tacoma Rolling Out New 'Predictive Policing' Software*, KPLU (Feb. 27, 2013), http://www.kplu.org/post/seattle-tacoma-rolling-out-new-predictive-policing-software [http://perma.cc/G6F5-ZCYD].

[10] *See* Rob Lever, *Researchers Use Twitter to Predict Crime*, YAHOO NEWS (Apr. 20, 2014), https://sg.news.yahoo.com/researchers-twitter-predict-crime-021341693.html [http://perma.cc/7ELW-33EQ].

uses big data tools to identify high risk persons based on the strength of a person's social networks: a technique borrowed from the military's analysis of insurgent groups.[11] These are not investigations about already identified suspects or crimes,[12] but rather the identification of potentially suspicious persons, places, and events.

The exercise of surveillance discretion in traditional policing attracts little attention from judges or legal scholars. Why? The answer is likely because 1) we assume that the police should possess such powers, and 2) even if theoretically worrisome, surveillance discretion is a power greatly limited in practice. After all, police investigations typically only focus on a limited number of persons because of practical limitations imposed by resources and technology. But those assumptions will become outdated when the police possess the tools to exercise automated surveillance discretion on a massive scale.

While the details leaked by Edward Snowden about the mass surveillance programs of the NSA are widely known, less familiar are the growing technological capabilities of local police departments. Yet these emerging technologies raise important questions about the expanded surveillance discretion of the more than 17,000 state and local police departments that assume primary responsibility for law enforcement in the United States.[13]

This expansion of surveillance discretion raises important legal and policy questions with regard to police oversight. In the traditional model of police investigation, the police may decide, after some initial investigation, to target a specific person or persons for further scrutiny. The Supreme Court's decisions make clear that the Fourth Amendment has little regulatory power over this discretionary process.[14] Unlike arrests or wiretaps, the decision to focus police attention on a particular person, without more, is unlikely to be considered a Fourth Amendment event. Thus, the police are not required to demonstrate probable cause or reasonable suspicion—the usual standards of individualized suspicion—to decide whether to conduct surveillance on an individual.[15]

---

[11] *See* Clay Dillow, *Building a Social Network of Crime*, POPULAR SCIENCE (Jan. 14, 2014), http://www.popsci.com/article/science/building-social-network-crime [http://perma.cc/UM2C-EDSN].

[12] This might be considered "suspect-driven" and "crime-out" uses of big data. Jane Bambauer, *The Lost Nuance of Big Data Policing*, 94 TEX. L. REV. (forthcoming 2015) (manuscript at 3, 27) (on file with author) (explaining that "crime-out investigations study clues from an already-committed crime" and arguing that warrants should be required for suspect-driven big data searches, but not crime-driven searches).

[13] Brian A. Reaves, *Census of State and Local Law Enforcement Agencies, 2008*, U.S. DEP'T OF JUSTICE, July 2011, at 2, http://www.bjs.gov/content/pub/pdf/csllea08.pdf [http://perma.cc/XAN2-WJYG].

[14] *See, e.g.*, United States v. Wallace, 811 F. Supp. 2d 1265, 1272 (S.D. W. Va. 2011) ("There is no constitutional prohibition against law enforcement watching, or following, particular individuals in high-crime areas.").

[15] *See, e.g.*, Safford Unified School Dist. No. 1 v. Redding, 557 U.S. 364, 370 (2009) (noting the Fourth Amendment "generally requires a law enforcement officer to have probable cause for conducting a search"); Terry v. Ohio, 392 U.S. 1, 20 (1968) (noting that "police

Surprisingly, there is little discussion of these decisions that the police make about individuals *before* any search, detention, or arrest takes place.[16] Rather, current unresolved issues of police technology have focused on whether a particular use is a Fourth Amendment search requiring a warrant and probable cause. Whether such constitutional requirements apply to the collection of historical cell site data is one such example.[17] Courts around the country have disagreed about whether these situations implicate Fourth Amendment protections, and it may take years for the United States Supreme Court to resolve these disputes.

And while the *enforcement* discretion of police and prosecutors—whether to enforce the law against a particular defendant or not—is a familiar topic in legal scholarship,[18] surveillance discretion—when, how, and whether the police may target a person or persons in the initial phases of governmental investigation—does not attract the same attention. Little scholarship has addressed when and how people should be considered targets for police surveillance in the first place—even if the police do nothing but watch closely. Some attention has already been paid to the use of big data by the police, such as with predictive policing software, but it addresses an important but familiar line drawing problem: whether decisions made by software can help justify conventional Fourth Amendment activities like stop-and-frisks.[19]

Surveillance discretion addresses the power of the police at an earlier stage: when the police focus on persons suspected of ongoing or future criminal activity but before any intervention takes place.[20] This preliminary investigative power is essential, since police need to possess some legal means to develop the required Fourth Amendment standard of individualized suspicion for a later search or seizure.[21] This preliminary stage of police investiga-

---

must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure").

[16] Of course, some of the scholarship in this area argues that some collections of data should in fact qualify as Fourth Amendment searches. *See, e.g.*, Jace C. Gatewood, *District of Columbia Jones and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory*, 92 NEB. L. REV. 504 (2014).

[17] *See, e.g.*, United States v. Graham, 796 F.3d 332 (4th Cir. 2015) (requiring a warrant); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (not requiring warrant).

[18] *See, e.g.*, Marc L. Miller & Ronald F. Wright, *The Black Box*, 94 IOWA L. REV. 125 (2008).

[19] *See, e.g.*, Ferguson, *supra* note 2.

[20] When defined this way, surveillance discretion does not focus on the use of big data to determine suspects in completed crimes, or to determine relevant information about one particular suspect in a completed crime. These types of suspect-driven investigations raise their own important questions, as recent cases involving challenges to warrantless searches of historical cell site data have shown.

[21] *See, e.g.*, Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: a Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 13 (2012); Bambauer, *supra* note 12 (manuscript at 9) (arguing that police need some way to build up suspicion about a suspect, and keeping every last third party record off limits until the case progresses to probable cause would unacceptably frustrate investigations); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 328 (2012)

tion usually receives little attention because it is not typically considered activity reached by the Fourth Amendment at all.[22]

Yet this new expansion of surveillance discretion by big data presents an underappreciated challenge to our usual thinking about police regulation.[23] How the police will use big data tools, particularly in future-oriented ways, is as pressing an issue of police accountability as individual officer bias, excessive force, and other pressing issues currently the topic of public debate. Unlike a police brutality case captured on a cellphone video, however, expanded police power by means of big data is difficult for most of the public to see and understand. Such secrecy and opacity calls for new tools of accountability.

II. How Big Data Expands Surveillance Discretion

Big data will revolutionize the surveillance discretion of the police.[24] By allowing the identification of large numbers of suspicious activities and people by sifting through large quantities of digitized data, big data expands the surveillance discretion of the police.

Of course, the use of big data is not the first time the police have focused on numbers, information, or record-keeping. Accurate documentation of crime and criminals has been a concern that reaches back to the nineteenth century and the invention of the *Bertillonage* system.[25] As they became more professional and bureaucratic, police of the twentieth century have sometimes been described as "knowledge workers" for whom information processing, rather than crime control, is a primary focus.[26] Even in their crime control capacities, large urban police departments in the 1990s had already turned toward data-driven or intelligence-based policing styles, of which the most famous is the N.Y.P.D's Compstat system.[27] The use of big

("The repeated use of nonsearch techniques has been considered an essential way to create probable cause that justifies searches rather than an unlawful search itself.").

[22] *See, e.g.*, United States v. Wallace, 811 F. Supp. 2d 1265, 1272 (S.D. W. Va. 2011).

[23] Some scholars are cautiously optimistic about big data policing tools. *See, e.g.*, Bambauer, *supra* note 12 (manuscript at 11) ("However, criminal procedure scholarship has not yet acknowledged how automated searching and filtering can dramatically change criminal investigations, largely (though not exclusively) for the better.").

[24] While there is no single definition of big data, most commentators agree that the term refers to the application of artificial intelligence to large amounts of digital information. *See* Lohr, *supra* note 6.

[25] *See* Simon A. Cole, Suspect Identities 32–59 (2001). Alphonse Bertillon, who in the late nineteenth century developed a method to index offenders based on physical measurements and observations, introduced the "first modern system of criminal identification." *Id.* at 32.

[26] Richard Ericson & Kevin Haggerty, Policing the Risk Society 19 (1997).

[27] Compstat is a "performance management system that is used to reduce crime and achieve other police department goals" that typically includes "(1) Timely and accurate information or intelligence; (2) Rapid deployment of resources; (3) Effective tactics; and (4) Relentless follow-up." *See* Police Executive Research Forum, Bureau of Justice Assistance, Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies 2 (2013), https://www.bja.gov/Publications/PERF-Compstat.pdf [https://perma.cc/8NJL-

data, then, accelerates and magnifies trends that until now had been slowly moving toward a heavier reliance on information and computers—with a specific emphasis on data analytics.

Understanding how expanded surveillance discretion should be regulated requires both an understanding of the big data phenomenon and how it has begun to influence policing.

A. What is Big Data?

The amount of data in big data almost defies comprehension. Nearly all of the world's stored information today is digital,[28] and we are surpassing existing mathematical terms to quantify it.[29] The types of information that are now digitized include ones that once existed in analog format (books, phone call logs, retail purchases) as well as new kinds of information made possible by today's technologies (internet searches, social media posts, data from the Internet of Things).[30] The Library of Congress, which has archived every Twitter tweet since 2010, receives about half a billion per day.[31] Every day, some of Facebook's 1.15 billion users upload more than 350 million photos to its website.[32] And digitization alters the nature of the information itself. Information that can be digitized can also be collected, searched, quantified, compared, assessed, and endlessly repurposed.[33] Most people know this is true from the automated suggestions they have encountered on services like Facebook, Netflix, and Amazon.[34]

FW77]. For representative accounts of the NYPD's reliance on Compstat, see, e.g., VINCENT E. HENRY, THE COMPSTAT PARADIGM: MANAGEMENT ACCOUNTABILITY IN POLICING, BUSINESS AND THE PUBLIC SECTOR (2003); ELI B. SILVERMAN, NYPD BATTLES CRIME: INNOVATIVE STRATEGIES IN POLICING 97–124 (1999).

[28] In 2012, there were approximately 2.7 zettabytes of stored digital information in the world. *See* Albert Pimentel, *Big Data: The Hidden Opportunity*, FORBES (May 1, 2012), http://www.forbes.com/sites/ciocentral/2012/05/01/big-data-the-hidden-opportunity/ [http://perma.cc/T9XQ-TAEW].

[29] The largest current recognized number is a yottabyte: a digit with twenty-four zeros. *See* John Foley, *Extreme Big Data; Beyond Zettabytes and Yottabytes*, FORBES (Oct. 9, 2013), http://www.forbes.com/sites/oracle/2013/10/09/extreme-big-data-beyond-zettabytes-and-yottabytes/ [http://perma.cc/L56V-SRCP].

[30] *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (May 2014), https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [http://perma.cc/87G9-HSCP] [hereinafter BIG DATA AND PRIVACY] (distinguishing between data "born digital" and "born analog").

[31] Erin Allen, *Update on the Twitter Archive at the Library of Congress*, LIBRARY OF CONGRESS BLOG (Jan. 4, 2013), http://blogs.loc.gov/loc/2013/01/update-on-the-twitter-archive-at-the-library-of-congress/ [http://perma.cc/9F9V-8KLB].

[32] INTERNET.ORG, A FOCUS ON EFFICIENCY (Sept. 16, 2013), http://www.meducationalliance.org/sites/default/files/internet.org_-_a_focus_on_efficiency.pdf [http://perma.cc/MTY9-6JDG].

[33] *See, e.g.*, VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 122 (2013) ("The crux of data's worth is its seemingly unlimited potential for reuse: its option value.").

[34] *See, e.g.*, Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [http://perma.cc/

Apart from its quantity, big data provides a very different way of understanding and probing the world of information.[35] Consider how big data has altered conventional research. If traditional scientific research begins with a question and then uses that hypothesis to identify and collect the appropriate data, big data upends that practice.[36] Because data is being generated all of the time, researchers working with big data do not have to shape or limit their data collection. Nor do they need to begin with a question. Indeed, the question can arise from the data itself. This is why, for example, the constant stream of posted tweets on Twitter can generate data and insights for meteorologists, advertisers, and epidemiologists.[37]

That insight has implications for the surveillance discretion of the police as well. Just as questions may emerge from the data for the purposes of research, suspects can emerge from the data for purposes of investigation. These suspicious persons and activities can appear even if police do not seek a particular person for a particular crime. Nor do they need to begin the collection of data, *if data is already being collected all of the time*.

Moreover, the search for causality—a primary objective in scientific research—is rendered unnecessary by big data, since correlations found on a mass scale can be just as, if not more, useful than attempts to find causes.[38] That is why, for example, Google's identification of the forty-five search terms most strongly correlated with historical flu data held the promise of predicting future outbreaks, even if they provided correlations rather than causes.[39] In the big data world, "knowing *what* is often good enough" rather than *why*.[40] In criminal investigations, it may not be necessary to know why certain patterns of driving, purchasing, or movement are associated with crime if the police can claim a high correlation between the two. A high degree of correlation itself might provide justification for heightened police attention.

8CZ2-R647] ("Almost every major retailer, from grocery chains to investment banks to the U.S. Postal Service, has a 'predictive analytics' department . . . .").

[35] *See, e.g.*, Adam Frank, *Big Data Is the Steam Engine of Our Time*, NPR (Mar. 12, 2013), http://www.npr.org/blogs/13.7/2013/03/12/174028759/big-data-is-the-steam-engine-of-our-time [http://perma.cc/H676-9EBM] ("Big Data may be the steam engine of our time.").

[36] MAYER-SCHÖNBERGER & CUKIER, *supra* note 33, at 61 ("In a small-data world, because so little data tended to be available, both causal investigations and correlation analysis began with a hypothesis, which was then tested to be either falsified or verified. . . . Today, with so much data around and more to come, such hypotheses are no longer crucial for correlational analysis.").

[37] Victor Luckerson, *What the Library of Congress Plans to Do with All Your Tweets*, TIME (Feb. 25, 2013), http://business.time.com/2013/02/25/what-the-library-of-congress-plans-to-do-with-all-your-tweets/ [http://perma.cc/F5RN-UB5M].

[38] *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 33, at 61.

[39] GOOGLE FLU TRENDS, https://www.google.org/flutrends/about/data/flu/us/data.txt [http://perma.cc/E6VZ-K6KD]. Google shut down its Flu Trends website in August 2015 after criticism of its forecasting failures, and instead makes its data available to researchers. Beth Mole, *New Flu Tracker Uses Google Search Data Better than Google*, ARS TECHNICA (Nov. 9, 2015), http://arstechnica.com/science/2015/11/new-flu-tracker-uses-google-search-data-better-than-google/ [http://perma.cc/2SJG-W9CD].

[40] MAYER-SCHÖNBERGER & CUKIER, *supra* note 33, at 59 (emphasis in original).

B. How Big Data Expands Surveillance Discretion

Like marketers, health care professionals, and traffic controllers, police departments have begun to test and adopt the tools of big data. These approaches hold the potential to change many aspects of traditional policing, including surveillance discretion. Three examples illustrate the range of big data tools already in preliminary use or under consideration by police departments.

The first is the use of automatic license plate readers (sometimes also referred to as "ALPR" or "ANPR") by the police. While the police have used cameras to take pictures of car license plates since the 1970s,[41] ALPR technology is especially notable today because it has become inexpensive, sophisticated, and increasingly pervasive.[42] ALPR systems use cameras mounted on patrol cars or at fixed locations and data analytics to identify license plate numbers.[43] These devices can read up to fifty license plates per second, and typically record the date, time, and GPS location of every scanned plate.[44] ALPR systems then read the scans and compare them against a "hot list," which contains license plate data for information such as stolen cars, parking violations, and terrorist watch lists.[45] One city even has used ALPR scans to detect those with delinquent property taxes.[46] The use of multiple cameras at multiple times makes it possible to see where and when one car (and presumably the person registered as the owner) moves around in time and space. Far from a specialized surveillance technique, ALPR cameras are used by the vast majority of police departments around the country.[47]

---

[41] *See, e.g.*, N.Y State Division of Criminal Justice Services, Suggested Guidelines: Operation of License Plate Reader Technology 5 (Jan. 2011), http://www.criminaljustice.ny.gov/ofpa/pdfdocs/finallprguidelines01272011a.pdf [http://perma.cc/U7YV-7T3T] ("The concept of using cameras as a method to record a vehicle passing through a specific location and then identifying the owner/operator has been in development since the 1970s. Early technology could capture a picture of a license plate and vehicle with the date and time. Upon retrieving the plate number after searching hours of captured images, the plate number could then be manually searched against a database. This technology was time consuming, expensive and limited by lighting and weather conditions.").

[42] *See, e.g.*, *id.* (describing later analog to digital processing method that, "while better than earlier methods, still had many drawbacks, including high costs that limited its general use by state and local governments").

[43] *Id.* at 11.

[44] *Id.* at 7.

[45] *See id.* at 5.

[46] *See* Theresa Clift, *Newport News to Begin Scanning License Plates to Find Delinquent Taxpayers*, Daily Press (Mar. 20, 2015), http://www.dailypress.com/news/newport-news/dp-nws-nn-license-scanners-20150319-story.html [http://perma.cc/48LQ-LN64].

[47] *See* ACLU, You Are Being Tracked: How License Plate Readers Are Being used to Record Americans' Movements 12 (July 2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/JFH4-8JK7] (reporting almost three-quarters of law enforcement agencies surveyed used ALPR technology); *see also* Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, Ars Technica (Sept. 27, 2012), http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/ [http://perma.cc/N8EZ-2Z7Z] (reporting ALPR use in the "tens of thousands").

A recent investigation by the news outlet *Ars Technica* shows the extent of information that can be captured by a single police department's ALPR system.[48] Responding to a public records request, the police department of Oakland, California released 4.6 million scans of 1.1 million unique plates representing three years' worth of ALPR data.[49] While most vehicles in the data set only appeared a few times, some notable exceptions illustrate how much information ALPR scans can reveal. One car was recorded 459 times over two years.[50] *Ars Technica*, with the help of a data analyst, was able to make "educated guesses" about the habits and addresses of those identified through their locational data.[51]

In addition to the scans taken directly by cameras operated by the police themselves, private databases of billions of ALPR scans provide the police with another source of surveillance data. Private ALPR cameras are now a routine tool of "repo men": repossession agents with truck-mounted ALPR cameras that can scan up to 8,000 plates a day and compare them against bank default lists.[52] These ALPR databases are available both for private and public customers, including law enforcement agencies. In March 2015, the New York Police Department announced a proposed contract with Vigilant Solutions, one of the largest ALPR companies in the United States, with a reported database of 2.2 billion scans.[53]

These ALPR readers can function as time machines to investigate already completed crimes. For instance, Vigilant Solutions demonstrates in a YouTube video how the police, in a hypothetical homicide investigation, can identify ALPR scans with a specified set of spatial and temporal parameters to see which cars (and registered drivers) have passed through the area and may serve as potential suspects.[54] Similarly, ALPR data can be used to track an individual person through time and space to determine his whereabouts (to check an alibi, to investigate a lead, etc.).

But ALPR data can expand surveillance discretion further to identify as yet unknown patterns of suspicious activity. Geo-fencing involves the designation of a specific geographical area that can be circumscribed with an

---

[48] Cyrus Farivar, *We Know Where You've Been: Ars Acquires 4.6M License Plate Scans From the Cops*, Ars Technica (Mar. 24, 2015), http://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/ [http://perma.cc/J86S-6HP9].

[49] *Id.*

[50] *See id.*

[51] *Id.*

[52] Bob Parks, *Scan Artist*, Popular Science (July 7, 2014), http://www.popsci.com/article/technology/scan-artist [http://perma.cc/B73H-53DV].

[53] *See* Cyrus Farivar, *NYPD to Conduct "Virtual Stakeouts," Get Alerts on Wanted Cars Nationwide*, Ars Technica (Mar. 2, 2015), http://arstechnica.com/tech-policy/2015/03/nypd-to-conduct-virtual-stakeouts-get-alerts-on-wanted-cars-nationwide/ [http://perma.cc/R4TJ-NAJP].

[54] Vigilant Solutions, *Vigilant Solutions License Plate Recognition (LPR) - Pattern Crime Case Study of Stakeout Feature*, http://vigilantsolutions.com/news/watch-videos [http://perma.cc/WDE7-3UUG].

ALPR "virtual fence" that identifies every car that enters that zone.[55] Consider, for example, a program that would identify suspicious patterns of activity, such as repeated visits by individual drivers to a location associated with drug trafficking.

A second use of big data is the collection and analysis of social media data. While many police departments polled state they monitor social media, these uses usually take the form of individual officers personally searching or using social media sites.[56] The Los Angeles Police Department, for instance, reportedly directs forty officers for this purpose.[57] Human monitoring of social media can include discrete searches for threatening words, suspects, and gangs. In other cases, the police might find information through social media by "friending" suspected criminals and learning information through online posts.[58] But such uses of social media are limited. Individual officers cannot search for every conceivable variation of suspicious language, and social connections with suspects online require identifying them in the first place.

Instead of relying on human beings, a big data approach looks through all, or nearly all, of the available data and uses computer algorithms to identify suspicious patterns of activity or to reveal previously unknown links among criminal suspects. That is the premise of a number of commercial software products now marketed to police departments.[59] *Social Media Monitor* is a "cloud-based service [that] will watch social networks" for suspicious activities.[60] Applying language analytics and sentiment analysis to services like Twitter and Facebook, *Social Media Monitor* claims to warn law enforcement clients of ongoing or potential threats of violence. Another software product, Intrado's *Beware*, promotes itself as a "tool to help first responders understand the nature of the environment they may encounter during the window of a 9-1-1 event."[61] *Beware* does so by assigning a "threat rating" to a person based on an analysis of billions of commercial

---

[55] ACLU, *supra* note 47.

[56] Int'l Ass'n of Chiefs of Police, 2014 Social Media Survey Results (2014), http://www.iacpsocialmedia.org/Portals/1/documents/2014SurveyResults.pdf [http://perma.cc/5RSB-KMS5].

[57] Chan & Dobuzinskis, *supra* note 1.

[58] *See, e.g.*, Oren Yaniv, *Cop Helps Take Down Brooklyn Crew Accused of Burglary Spree by Friending Them on Facebook*, N.Y. Daily News (May 30, 2012), http://www.nydailynews.com/new-york/helps-brooklyn-crew-accused-burglary-spree-friending-facebook-article-1.1086892 [http://perma.cc/8ECP-R3UQ] ("A Brooklyn cop helped take down a prolific burglary crew by friending its members on Facebook and monitoring their status updates for boasts about upcoming heists."); *see also* Elizabeth E. Joh, *Bait, Mask, and Ruse: Technology and Police Deception*, 128 Harv. L. Rev. F. 246 (2015), http://harvardlawreview.org/2015/04/bait-mask-and-ruse/ [http://perma.cc/UL4Q-67AJ].

[59] *Cf.* Big Data and Privacy, *supra* note 30, at 24 ("Analytics is what creates the new value in big datasets, vastly more than the sum of the values of the parts.").

[60] Sean Gallagher, *Staking Out Twitter and Facebook, New Service Lets Police Poke Perps*, Ars Technica (Nov. 13, 2013), http://arstechnica.com/information-technology/2013/11/staking-out-twitter-and-facebook-new-service-lets-police-poke-perps/ [http://perma.cc/CN9T-3CBV].

[61] *Intrado Beware*, Intrado, http://www.intrado.com/beware [http://perma.cc/D2CJ-LNB4].

and public records.[62] The *Beware* algorithm sorts through both information already familiar to the police (like registered cars and rap sheets) and novel (like "residents' online comments, social media and recent purchases for warning signs").[63]

A third example of expanded surveillance discretion is the use of social network analysis by police to identify suspicious or vulnerable individuals.[64] Social networks refer to a set of personal connections among a group of people. The basic unit of analysis in social network analysis consists of the link between two people.[65] The ties (relationships) between nodes (people) can take many forms: drug transactions, phone calls, or physical contacts between victims and offenders. Based on mathematical modeling, social network analysis maps a particular groups of relationships. Most importantly, the approach identifies the relative importance or centrality of nodes (individuals): "their importance to the criminal system, role, level of activity, control over the flow of information, and relationships."[66]

Social network algorithms developed for law enforcement purposes by private companies promise to identify non-obvious relationships in known criminal associations. While the police might know the leadership of a criminal gang, they may not know others who "ha[ve] the most influence in a gang, or who transmit[ ] the most information in the fastest amount of time."[67] This information can then be used by the police to focus their attentions on particular individuals that may have escaped police attention through conventional surveillance.

The aggressive use of social network analysis by the Chicago Police Department is illustrative.[68] Beginning in 2012, the Chicago police have relied upon the use of network analysis to direct preventive policing measures.[69] Beginning with the identification of the sixty known gangs and 600

---

[62] Brent Skorup, *Cops Scan Social Media to Help Assess Your 'Threat Rating'*, REUTERS (Dec. 12, 2014), http://blogs.reuters.com/great-debate/2014/12/12/police-data-mining-looks-through-social-media-assigns-you-a-threat-level/ [http://perma.cc/4L5T-ULB7].

[63] *Id.*

[64] *See, e.g.*, BIG DATA AND PRIVACY, *supra* note 30, at 28 ("Social-network analysis refers to the extraction of information from a variety of interconnecting units under the assumption that their relationships are important and that the units do not behave autonomously.").

[65] Jennifer A. Johnson et al., *Social Network Analysis: A Systematic Approach for Investigating*, FBI LAW ENFORCEMENT BULLETIN (Mar. 5, 2013), http://leb.fbi.gov/2013/march/social-network-analysis-a-systematic-approach-for-investigating [http://perma.cc/47QG-ZNYC].

[66] *Id.*

[67] Aaron Lester, *Police Clicking into Crimes Using New Software*, BOSTON GLOBE (Mar. 18, 2013), http://www.bostonglobe.com/business/2013/03/17/police-intelligence-one-click-away/DzzDbrwdiNkjNMA1159ybM/story.html [http://perma.cc/L2VN-YDP3] (describing software by founders of Mark43, http://scottmk43.herokuapp.com/platform.html [http://perma.cc/E6VH-WRC7] (claiming to be "the very first relationship based RMS [risk management system]")).

[68] Tony Dokoupil, *'Small World of Murder': As Homicides Drop, Chicago Police Focus on Social Networks of Gangs*, NBC NEWS (Dec. 17, 2013 3:48 AM), http://www.nbcnews.com/news/other/small-world-murder-homicides-drop-chicago-police-focus-social-networks-f2D11758025 [http://perma.cc/MJ4T-JQX5].

[69] *Id.*

factions within the city, the Chicago police then map out these relationships to identify both positive and negative connections among groups and individual members.[70] The name of a shooting victim, for instance, might trigger a computer warning to the police that four individuals should be treated with suspicion, not because of anything they did, but because they are known gang members feuding with the victim's gang.[71] In addition, another notification might alert the police of eight potential members of the victim's own gang who might be at risk of turning to violence in retaliation.[72] No traditional physical evidence links these persons to the actual shooting, but social network analysis predicts future violence associated with them, and thus directs police resources and attention.

The Chicago Police Department uses a "heat list" to focus its preventive policing efforts. This heat list is based upon research that found that those with close social ties to a homicide victim were 100 times more likely to be involved as a future victim or perpetrator of violence. In response, the Chicago police piloted a program in 2013 to identify these persons at high risk for future violence.[73] A computer analysis weighs risk factors: some that are not especially surprising, such as a person's rap sheet, his warrant or parole status, weapons or drug arrests, but also some that are, including a person's acquaintances and the arrest records and possible violent victimization of *those socially connected to the person*.[74] The approximately 400 people who emerge from the analysis with the highest scores constitute the heat list: a group targeted for the Chicago Police Department's Custom Notifications program.[75]

Being on the heat list results in a personal home visit from a Chicago Police officer, who warns the person of the legal consequences that will result if he engages in criminal activity.[76] Those on the list are also told that they are also at a high risk for becoming victims, not just perpetrators, of future violence.[77] Those who receive these "custom notifications" are not always obvious perpetrators of violence. They might be people who have otherwise escaped police notice because of an absence of serious convictions or a long rap sheet.[78] Moreover, it may be a social connection with a homicide victim that increases their risk rating.[79]

---

[70] *Id.*

[71] *See id.*

[72] *See id.*

[73] *See* Garry F. McCarthy, *Custom Notifications in Chicago - Pilot Program D13-09*, Chicago Police Dep't, http://directives.chicagopolice.org/directives-mobile/data/a7a57bf0-13fa59ed-26113-fa63-2e1d9a10bb60b9ae.html [http://perma.cc/M74N-D9L7].

[74] *See* Jeremy Gorner, *Chicago Police Use 'Heat List' as Strategy to Prevent Violence*, Chi. Trib. (Aug. 21, 2013), http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list/2 [http://perma.cc/H5MB-JKKF].

[75] *See* McCarthy, *supra* note 73.

[76] *See* Gorner, *supra* note 74.

[77] *See id.*

[78] *See id.*

[79] These are not the only uses of network analysis by the Chicago Police. For further discussion, see Jennifer Margolis & DaWana Williamson, *Notes from the Field: Chicago Vio-*

License plate readers, network software, and social media are not the only way the police use big data in intelligence or to predict suspicious activity. Predictive policing models that attempt to focus police attention to locations where crime is likely to occur in the future are already in use.[80] Moreover, some of these tools may be used in combination. License plate recognition tied with network analysis might be used to find cars associated in time and space with a car of primary interest to the police.

C. How the New Surveillance Discretion is Different

Surveillance discretion isn't new, but with big data tools the police have greatly expanded powers. This section examines what is distinct about the new surveillance discretion, as well as its potential benefits and concerns.

1. *Characteristics*

Innocent data aggregated to suspicious big data: Big data tools permit the police to sift through vast amounts of data that have no obvious connections to crime but through computer assisted analysis may suggest criminally suspicious activity. This is similar to traditional surveillance discretion; courts have permitted police to conduct stops based on facts that would not seem suspicious to us at all. Yet it is different, vastly different, in scale.

Mining social connections: Whether social connections can be plotted on a map, through online postings, or through social network analysis, big data tools allow law enforcement agencies to collect, aggregate, and analyze social connections using tailored algorithms. Rather than a specialized human skill,[81] mining social connections might one day be an ordinary aspect of local police departments.

From active investigations to passive alerts: The traditional methods the police use to identify or predict ongoing or future crimes require time and effort. The process is by necessity inefficient; by deciding to focus on some individuals, the police miss other opportunities. More generally, decisions to focus human resources on some kinds of suspicious activity rather than others reflect enforcement priority decisions that all law enforcement agencies must make.

---

lence Reduction Strategy: Applications of Social Network Analysis, National Network for Safe Communities, http://nnscommunities.org/uploads/Chicago_VRS_SNA_Notes_from_the_Field_0505_FINAL.pdf [http://perma.cc/7M3D-TQ5N] (discussing network analysis to identify gang members for "call-ins").

[80] *See, e.g.*, Joh, *supra* note 4; Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 Emory L. J. 259 (2012).

[81] *Cf.* Katrin Bennhold, *London Police 'Super Recognizer' Walks Beat With a Facebook of the Mind*, N.Y. Times (Oct. 9, 2015), http://www.nytimes.com/2015/10/10/world/europe/london-police-super-recognizer-walks-beat-with-a-facebook-of-the-mind.html [http://perma.cc/8STP-H694] (profiling British police officer with facial recall ability found among one to two percent of all people).

Automating the suspicion analysis—in whole or in part—could dramatically change policing. Some information that previously would not have been known to individual officers, either because it was unknown or because it would have been too cumbersome to retrieve quickly, becomes part of the investigations process. Big data might also bring new and unexpected insights about criminal behavior.[82] The scale of automation also widens the scope of surveillance over many more potentially suspicious persons.

2. *Potential Benefits*

Diminishing troubling uses of discretion: Big data tools, at least in theory, promise to introduce more fairness into surveillance discretion. Traditional policing relies upon an officer's ability to identify suspicious behavior. But because "nothing is inherently suspicious,"[83] conventional police decisions are normative judgments that are highly dependent on subjective considerations, and sometimes improper ones.[84] How police identify suspicious people thus sometimes reflects stereotypes about race and class, particularly about young African American men in economically depressed neighborhoods. After all, the police, like the rest of us, are "cognitive misers" who rely upon shortcuts to process the world around most efficiently.[85] Discretion also plays a role in departmental as well as individual decisions. Departments set priorities on whether to focus on prostitution and drugs sales on the streets, for instance, rather than within private spaces.[86]

Big data tools could curb police discretion in two ways. First, algorithms that search for suspicious activity could greatly reduce or eliminate race- or class-based biases for which the police are often criticized (although this too may hide hidden problems).[87] Second, certain crimes that may be especially amenable to big data policing, particularly white-collar financial fraud, may lead to more equitable distribution of law enforcement resources.[88]

Alternatives to flawed investigative tools: Increasing reliance on big data tools might one day eclipse the use of traditional surveillance and inves-

---

[82] *See* Ferguson, *supra* note 2, at 395–96 (suggesting that police track sales commonly used in crimes).

[83] Clive Norris, *From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control*, *in* Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination 248, 252 (David Lyon ed., 2003).

[84] Perhaps police suspicion can be best understood as a process generated from the exigencies of the moment rather than a fixed set of objective criteria. *See* David Dixon et al., *Reality and Rules in the Construction and Regulation of Police Suspicion*, 17 Int'l J. Soc. L., 185, 185 (1989).

[85] Susan Fisk & Shelley Taylor, Social Cognition 12 (1984).

[86] *See, e.g.*, Nirej Sekhon, *Redistributive Policing*, 101 J. Crim. L. & Criminology 1171, 1186 (2011) (noting "it is departmental choices—choices made by policymakers and administrators—that determine how arrests are distributed").

[87] *See infra* Part III.C.

[88] Law professors Jane Bambauer and Andrew Ferguson both contend that big data could make law enforcement more equitable. *See* Bambauer, *supra* note 12 (manuscript at 34); Ferguson, *supra* note 2.

tigation methods that have received significant criticism. Consider police reliance on informants.[89] When police rely on one or a few people to identify suspects, the results are necessarily skewed. Informants only identify people they know, from the neighborhoods they know. Informant culture then plays a key role in reproducing racial disparities within the criminal justice system.[90] Rather than rely on the usual suspects or the usual neighborhoods, big data programs search through all available information for future or ongoing crimes.[91]

Big data tools might also supplant some needs for covert policing in the physical world. Undercover operations are justified as a "dirty but necessary" business because without them, many types of crimes could not otherwise be investigated.[92] Big data tools may provide an alternative. White collar crime, for instance, is now difficult to identify without undercover investigations (and informants). However, with a computer program that can scan the enormous quantities of securities trading data for patterns of potential insider trading,[93] law enforcement officials may be able to rely less on covert operations, often criticized for their secrecy and implementation. Alternatively, though, the police may simply use big data tools in addition to covert tactics they adopt online.[94]

Production of data: Big data policing will produce information capable of audits and third party examination—a stark contrast from conventional surveillance. Fourth Amendment law requires police to provide specific articulable facts to justify stops and arrests.[95] These reasons are usually a mix of experience and observation. To make matters more difficult, the police feel pressure to conform their justifications to requirements about legally sufficient reasons that will hold up in court if challenged. Yet the complete explanation for what motivates a stop is likely unknowable, even to the officer himself. What stands out in an officer's mind as suspicious is the product of an "idiosyncratic, unaccountable, unknowable personal algorithm."[96] Moreover, in its Fourth Amendment decisions, the Supreme Court has

---

[89] For an incisive critique of police informant use, see Alexandra Natapoff, *Snitching: The Institutional and Communal Consequences*, 73 U. CIN. L. REV. 645 (2004).

[90] *Id.*

[91] *Cf.* Bambauer, *supra* note 12 (manuscript at 3) (arguing that "crime-out" search "constrains police discretion and limits the grip of confirmation bias").

[92] Elizabeth E. Joh, *Breaking the Law to Enforce It: Undercover Police Participation in Crime*, 62 STAN. L. REV. 155, 168 (2008).

[93] *See* Mary Jo White, *Keynote Address: 41st Annual Securities Regulation Institute*, S.E.C., http://www.sec.gov/News/Speech/Detail/Speech/1370540677500 [http://perma.cc/NK4H-N7TL] (describing operation of NEAT: National Exam Analytics Tool).

[94] *See, e.g.*, Tom Hays, *NYPD Is Watching Facebook to Fight Gang Bloodshed*, YAHOO! FINANCE (Oct. 2, 2012), http://finance.yahoo.com/news/nypd-watching-facebook-fight-gang-bloodshed-202724034.html [http://perma.cc/SC4A-RMXF] (describing "having officers adopt Internet aliases, create phony profiles and seek to 'friend' suspects to gain access to nonpublic information").

[95] *See* Terry v. Ohio, 392 U.S. 1, 21 (1968).

[96] Bambauer, *supra* note 12 (manuscript at 36).

shown little interest in subjecting the internal decision-making processes of police officers to any real scrutiny.[97]

3. *Potential Concerns*

Old problems in new packages: How, whether, and when the police use their legal authority to make choices poses a basic challenge for democratic policing. Law enforcement is impossible without giving the police choices, yet delegating the police discretion raises questions about fair-minded law enforcement in a democratic society.[98] Compounding our discomfort with police discretion is the fact that police are notoriously secretive, not just about their discretion but about nearly everything.[99] In theory, the increasing use of computers and numbers might force policing practices to be more transparent and accountable. Yet powerful big data tools can operate secretly and without public awareness in ways that cases of street police brutality cannot.

Hidden discretion: By applying data analytics to digitized information, big data tools appear to provide an objective analysis of information. But discretionary human decisions can play an important role in big data in ways that may not be obvious. First, very basic decisions about big data tools involve discretion: which mathematical model to adopt, what data to use, and how to display that data, among other considerations.[100] Second, police departments will make choices about how and where to apply big data tools; these are discretionary decisions similar to how departments deploy human resources. Predictive policing software, already in use by some police departments, focuses heavily on property crimes because its predictions about other crimes are not as accurate.[101]

The information used by big data tools may also be products of hidden police discretion.[102] Arrest information, at least for minor offenses, reflects highly discretionary decisions. If arrest records are used in an analysis to focus police resources, this can lead to further discretionary arrest patterns against the same neighborhoods and people. Even more reflective of police discretion are field interview cards: information officers collect about people

---

[97] *See, e.g.*, Whren v. United States, 517 U.S. 806 (1996).

[98] Joseph Goldstein, *Police Discretion Not to Invoke the Criminal Process: Low-Visibility Decisions in the Administration of Justice*, 69 YALE L. J. 549 (1960).

[99] *See, e.g.*, Jerome Skolnick, *Corruption and the Blue Code of Silence*, 3 POLICE PRAC. & RES.: AN INT'L J. 7 (2002).

[100] *See, e.g.*, Joh, *supra* note 4, at 58; Jennifer Bachner, *Predictive Policing: Preventing Crime with Data and Analytics,* IBM CENTER FOR THE BUSINESS OF GOVERNMENT 21 (2013), http://www.businessofgovernment.org/sites/default/files/Predictive%20Policing.pdf [http://perma.cc/KTV6-5VRW].

[101] *Predictive Policing: Don't Even Think About It*, ECONOMIST (July 20, 2013), http://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it [http://perma.cc/FN8B-CU2T].

[102] Sociologist Sarah Brayne describes this hidden police discretion vividly in her field work with the LAPD and its use of new data-driven surveillance. Sarah Brayne, Stratified Surveillance: Policing in the Age of Big Data ch. 4 (2015) (unpublished dissertation) (on file with author).

they encounter on the street for consensual, information-producing conversations.[103] Contact cards are unlikely to have an even or random distribution. Once transformed into data, this information can appear neutral and objective, even though they are the products of individual discretionary decisions. Moreover these highly discretionary decisions can be further influenced by other ones, such as departmental pressures to produce contact cards, or by metrics that assess officer productivity through consensual contacts, stops, and arrests.

Clerical mistakes and errors: In the dystopian 1985 movie *Brazil*, the plot centers on a kind of big data mistake: a clerical error leads to the government detention and death of a Mr. Buttle, instead of the intended target, a Mr. Tuttle.[104] While the movie offers a dark satire of a highly bureaucratic state, its observations are relevant today. The sheer amount of information that the police, like many other institutions and industries, must confront and assess is "overwhelming."[105] Errors and mistakes are inevitable.

The consequences of big data errors and distortions in policing can be severe. When marketers make decisions based on a faulty algorithm, the results may be embarrassing or annoying, but the stakes are comparatively low.[106] The same cannot be said of policing. The wrong person may be eventually detained, perhaps at gunpoint. Or she may face unwarranted humiliation because of police attention that may be noticed by family, friends, or employers.

For instance, algorithms can rely upon data that is itself incomplete or erroneous. For example, on the evening of March 30, 2009, San Francisco Police officers conducted a "high risk" traffic stop of Denise Greene, a forty-seven-year-old African American woman with no criminal record.[107] An automatic license plate reader mounted on a SFPD patrol car alerted officers that Greene's car was stolen.[108] The result, however, was a false hit; the camera misidentified Greene's car because the scan was blurry.[109] The police discovered their mistake, but not until after Greene was forced to kneel outside of her car at gunpoint, and to undergo a physical pat-down and a search of her car.[110]

---

[103] *See id.*

[104] BRAZIL (20th Century Fox 1985).

[105] Jean-Paul Brodeur & Benoit Dupont, *Knowledge Workers or "Knowledge" Workers?*, 16 POLICING & SOC'Y 7, 17 (2006).

[106] However, they can be non-trivial. While consumers have access to their own credit scores (and are thus provided with an opportunity for corrections), those afflicted with faulty predictions about whether they are likely to pay a debt or whether they would take their medications have no means of correcting or disputing them. E. Scott Reckard, *Data Compilers' Secret Scores Have Consumers Pegged—Fairly or Not*, L.A. TIMES (Apr. 8, 2014), www.latimes.com/business/la-fi-secret-consumer-scores-20140409,0,6240971.story, [http://perma.cc/VAW5-BYN8]; *see also* Bambauer, *supra* note 12 (manuscript at 14) (noting that "if law enforcement data collection is a problem, it is because law enforcement is special").

[107] Greene v. San Francisco, 751 F.3d 1039, 1042–43 (9th Cir. 2014).

[108] *Id.*

[109] *Id.*

[110] *Id.*

The surveillance tax: Even short of an investigative detention or arrest, surveillance can be intrusive. Knowledge of surveillance alone can inhibit our ability to engage in free expression, movement, and unconventional behavior. Judges and lawmakers have also occasionally acknowledged the stigmatizing effect of investigation itself, even if the police take no physically intrusive actions. As a Congressional report noted in 1984, "[t]he stigma which results from involvement in any investigation is substantial."[111] In neighborhoods with a fraught relationship between the community and the police, a "preventive" visit may be misinterpreted as the targeted person's conversion to an informant: a misinterpretation with potentially fatal consequences.[112]

Even in small doses, expansive uses of surveillance discretion can be worrisome. Expanded considerably, it is even more troubling, especially as big data tools have eroded the natural limits placed on surveillance discretion. Increased use of tools with a wider surveillance scope further increases the costs of "hassle": increased police attention or intervention that later turns out to be unwarranted.[113] These burdens of time, humiliation, and insecurity in law enforcement are inevitable,[114] but increasing these surveillance burdens requires accountability tools to accompany them.

Eliminating good discretion: If technology could eliminate some bad uses of police discretion (such as racial bias), it has the potential to dampen the power of good police discretion as well. Good discretion means many things, including giving an otherwise technically eligible person a break on behavior which would otherwise warrant a summons, a citation, or an arrest. Good discretion also includes what police might know about a neighborhood and its community: local knowledge that might not be amenable to data capture. Personal relationships and neighborhood knowledge can help police distinguish real dangers from false ones. An initial determination about suspicion, once perceived in context, may lead to a conclusion that nothing is amiss at all. In other words, traditional surveillance discretion is an aspect of local, contextualized police knowledge.

III. Accountability for Expanded Surveillance Discretion

When the police can watch many more people and activities with increasing sophistication and at lower cost, we need new transparency and accountability mechanisms. This section considers what issues will be raised by the development of new accountability mechanisms, as well as some suggestions for what form those mechanisms might take.

---

[111] *Cf.* Staff of S. Comm. on the Judiciary, 98th Cong., Rep. on FBI Undercover Operations (Comm. Print 1984).

[112] *See, e.g.*, Gorner, *supra* note 74, at 2 ("All the attention made him nervous because his neighbors noticed, leading them, he feared, to wonder if he was a police snitch.").

[113] *See* Jane Bambauer, *Hassle*, 11 Mich. L. Rev. 461, 464 (2015).

[114] *See* Bambauer, *supra* note 12, at 17.

A. Why the Fourth Amendment Does Not Apply

Traditionally surveillance discretion is a power enjoyed by the police with few legal constraints. When the police investigate a crime, they might decide to focus their attention on one particular person or group of people to confirm or dispel suspicions that arise after their preliminary investigation. The police may watch or follow the suspect on the street, talk to his associates, or comb through publicly available information.[115]

So long as the police confine the targets of their investigation to areas that are not private—even if their methods are secretive or covert—the police are not required to have any particular individualized suspicion about the suspect to focus their attention on him.[116] How long the police watch a person, why the police decide to investigate one person rather than another, and why they decide to investigate a crime at all are matters for police discretion, largely because the Fourth Amendment does not usually apply to these activities.[117]

That the Fourth Amendment does not regulate these early stages of investigation draws on well-established Supreme Court case law. Ever since the Supreme Court formulated the "reasonable expectation of privacy" test nearly fifty years ago in *Katz v. United States*,[118] it is generally understood that the police are free to investigate public places, speak with people consensually,[119] and access information that has already been given to third parties.[120] None of these areas are searches for Fourth Amendment purposes. All of these areas are those in which people "knowingly expose" information to the public, and thus also to the police.[121]

Fourth Amendment requirements apply, then, *after* the police have decided to use any information they have collected as a basis to interfere with a person's legally recognized interests. If the police subject a person to a temporary investigative detention, they are required to have reasonable suspi-

---

[115] *See, e.g.*, United States v. Wallace, 811 F. Supp. 2d 1265, 1272 (S.D. W. Va. 2011) ("There is no constitutional prohibition against law enforcement watching, or following, particular individuals in high-crime areas.").

[116] *See, e.g.*, State v. Talley, 307 S.W.3d 723, 730 (Tenn. 2010) (noting that "an investigation by governmental authorities which is not a search as defined by the Supreme Court may be conducted without probable cause, reasonable suspicion or a search warrant") (quoting State v. Bell, 832 S.W.2d 583, 589–90 (Tenn. Crim. App. 1991)); *cf.* United States v. Steinhorn, 739 F. Supp. 268, 271–72 (D. Md. 1990) ("It is readily accepted that law enforcement officials may conceal their investigatory activities when collecting evidence against potential defendants without compromising any principles of fairness or propriety.").

[117] *See, e.g.*, United States v. Taylor, 90 F.3d 903, 908 (4th Cir. 1996) ("[A] law enforcement 'officer's observations from a public vantage point where he has a right to be' and from which the activities or objects he observes are 'clearly visible' do not constitute a search within the meaning of the Fourth Amendment." (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986))).

[118] Katz v. United States, 389 U.S. 347, 360 (1967).

[119] *See, e.g.*, Illinois v. Lidster, 540 U.S. 419, 425 (2004) (noting "the law ordinarily permits police to seek the voluntary cooperation of members of the public in the investigation of a crime").

[120] Smith v. Maryland, 442 U.S. 735, 744 (1979).

[121] *Katz*, 389 U.S. at 365.

cion before doing so.[122] An arrest or full search requires probable cause, and in some cases, prior judicial approval in the form of a warrant.[123]

Before that point of intervention, however, the police can select a person or group of persons for particular attention without having to provide a justification for doing so. The police are "not restricted by being required to have a reasonable suspicion to observe or investigate persons in public and public data . . . to detect those [persons] who commit crime."[124] In other words, surveillance that does not intrude upon recognized Fourth Amendment interests requires no prior justification by the police.[125] The who, how, and why of police decisions to single out persons for attention is a matter of police discretion.

And because the Fourth Amendment does not regulate surveillance discretion, courts have had little to say about it. In response to claims that police surveillance is overly intrusive or controlling, courts have been generally unsympathetic. Lawful surveillance in the form of officers "walking their 'beat' or riding in 'prowl cars' " has been described as "proper police function," even if the surveillance might influence the targeted person's actions in public.[126] As the Eighth Circuit observed in one case, "judicial review of investigative decisions, like oversight of prosecutions, tends 'to chill law enforcement by subjecting the [investigator's] motives and decisionmaking to outside inquiry.' "[127] In rejecting claims regarding surveillance discretion, some courts have simply stated that "there is no constitutional right to be free of investigation."[128] The only caveat that courts raise is that surveillance discretion cannot be "exercised in a discriminatory fashion."[129]

---

[122] *See* Terry v. Ohio, 392 U.S. 1, 10 (1968).

[123] *See, e.g.*, Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 370 (2009) (noting the Fourth Amendment "generally requires a law enforcement officer to have probable cause for conducting a search"); *Terry*, 392 U.S. at 20 (noting that "police must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure").

[124] United States v. Steinhorn, 739 F. Supp. 268, 272 (D. Md. 1990).

[125] *See, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 850 n.24 (11th Cir. 2010) ("The Constitution does not require evidence of wrongdoing or reasonable suspicion of wrongdoing by a suspect before the government can begin investigating that suspect." (citing United States v. Aibejeris, 28 F.3d 97, 99 (11th Cir. 1994))); Metoyer v. State, 860 S.W.2d 673, 678 (Tex. App. 1993) (stating "neither probable cause nor reasonable suspicion are necessary to authorize a [police] surveillance" (citing Hamilton v. State, 590 S.W.2d 503 (Tex. Crim. App. 1979))).

[126] Sckorhod v. Stafford, 550 S.W.2d 799, 803 (Mo. Ct. App. 1977).

[127] Flowers v. Minneapolis, 558 F.3d 794, 798 (8th Cir. 2009) (quoting Wayte v. United States, 470 U.S. 598, 607 (1985)); *see also Sckorhod*, 550 S.W.2d at 798 ("Law enforcement's decision about whom to investigate and how, like a prosecutor's decision whether to prosecute, is ill-suited to judicial review.").

[128] *See, e.g.*, United States v. Trayer, 898 F.2d 805, 808 (D.C. Cir. 1990); *accord Rehberg*, 611 F.3d at 850 ("The initiation of a criminal investigation in and of itself does not implicate a federal constitutional right."); United States v. Crump, 934 F.2d 947, 957 (8th Cir. 1991); Sloan v. Dep't of Hous. & Urban Dev., 231 F.3d 10, 18 (D.C. Cir. 2000); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 186 (D. Conn. 2005); *cf.* Aponte v. Calderon, 284 F.3d 184, 193 (1st Cir. 2002) (noting "it is clear that investigations conducted by administrative agencies, even when they may lead to criminal prosecutions, do not trigger due process rights").

[129] Cole v. Fed. Bureau of Investigations, 719 F. Supp. 2d 1229, 1248 (D. Mont. 2010).

The view that no individual has a right to be free of investigation has also been the premise of a related legal question: whether the police must have at least reasonable suspicion before beginning an undercover operation targeting a particular person. The answer from courts has been a resounding "no."[130] Consider the ABSCAM scandal of the 1970s, which began with an FBI undercover operation that focused first on the trafficking of stolen property but eventually turned to political corruption. Evidence from ABSCAM eventually led to the convictions of several government officials, including a U.S. Senator and six members of the House of Representatives. Once ABSCAM was brought to public attention,[131] members of Congress considered whether individualized suspicion requirements should apply at this earlier investigative stage, but proposed legislation imposing a warrant requirement for undercover investigations never came to pass.[132]

In some rare instances, police surveillance by itself can give rise to constitutional claims. "Otherwise lawful surveillance" by the police can be the basis of a civil rights claim if the surveillance interferes with other constitutional rights.[133] For example, in October 2015, the Third Circuit reinstated a federal civil rights lawsuit alleging that the NYPD violated First Amendment and Equal Protection rights by engaging in a surveillance program of Newark's Muslim community.[134] The Supreme Court's 1972 decision in *Laird v. Tatum*,[135] however, makes it difficult for plaintiffs to win cases simply because they are concerned about the effects of lawfully collected surveillance. In *Laird*, the plaintiffs claimed that Army surveillance of civilian political activity infringed upon their First Amendment rights.[136] The Supreme Court held, however, that the *Laird* plaintiffs lacked standing to bring their claims because they lacked any justiciable injury. Absent a "specific present objective harm due to the surveillance or threat of a specific future harm," "the mere existence, without more, of a governmental investigative and data-gathering activity" could not form the basis of a federal

---

[130] *See, e.g.*, United States v. Allibhai, 939 F.2d 244, 249 (5th Cir. 1991). In *Allibhai*, the Fifth Circuit joined those "circuits that have . . . uniformly dismissed the notion that the government must have a pre-existing basis for suspecting criminal activity before targeting an individual in an investigation." The *Allibhai* court noted that "these decisions are premised upon the realization that '[a defendant] has no constitutional right to be free of investigation.'" *Id.* (quoting United States v. Jacobson, 916 F.2d 467, 469 (8th Cir. 1990)).

[131] *See* OFF. OF INSPECTOR GEN., THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES 41–42 (2005).

[132] *See id.* at 44.

[133] Bootz v. Childs, 627 F. Supp. 94, 103 (N.D. Ill. 1985) (citing Laird v. Tatum, 408 U.S. 1, 3 (1972)).

[134] *See* Hassan v. City of New York, No. 14–1688, 2015 WL 5933354, at *24 (3d Cir. Oct. 13, 2015); Benjamin Weiser, *Lawsuit Over New York Police Surveillance of Muslims Is Revived*, N.Y. TIMES (Oct. 13, 2015), http://www.nytimes.com/2015/10/14/nyregion/appeals-court-reinstates-lawsuit-over-police-surveillance-of-muslims.html [http://perma.cc/8CEE-998D].

[135] *Laird*, 408 U.S. at 3.

[136] *Id.* at 2.

lawsuit.[137] As a result of this standard, lawsuits complaining only about intrusive but otherwise lawful surveillance often fail.[138]

Because so few cases state much about surveillance discretion other than to acknowledge the wide latitude given to police to exercise their powers, we might look to other analogous areas of the law where courts have considered challenges to the preliminary exercises of governmental power.

For instance, many defendants have challenged the discretion of police and prosecutors for singling them out for arrest or prosecution. Many cases have considered defendants' claims that the police (or prosecutors) have unfairly or arbitrarily focused on them. But here too courts have yielded considerable discretion to law enforcement officials in deciding how, whether, and when to exercise their powers.[139] Claims of discriminatory enforcement in violation of the Fourteenth Amendment are available in theory, but in practice most fail because of the difficulty of proving the necessary elements.[140] Moreover, the Supreme Court's decisions in *Whren v. United States*[141] and *Atwater v. City of Lago Vista*[142] foreclose the ability of defendants to complain of arbitrary or pretextual enforcement in Fourth Amendment claims.[143]

What serves as a check on traditional surveillance discretion of the police, then, if not Fourth Amendment law? The answer lies in practical rather than legal restraints. First, surveillance has been naturally limited by the expense and limits of available technology. While the police have adopted many new technological advances over time, in the first 150 years of policing local police departments were simply not capable of constant and pervasive surveillance. Employing armies of officers to watch any particular person or persons all of the time is impracticable for ordinary police departments.[144] And the use of high-tech surveillance methods until recently has

---

[137] *Id.* at 10, 13–14.

[138] *See, e.g.*, Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 780 (6th Cir. 1983) ("The mere existence of a military data-gathering system does not constitute a justiciable controversy."); United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms."). *But see* White v. Davis, 13 Cal. 3d 757, 764–65 (1975) (permitting lawsuit against Los Angeles Police Department surveillance on state grounds and distinguishing *Laird*).

[139] Flowers v. City of Minneapolis, 558 F.3d 794, 798 (8th Cir. 2009) ("The State, of course, retains broad discretion to decide whom to prosecute for violating the criminal laws, and the State's discretion as to whom to investigate is similarly broad." (citing Wayte v. United States, 470 U.S. 598, 607 (1985))).

[140] 4 LaFave, Israel, King & Kerr, Criminal Procedure § 13.4(a) (3d ed. 2014) (stating elements as "(1) that other violators similarly situated are generally not prosecuted; (2) that the selection of the claimant was 'intentional or purposeful'; and (3) that the selection was pursuant to an 'arbitrary classification.' ").

[141] 517 U.S. 806, 819 (1996).

[142] 532 U.S. 318, 318 (2001).

[143] Pretextual policing refers to those enforcement actions justified by the police for one reason when they are actually motivated by another. Traffic law enforcement used to look for evidence of illegal drugs is one example. *See, e.g.*, Whren v. United States, 517 U.S. 806, 810–13 (1996).

[144] *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory,

been limited; what means existed have been prohibitively expensive for most local police departments. Thus, "as a practical matter, investigative agencies will rarely expend their limited manpower and resources on a mere whim . . . ."[145]

Second, the mere visibility of most traditional police practices provides a check on police behavior because an objecting public can monitor and sometimes call for change.[146] Most routine street policing is visible. Indeed, as recent national attention to several cases of people who have died in encounters with the police has shown, bystander videos have led to protests and calls for action with regard to excessive force.[147]

Thus, the Fourth Amendment is unlikely to be a useful choice to curb surveillance discretion. To be sure, judges and law professors have raised concerns that the Supreme Court's Fourth Amendment cases decided in the 1980s give insufficient protections to those whose movements and actions in public have been monitored by the police, particularly since that information in the aggregate can provide highly revealing information about one's religious beliefs, health conditions, political affiliations, and vices.[148] Thus, some have argued that police collection of large amounts of a person's "public" data should constitute a Fourth Amendment search even if the collection of each data point in isolation would not likely be considered a search. This "mosaic theory" of the Fourth Amendment may be helpful to defendants when the police single them out for particularized data collection.[149] As to whether big data analysis might provide a basis for individualized suspicion,

---

but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.").

[145] *See* United States v. Allibhai, 939 F.2d 244, 249 (5th Cir. 1991).

[146] *See, e.g.*, *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (noting "ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004))).

[147] *See* Editorial, *The Walter Scott Murder*, N.Y. TIMES (Apr. 8, 2015), http://www.nytimes.com/2015/04/09/opinion/the-walter-scott-murder.html [http://perma.cc/5BSE-HUBN] (noting fatal shooting of fleeing unarmed black man "would have passed into the annals of history unremarked upon had a bystander not used a cellphone to document what happened"); J. David Goodman, *Man Who Filmed Fatal Police Chokehold Is Arrested on Weapons Charges*, N.Y. TIMES (Aug. 3, 2014), http://www.nytimes.com/2014/08/04/nyregion/after-recording-eric-garner-chokehold-ramsey-orta-gets-charged-with-gun-possession.html [http://perma.cc/4LFN-4M8A] (describing "visceral cellphone images" that "helped galvanize protests and set off a citywide debate over police practices").

[148] Justice Sotomayor's concurring opinion in *Jones* illustrates the problem: "Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

[149] The theory first arose in the case of United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), which the Supreme Court later reviewed as *Jones*, 132 S. Ct. at 955. For a skeptical view of the mosaic theory, see Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

some commentators have already raised doubts as to whether the Fourth Amendment alone should regulate these determinations.[150]

But the Fourth Amendment's focus on individualized suspicion and its conceptualization of rights that better describe a physical rather than a digital world is likely a poor fit for expanded surveillance discretion. Certainly those at the receiving end of the increased scrutiny made possible by big data may complain that the police have insufficient justification. Yet when the police are sifting through the data of hundreds, thousands, or millions of people at the same time, we cannot expect the police to provide individualized suspicion before looking at a lone online post.

If big data is changing the *structure* of police discretion, then commensurate tools of accountability should focus on reining in these practices as a whole. Because all big data tools pose similar concerns, accountability measures should focus on policy outcomes rather than technology specific measures.[151]

B. The Secrecy Problem

Secrecy often accompanies the new surveillance discretion. Some of this secrecy can be attributed to the private companies providing the police with the software or data they use. Moreover, the police themselves tend to be secretive and insular in ways that inhibit external oversight. For these reasons, we often know little about the adoption or development of surveillance discretion.

First, big data tools are often private market products; police departments are just another group of customers. In a number of recent instances, private companies providing surveillance technology have required agreements from police departments that prevent disclosure of information about the technology itself.

For example, civil liberties organizations and journalists have discovered the police use of cell site simulators, a surveillance technology that tricks nearby cell phones into providing data by behaving as a fake mobile cell tower.[152] Detailed information about the use of these devices, sometimes referred to as "stingrays" or IMSI catchers, is difficult to find, however, because the dominant manufacturer of these devices, the Harris Corporation, has required participating law enforcement agencies to sign nondisclosure

---

[150] *See, e.g.*, Rich, *supra* note 7 (manuscript at 7) (arguing that "[Automated Suspicion Algorithm] accuracy cannot be regulated through the courts alone").

[151] *See* BIG DATA AND PRIVACY, *supra* note 30, at xiii ("To avoid falling behind the technology, it is essential that policy concerning privacy protection should address the purpose (the 'what') rather than prescribing the mechanism (the 'how').").

[152] As of April 2015, the American Civil Liberties Union has identified several federal agencies and fifty-seven agencies in twenty-two states and the District of Columbia that own or use stingrays. *See* ACLU, STINGRAY TRACKING DEVICES: WHO'S GOT THEM?, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them [http://perma.cc/5ZT9-WNDP].

agreements.[153] Nondisclosure agreements bar police departments adopting the technology from disclosing "any information"[154] relating to the surveillance equipment to any third parties, private and public.[155] Some prosecutors have even chosen to withdraw evidence in cases rather than be forced to disclose details about any possible use of this cellphone surveillance technology.[156] After several investigative reports on stingray use, the Department of Justice announced in September 2015 new rules that would apply to the use of cellphone surveillance technology by the Department of Justice, including a warrant requirement.[157]

Similarly, Vigilant, one of the country's largest ALPR companies, includes in its terms and conditions a requirement of its licensees (i.e., police departments) that they "agree not to voluntarily provide ANY information, including interviews, related to [Vigilant] products or its services to any member of the media without express written consent of [Vigilant]."[158] Little prevents other companies from imposing similar requirements as a condition of sale or use by police departments.

---

[153] *See* Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. TIMES (Mar. 15, 2015), http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html [http://perma.cc/7Y86-6N5C].

[154] The New York Civil Liberties Union in April 2015 published a nondisclosure agreement the FBI imposed upon the Erie County, New York, Sheriff's Office. The agreement includes a directive that the Sheriff's Office will "not distribute, disseminate, or otherwise disclose any information [regarding the stingray] to the public, including to any non-law enforcement individuals or agencies." Letter from Christopher M. Piehota, Special Agent in Charge, Buffalo Division, Fed. Bureau of Investigation, to Scott R. Patronik, Chief, Erie Cty. Sheriff's Office (June 29, 2012), http://www.nyclu.org/files/20120629-renondisclsure-obligations(Harris-ECSO).pdf [http://perma.cc/248A-2N88].

[155] *See* Kim Zetter, *Police Contract With Spy Tool Maker Prohibits Talking About Device's Use*, WIRED (Mar. 4, 2014), http://www.wired.com/2014/03/harris-stingray-nda/ [http://perma.cc/6MSX-7ACW]; Adam Lynn, *Defendant Challenges Use of Secret "Stingray" Cell Device*, NEWS TRIBUNE (Apr. 26, 2015), http://www.thenewstribune.com/news/local/crime/article26283343.html [http://perma.cc/7DEM-5V36] (reporting that Tacoma police "have refused to discuss publicly details of the Stingray, citing a nondisclosure agreement with the federal authorities who provided them with the tool").

[156] *See* Cyrus Farivar, *Prosecutors Drop Key Evidence at Trial to Avoid Explaining "Stingray" Use*, ARS TECHNICA (Nov. 18, 2014), http://arstechnica.com/tech-policy/2014/11/prosecutors-drop-key-evidence-at-trial-to-avoid-explaining-stingray-use/ [http://perma.cc/5B4E-AU9U] (reporting criminal case in Baltimore in which prosecutors withdrew evidence rather than provide information about suspected use of stingray surveillance); Robert Patrick, *St. Charles Woman Withdraws Guilty Plea in Case Linked to Secret FBI Cellphone Tracker*, ST. LOUIS POST-DISPATCH (Apr. 25, 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://perma.cc/9ADQ-CPCG] ("In some cities around the country, prosecutors have dropped cases rather than allow discussion of StingRay use.").

[157] Devlin Barrett, *Justice Department Changes Policy on Cellphone Surveillance*, WALL ST. J. (Sept. 3, 2015), http://www.wsj.com/articles/justice-department-changes-policy-on-cell phone-surveillance-1441314839 [http://perma.cc/94FF-PY72] (noting however that the rules do not apply to state or local police use of stingrays).

[158] Cyrus Farivar, *NYPD to Conduct "Virtual Stakeouts," Get Alerts on Wanted Cars Nationwide,* ARS TECHNICA (Mar. 2, 2015), http://arstechnica.com/tech-policy/2015/03/nypd-to-conduct-virtual-stakeouts-get-alerts-on-wanted-cars-nationwide/ [http://perma.cc/Q2ZL-KPNL].

Even without explicit nondisclosure agreements, big data tools can remain secret because they contain proprietary information that companies may be unwilling to release. Nor are private companies producing these tools subject to public records laws that would require them to divulge relevant and useful information.

Second, police departments have varied widely in their willingness to provide public access to their big data tools. The variation in ALPR policies is illustrative. As we saw with the police department of Oakland, California, the police agreed to provide journalists with their ALPR data. Other police departments, however, have resisted public records requests for ALPR data on the ground that *all* collected scans may be useful for investigations.[159]

C. Big Data Accountability

Transparency and accountability measures should be a first step to address some of the concerns raised by expanded surveillance discretion. This includes not only independent oversight measures familiar in traditional policing but also forms of "algorithmic accountability."[160] What should such accountability measures address?

Does it exist? Sometimes the most important question is whether the police have adopted a new surveillance technology at all. Local governments could require police departments to seek approval before the purchase of new technologies that expand surveillance capabilities. For instance, a surveillance notification ordinance passed in Seattle, Washington,[161] requires city council approval before any city department acquires "surveillance equipment."[162] The ordinance requires not only notification about a planned purchase of any surveillance equipment, but also a "mitigation plan describing how the department's use of the equipment will be regulated to protect privacy, anonymity, and limit the risk of potential abuse."[163] Public approval for new surveillance technology purchases could also include approval for

---

[159] The California Supreme Court in July 2015 granted review of a lawsuit filed by the Electronic Frontier Foundation (EFF) and the ACLU of Southern California in which they were denied public records requests for license plate reader data from the Los Angeles Police and Sheriff's Departments. *See* Jennifer Lynch, *EFF and ACLU Win Review of Automated License Plate Reader*, ELEC. FRONTIER FOUND. (July 29, 2015), https://www.eff.org/deeplinks/2015/07/eff-and-aclu-win-review-automated-license-plate-reader-case [http://perma.cc/4K5R-E8XF].

[160] Steve Lohr, *If Algorithms Know All, How Much Should Humans Help?*, N.Y. TIMES (Apr. 6, 2015), http://www.nytimes.com/2015/04/07/upshot/if-algorithms-know-all-how-much-should-humans-help.html [http://perma.cc/2JT5-BRJD].

[161] Cyrus Farivar, *New California Bill Would Require Local Approval for Stingray Use*, ARS TECHNICA (Apr. 16, 2015), http://arstechnica.com/tech-policy/2015/04/new-california-bill-would-require-local-approval-for-stingray-use/ [http://perma.cc/D6BF-TR8P].

[162] SEATTLE, WASH., ORDINANCE 124142 (Mar. 27, 2013), http://clerk.seattle.gov/~archives/Ordinances/Ord_124142.pdf [http://perma.cc/9WPL-MV98].

[163] *Id.*

third parties with whom police departments might contract for such services.[164]

Without such required disclosures, local governmental bodies may find out about technologies that significantly expand surveillance discretion only by accident or happenstance. In 2014, the city council of Bellingham, Washington, held a formal public hearing expressing alarm after news that its police department planned to purchase Intrado's *Beware* social media analysis software with a federal grant.[165] The Council urged its police department not to purchase *Beware*.[166] The police department withdrew its grant request after the city council voted to ask the department to do so.[167]

How is it being used? Securing public approval is only a first step. Local governments can take additional measures to ensure continuing public oversight of big data technologies that expand surveillance discretion. For example, local governments can require police departments to adopt "surveillance use policies" that specify how and when surveillance technologies might be used.[168]

Logging requirements can enable accountability by ensuring third parties can access and review how big data policing tools work. Local governments can provide independent third parties with responsibilities and powers to review how such programs work.[169] Auditors should be given access to both the technology and the data produced by it (e.g., access controls and audit logs).[170]

How accurate is it? With that knowledge, we can assess the nature of the raw information used by these computer algorithms. As we have seen, some kinds of information reflect highly discretionary decisions. Arrests are often the outcome of decision-making about enforcement priorities, law enforcement resources, and other contingencies. That a person is a known gang member is a contestable designation. Yet these factors may be used to justify further law enforcement attention, if not eventual detention or arrest.

---

[164] An ordinance passed in 2013 by the Spokane, Washington, City Council makes such explicit reference to third party relationships. *See* SPOKANE, WASH., ORDINANCE No. C-35018 (Aug. 28, 2013); Jamela Debelak, *Surveillance: Spokane Acts to Protect Privacy and Provide Transparency*, ACLU OF WASH. ST. (Aug. 21, 2013), https://aclu-wa.org/blog/surveillance-spokane-acts-protect-privacy-and-provide-transparency [http://perma.cc/UB2F-7LLU].

[165] Tim Johnson, *Intrado Intrusion: City Council Backs Away from Social Spyware*, CASCADIA WKLY. (July 9, 2014), http://www.cascadiaweekly.com/currents/intrado_intrusion [http://perma.cc/692V-ELRY].

[166] *See id.* Notably, however, the Council lacked the authority to block the grant or to direct its expenditure toward a different use.

[167] Dick Conoboy, *Intrado Not to Intrude in Bellingham*, NORTHWEST CITIZEN (July 8, 2014), http://www.nwcitizen.com/entry/intrado-not-to-intrude-in-bellingham [http://perma.cc/KEG9-PMCG].

[168] ACLU OF CALIFORNIA, MAKING SMART DECISIONS ABOUT SURVEILLANCE 15 (Nov. 2014), https://www.aclunc.org/sites/default/files/Smart%20About%20Surveillance.pdf [http://perma.cc/N2GN-VT44]. The guide provides a model local ordinance as well. *See id.* at 22–24.

[169] *See id.* at 19; Bambauer, *supra* note 12 (manuscript at 43) ("All uses of pattern-driven algorithms should be subjected to logging so that auditors and criminal defendants can review how the government has used its data mining programs.").

[170] ACLU, *supra* note 168 at 20.

How effective is it? When we know *whether* and *how* the police have adopted a big data tool to expand their surveillance discretion, we can assess whether such technologies are worth their financial, institutional, and social costs. For example, ALPR surveillance is touted as a quick, efficient, and cost-effective policing technology, but we often know little about how well the technology reduces crime. The available evidence suggests that comparatively few crimes are identified through mass plate collection. In Oakland, California, journalists reported that the "hit" rate of its ALPR use—when compared to the number of license plate scans captured—was a mere 0.16%.[171]

IV. Conclusion

The police have always possessed surveillance discretion. Big data promises to expand and accelerate their ability to discover crime and identify suspects. One day the ability to sort, score, and predict social activity will be an ordinary aspect of policing, in the same way we now experience entertainment, dating, and shopping.

Yet the use of big data in policing will be different because of its consequences. To be sure, big data policing may remedy some entrenched policing inequities. And it may heighten expectations about accountability. But enhancing the scope and power of the police to designate people as suspects will also further complicate longstanding concerns about discretion. Secrecy about these processes, moreover, can further alienate the public from the police. Because policing is a democratic institution and not just a technological enterprise, those concerns should trouble us.

[171] Cyrus Farivar (@cfarivar), Twitter (Mar. 24, 2014), https://twitter.com/cfarivar/status/580404313958301696 [https://perma.cc/69YP-7HTL].