Big Data Policing and the Redistribution of Anxiety

Kiel Brennan-Marquez*

I.

By equipping police with data, what are we trying to accomplish? Certain answers ring familiar. For one thing, we are trying to make criminal justice decisions, plagued as they often are by inaccuracy and bias, more refined.[1] For another, we are trying to boost the efficiency of governance institutions—police departments, prosecutor's offices, municipal courts—that operate under the pall of scarcity.

For the moment, I want to put answers like these to one side; not because they are wrong, but because they seem like only part of the story. *Another* goal of big data policing,[2] in addition to those just described, is to produce a social order—a surveillance society—in which people constantly monitor and curate the data-trails they leave behind in everyday life. The idea of self-monitoring in response to surveillance is not new. Data intensifies and extends this dynamic; it does not create the dynamic *ex nihilo*. But the fact remains: in both scale and scope, data surveillance today lacks meaningful precedent. We are fast approaching a world in which virtually everything one does at t_1—every movement one makes in public, every bond one forges on social media, every transaction one participates in—will be recorded and archived, becoming a potential foundation for adverse treatment at t_2.

Yes, there will continue to be limits on the ability of police to collect data, and yes, use-restrictions may be imposed, to greater or lesser practical effect, on data already in hand. But the endgame is not hard to see. Given enough sensors,

---

* Research Fellow & Adjunct Professor, Georgetown University Law Center. Associate Professor of Law, University of Connecticut, beginning August 2018. I would like to thank Ric Simmons for inviting me to participate in this splendid symposium, as well as the editors of the *Ohio State Journal of Criminal Law* for helping to get this essay into publishable shape.

[1] Numerous symposium papers touch on this theme. *See, e.g.*, Bennett Capers, *Techno-Policing*, 15 OHIO ST. J. CRIM. L. 495 (2018); Andrew Guthrie Ferguson, *Illuminating Black Data Policing*, 15 OHIO ST. J. CRIM. L. 503 (2018); Ravi Shroff, *Statistical Tests to Audit Investigative Stops*, 15 OHIO ST. J. CRIM. L. 565 (2018).

[2] Here, and throughout the essay, I am adopting Andrew Ferguson's phrase (and drawing inspiration from his work). *See* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017).

enough computational power, enough channels of data "insourcing,"[3] enough *time*, and traditional safeguards will run dry. Long term, we cannot hope to curb the psychological effects of totalizing data surveillance.[4]

Those effects are best conveyed, I think, by a label the Supreme Court itself recently adopted to describe information privacy harms: *anxiety*.[5] The organizing principle of a surveillance society like the one just described—the one we increasingly inhabit—is constant, low-level consternation about the way one's activity may be perceived by those in power. The paradigm, you could say, is that of a routine, not-yet-escalated traffic stop. As police enjoy access to more and more data, individuals will increasingly stand, at all times, in relation to the state the way someone who has been pulled over, awaiting a license-and-registration check, does: in a slight-but-taxing state of worry, cautiously hoping that everything will be fine. Or maybe the paradigm is slightly less dramatic: seeing a patrol car in your rear-view mirror and feeling your pulse quicken; awareness heightened and senses alert, as you try not to break any traffic rules. (Good luck.)

Cast in this light, the distinctive feature of big data policing—beyond its statistical promise—is that it multiplies, both quantitatively and qualitatively, the experience of being subject to "police presence." Once all of life is documented and databased, once officials can make use (in Stephen Henderson's words) of "time machines,"[6] officers no longer need to be investigating contemporaneously, let alone physically present, to inspire self-monitoring and behavior modification. The logic here is essentially panoptic: a technologically-updated version of Bentham's idealized prison. Even if no guards currently occupy in the central tower, even if no guards *ever* occupy the central tower, so long as each cell is fitted with sensors that record all aspects of the daily life and the records are always available for review—a rough analogy to totalizing data surveillance—the disciplining effects will be the same. In many ways, this simple insight is the

---

[3] *See* Kimberly N. Brown, *Outsourcing, Data Insourcing, and the Irrelevant Constitution*, 49 GA. L. REV. 607 (2015) (examining the ways in which outsourcing of government functions, paired with "data insourcing" by state agencies, permits the circumvention of various regulatory mechanisms, including constitutional rules). *See also* Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 KAN. L. REV. 485 (2018) (exploring similar themes).

[4] *See, e.g.*, Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1348 (2012) (arguing that we are fast approaching a future in which law enforcement is "awash in probable cause" and the possibility of police intrusion is constant and universal).

[5] *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2178 (2016) (holding that police must obtain a warrant before performing a blood test pursuant to a DUI arrest, because more information than BAC can be extracted from blood samples, which "may result in anxiety for the person tested"); Kiel Brennan-Marquez & Stephen E. Henderson, *Fourth Amendment Anxiety*, 55 AM. CRIM. L. REV. 1 (2018) (unpacking the implications of *Birchfield*).

[6] *See* Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933 (2016).

foundation of predictive policing. By directing officer attention to areas where crime has been forecast as likely, the hypothesis is that we can deter wrongdoing before it occurs. And preliminary empirics seem to bear the hypothesis out.[7]

To be clear, I am not saying that data surveillance is liable to make every person feel, at every moment, exactly as they would when being directly monitored by police. The point is that the two *forms* of experience—and of self-monitoring that plausibly results from those experiences—are comparable. They occupy the same spectrum.

II.

All this may sound grim, even fatalistic. But not so fast. Anxiety has many benefits. It can be a wellspring of virtuous behavior—or short of that, at least compliant behavior. The reality is that we *want* people to worry about breaking the rules; just not so much that it spills over into other domains of life, hobbling autonomy—what we say, think, and do—and frustrating democratic participation.[8]

How exactly to strike this balance is, of course, a complex and controversial question. For present purposes, the point is simply that low-level anxiety—as a result of data-driven law enforcement—may not be such a bad thing, especially if it trades off against the not-so-low-level anxiety that accompanies (1) traditional policing, as well as (2) the *absence* of police.[9] And the point is not just quantitative. Not only does big data policing stand to rein in certain pathologies of law enforcement; it promises—at least in principle—to do so in progressive ways. In other words, the anxiety produced by big data policing has the capacity to be *redistributive*: to impose a small burden on a large swath of the population instead of imposing an outsized burden on specific communities where law enforcement harms have traditionally run rampant.

Of course, I'm painting a consciously abstract—and idealized—picture. Data-driven solutions are not inherently more progressive (in a distributional sense) than their traditional counterparts. If anything, the practical tendency is often the opposite.[10] The point is simply that data-driven anxiety plausibly *could* be more equally dispersed than the anxiety wrought by traditional policing. And as

---

[7] *See, e.g.*, Samantha Melamed, *Can Atlantic City's Bold Experiment Take Racial Bias Out of Predictive Policing?*, PHILA. INQUIRER (Aug. 10, 2017, 5:03 AM), http://www.philly.com/philly/news/crime/atlantic-city-risk-terrain-modeling-rutgers-predictive-policing-joel-caplan-20170810.html [https://perma.cc/H8MX-MVVB].

[8] For a fuller discussion of these kinds of chilling effects as the central risk of data-driven law enforcement, see Brennan-Marquez, *supra* note 3.

[9] Among criminal justice reformers, it has long been a maxim that in many places, the only thing worse than too much policing is too little.

[10] *See, e.g.*, Ferguson, *supra* note 1.

scholars, advocates, and judges craft doctrinal responses to big data policing, it should be with its redistributive potential in mind.

Specifically, there are (at least) two forms of "anxiety redistribution" that big data policing might accomplish. The first is to curb false-positives, which could occur in numerous ways. For one thing, data can discourage police from relying on bias, conscious or unconscious, to guide their decisions. To borrow an example from Bennett Capers, "the increased use of public surveillance cameras and facial recognition technology, coupled with access to Big Data and perhaps terahertz scanners capable of distance scanning for firearms, could do much [to] tackl[e] the . . . problem [of] racialized policing,"[11] and disrupt the "young plus black equals probable cause" equation that stands a shameful hallmark of much contemporary policing.[12] For another thing, data analysis might facilitate changes in the allocation of police resources (say, where officers are dispatched for patrol) or the adoption of police tactics, based on historical crime patterns and efficacy rates.

The second form of "anxiety redistribution" is even simpler: big data tactics could displace older policing methods and/or preempt more crime. As police rely more on data, they may rely *less* on intrusive tactics like stop and frisk, or relatedly, they may find more efficient ways to deter low-level crime—or both.

To reiterate: *nothing about the logic or practice of data-driven law enforcement makes these redistributive impulses necessary*. On the contrary, they will be hard fought—and particularly in our current political climate, unlikely. In an ideal world, however, they would be the lodestar of academic and judicial efforts toward reform.

III.

Ultimately, then, the question is how best to manage the anxiety that accompanies big data policing—how to capitalize on its capacity both to deter crime and to displace more intrusive forms of police work, while keeping its darker externalities at bay. This, needless to say, is an enormous question. For now, I wish simply to call attention to one aspect of existing Fourth Amendment law that is plainly *not* up to the task: the idea that suspicion benchmarks will suffice, in the future, to limit police discretion.

Although this danger has not been lost on commentators,[13] I fear its gravity has been undersold. The problem is not merely, as scholars like Andrew Ferguson

---

[11] Capers, *supra* note 1, at 497.

[12] *Id.* (citing Elizabeth A. Gaynes, *The Urban Criminal Justice System: Where Young + Black + Male = Probable Cause*, 20 FORDHAM URB. L.J. 621 (1992)).

[13] *See, e.g.*, Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015); Ohm, *supra* note 4.

(rightly) note,[14] that in a data-rich world reasonable suspicion and probable cause will be much easier, perhaps even trivially easy, to satisfy. The problem is that, going forward, even near-perfect *knowledge* of wrongdoing may not be enough to justify intrusion. If the Fourth Amendment's purpose is to constrain the functional discretion that state officials enjoy when enforcing the law—and there is ample evidence to support this proposition[15]—big data policing may demand full-blown overhaul, not just reform.

Why? Because historically, Fourth Amendment doctrine has been able to rely on a natural synergy between (1) suspicion benchmarks, which require police to be able to explain their targeting decisions *ex ante*, and (2) anti-discretion principles. Demanding the former—requiring the police to build a "mini-case" in advance of intrusion—effectively vindicated the latter. Today, however, this synergy is poised to unravel. In a data-rich world, the police will soon find themselves (to borrow a phrase from Paul Ohm) "awash in probable cause,"[16] and the question should be whether they can justify their investigative activity on freestanding "reasonableness" grounds.[17] Furthermore, the problem cannot be solved by simply ratcheting up the amount of suspicion required to establish probable cause (or, depending on the setting, reasonable suspicion). That approach, though laudable, and perhaps appealing on incrementalist grounds, would ultimately just delay the inevitable. Eventually, we will have to confront the question of what requirements the Fourth Amendment's "reasonableness" mandate imposes *on top of* traditional suspicion benchmarks.

At risk of belaboring the point, consider a hypothetical. Suppose the NYPD develops a tool called the Pot Detector, which allows officers to stand outside a townhouse or apartment building, point the device toward the specific unit, and obtain a hyper-precise prediction ("yes" / "no") of whether the unit contains at least some amount of marijuana.[18] In other words, the Pot Detector operates like a

---

[14] *See* Ferguson, *supra* note 13.

[15] *See* Kiel Brennan-Marquez, *"Plausible Cause": Explanatory Standards in the Age of Powerful Machines*, 70 VAND. L. REV. 1249, 1288–95 (2017).

[16] Ohm, *supra* note 4.

[17] For an analysis that touches on the theme of reasonableness above and beyond probable cause, see Josh Bowers, *Probable Cause, Constitutional Reasonableness, and the Unrecognized Point of a "Pointless Dignity,"* 66 STAN. L. REV. 987, 995 (2014) (arguing for "a hybridized—or two-ply—reasonableness test, whereby an arrest must be supported by *both* probable cause *and* general reasonableness").

[18] *Cf.* JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES AND PERSPECTIVES 43 (5th ed. 2012) (imagining a "'radar' gun" that "can be tuned so that it will *only* signal the existence of substances that cannot be legally possessed under federal law" and exploring the issues this kind of device would raise). *See also* United States v. Jacobsen, 466 U.S. 109, 138 (1984) (Brennan, J., dissenting) ("[U]nder the Court's analysis . . . if a device were developed that, when aimed at a person, would detect instantaneously whether the person is carrying

radar gun; homing in on marijuana, it yields the correct prediction in virtually every case. The question is: should a "yes" output from the Pot Detector suffice to warrant a search of the unit? Traditionally, the answer would clearly be affirmative. The police all but *know* the unit contains pot. Surely that is sufficient—indeed, beyond sufficient—to establish probable cause.[19]

Yet imagine the discretion this would give police! The NYPD would be effectively free to choose among all residences flagged "yes" on the Pot Detector, and perform intrusive searches wherever they wanted. Maybe—hopefully—they would wield this power responsibly. But the whole point of the Fourth Amendment is that police are not allowed to wield power unsupervised; courts must be involved. And to the extent that technologies like the Pot Detector (or its real-world, algorithmic equivalent) allow police to bypass judicial supervision, they should be cause for constitutional concern.

I realize the Pot Detector is hyperbolic and reductive. But that's the point. As a thought-experiment, it underscores a limitation of using suspicion benchmarks like "probable cause" as tools for constraining law enforcement power. The premise of this approach is that *police operate from a default position of ignorance about crime*, from which it follows that requiring police to devise *ex ante* suspicion will circumscribe their power. But as the premise falters, so does the conclusion.

IV.

In a brilliant and provocative essay published under this very masthead a few years back, Paul Butler argued that stop and frisk programs are best understood by

---

cocaine, there would be no Fourth Amendment bar, under the Court's approach, to the police setting up such a device on a street corner and scanning all passersby. In fact, the Court's analysis is so unbounded that if a device were developed that could detect, from the outside of a building, the presence of cocaine inside, there would be no constitutional obstacle to the police cruising through a residential neighborhood and using the device to identify all homes in which the drug is present."). Note that I am putting to one side the question of whether using the Pot Detector would qualify as a search under *Kyllo v. United States*, 533 U.S. 27 (2001). I happen to think it does not, when *Kyllo* is synthesized with the so-called "binary search" doctrine—suggesting that detection methods that disclose only contraband do not qualify, in the first instance, as searches—on most prominent display in the dog sniff cases. In other words, the *Kyllo* rule would not apply (or at the very least, apply for different reasons than those articulated in *Kyllo*) if the "technological enhancement" in question were precisely-tailored to contraband. Either way, the point is that we can imagine at least *some* methods of "perfect detection" that (1) don't trigger *Kyllo* and (2) raise the concerns about discretion that I'm flagging here.

[19] Things get a little more complicated (1) if the output comes in the form of a conditional probability rather than a binary determination, and/or (2) if the false-positive rate is high enough that an output no longer seems to establish near-knowledge. Some of these questions are explored in Brennan-Marquez, *supra* note 15, but I put them to one side here.

analogy to torture and terror.[20] According to Butler, by detaining and harassing people in public (more often than not, men of color), police assert a form of control—a reminder of "who is in charge, and the violent consequences of dissent"[21]—similar to low-level torture practices, such as sleep deprivation.[22] And the result, in the aggregate, is a climate of fear and paralysis not unlike that of a community perpetually under siege by threats of terrorism.

Whether or not one agrees with Butler's claim, the exercise his essay instantiates and invites—drawing out the implications of extant law enforcement practices by reference to the ghastlier modes of social control they resemble—is quite fruitful. The difference between anxiety, on one hand, and torture and terror, on the other, is that anxiety can coexist, in principle, with liberal democracy, whereas torture and terror cannot. Accordingly, where the implication of Butler's analysis is that stop and frisk programs should be abolished, the implication of my analysis is not that big data policing must be abandoned. Rather, it's that regulation of big data policing must vindicate the Fourth Amendment's core promise: that citizens should be allowed to carry on with their lives, free from undue anxiety about arbitrary intervention by the state.

Historically, this promise has often lain fallow. Fourth Amendment doctrine has frequently served to justify police practices that are sloppy at best—and at worst, far worse. Big data holds out the possibility of something better. But to realize that possibility, we need legal rules that cause data to curtail, rather than exacerbate, the traditional pathologies of policing. The fear, of course, is they will do just the opposite.

---

[20] Paul Butler, *Stop and Frisk and Torture-Lite: Police Terror of Minority Communities*, 12 OHIO ST. J. CRIM. L. 57, 57–58 (2014).

[21] *Id.* at 69.

[22] *Id.* at 61.