3-2024

Filtered Dragnets and the Anti-Authoritarian Fourth Amendment

Jane R. Bambauer

FILTERED DRAGNETS AND THE ANTI-AUTHORITARIAN FOURTH AMENDMENT

JANE R. BAMBAUER*

ABSTRACT

Filtered dragnets are digital searches that identify a suspect based on the details of a crime. They can be designed to withhold information from law enforcement unless and until there is a very high probability that the individual has committed the offense. Examples today include DNA matching, facial recognition from photographs or video of a crime, automated child sexual abuse material detection, and reverse geolocation (geofence) searches. More are sure to come, and their wide-scale use will be irresistible to improve the low rates of criminal detection that currently afflict many communities.

However, filtered dragnets imperil society precisely because they detect crime too well. Sudden increases in the detection of criminal conduct will intensify the pathologies of American criminal justice: namely, that too many marginally harmful acts are criminalized, crimes are punished too harshly, and police and prosecutors have too much discretion. If nearly everybody commits some technical violation of criminal law that can be easily detected and harshly punished, all Americans will be at the mercy of the constable's pity.

These threats are not well constrained by current Fourth Amendment jurisprudence, based on privacy rights, because filtered dragnets detect crime without revealing irrelevant details. Thus, Fourth Amendment theory and doctrine must strengthen the anti-authoritarian objectives endowed in

* University of Arizona James E. Rogers College of Law. The author is grateful for the advice and invaluable feedback from Jordan Blair Woods, Tracey Maclin, Farhang Heydari, Toni Massaro, Tammi Walker, John Villasenor, Andrew Woods, Lilla Montagnani, Kiel Brennan-Marquez, Jeffrey Fagan, Christopher Slobogin, Derek Bambauer, Mark Verstraete, Xiaoqian Hu, Andrew Coan, Niva Elkin-Koren, Uri Hcohen, and Tal Zarsky.

its roots. A search conducted with a filtered dragnet should be considered reasonable only if it is administered in an evenhanded manner, and a subsequent seizure of a person is reasonable only when the misconduct is abhorrent enough to justify arrest and imprisonment.

TABLE OF CONTENTS

INTRODUCTION

Nearly forty years ago, Justice Brennan asked his colleagues, who had just given a constitutional stamp of approval to the drug-sniffing dog, to imagine a device "that, when aimed at a person, would detect instantaneously whether the person is carrying cocaine."[1] If the device could detect the

1. United States v. Jacobsen, 466 U.S. 109, 138 (1984) (Brennan, J., dissenting). Justice Brennan went on to criticize the majority for ignoring not only the privacy interest that is intruded upon, but also the accuracy of the technique (or lack thereof) and "whether the surveillance technique is employed randomly or selectively." *Id.* at 140.

presence of cocaine inside a building, "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."[2] He believed the prospect of police having a tool of near-perfect detection presented a catastrophic threat that the courts have a duty to stop.

We are not too far off from this scenario anymore,[3] and some strategies already in use by law enforcement and intelligence agencies are similar to Brennan's machine. Examples include DNA matching, facial recognition from photographs or video of a crime when it was in progress, automated child sexual abuse material detection, and reverse digital searches (where police use information known about the crime, such as location, timing, or special instrumentalities, to cross-check against service provider data in order to identify a suspect). Many more of these investigative techniques are sure to come, especially if or when the Internet of Things reaches its potential by placing increasingly powerful sensors on nearly every machine.

Twenty-first century policing will increasingly use data collected from tracking and sensing technologies to conduct investigations that work backwards. Law enforcement will use the particulars of a crime as a "fingerprint," so to speak, to determine who should belong in the pool of suspects. Unlike the standard dragnet, which permits law enforcement to observe large amounts of data and to choose their targets, *filtered* dragnets force investigations to focus on the evidence of a crime. Computers will automatically scan through data without exposing it and will make a disclosure only when there is probable cause to believe that a person's data matches the signature of the crime. Moreover, even when data is disclosed, filtered dragnet programs can be designed so that the only data revealed is potentially relevant data; extraneous details can be withheld.

When surveillance technologies meet all these benchmarks—that is, when (1) they are used to find an individual related to a crime (rather than to find a crime related to an individual), (2) when they report details from an otherwise private database only after meeting a high threshold of confidence (e.g., probable cause or higher), and (3) when they withhold details that are *ex ante* unlikely to be relevant to the current criminal investigation, the

2. *Id.* at 138. For a thoughtful discussion of this dissenting opinion, see Kiel Brennan-Marquez, *Big Data Policing and the Redistribution of Anxiety*, 15 OHIO STATE J. CRIM. L. 487, 491–92 (2018).

3. With the exception of conduct that takes place on the Internet and the geolocation of smart devices, the vast majority of human affairs still occurs outside the realm of digitized documentation. That said, sensor technologies, facial recognition, and biometric surveillance are beginning to convert more offline activities into tracked or trackable affairs. Perhaps the technology in development that is most analogous to Justice Brennan's cocaine device are quantum magnetometry sensors that are sensitive enough to detect materials through walls and underground. *See* CHRIS JAY HOOFNAGLE & SIMSON L. GARFINKEL, LAW AND POLICY FOR THE QUANTUM AGE 31–76 (2022).

nature of that surveillance is different from other types of police work. Filtered dragnets, as I will call them, are structured to avoid many problems traditionally associated with mass surveillance.

Fourth Amendment theory and reasoning is just starting to find its legs in digital search cases,[4] but filtered dragnets will destabilize criminal procedure law again. They will whittle down most of the privacy rationales for Fourth Amendment protection. Mounting a Fourth Amendment defense will require a litigant to convincingly argue that even though the defendant very likely committed a crime, and even though the police did not see or have discretionary access to data for any other persons and did not even have irrelevant data about the defendant for that matter, the search was nevertheless unreasonable. That sort of privacy *über alles* argument might work for crimes of questionable legitimacy—drug possession, for example—but it won't work in the context of universally reviled conduct like murder.

What is more, filtered dragnets may reduce privacy intrusions on net, as compared with current investigation techniques, because they can remove many people from the scope of suspicion who would otherwise become targets of investigation. In other words, filtered dragnets break the privacy-security trade-off because they simultaneously increase criminal detection *and* privacy. As Bennet Capers has explained, they may be a useful tool to simultaneously tackle under-protection *and* over-policing problems.[5] Outright bans of these technologies, as have been advocated in many corners,[6] would be irresponsible.[7]

4. *See* Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018) (accessing several days' worth of geolocation data constitutes a search that will ordinarily require a warrant); United States v. Jones, 565 U.S. 400, 413–15 (2012) (Sotomayor, J., concurring) (arguing that GPS tracking should be a search irrespective of whether a tracking device has physically intruded into a protected area).

5. I. Bennett Capers, *Techno-Policing*, 15 OHIO STATE J. CRIM. L. 495, 496 (2018) ("The task is to reimagine Big Brother so that he not only watches us; he also watches over us—to reimagine Big Brother as protective, and as someone who will be there to tell our side of the story."); I. Bennett Capers, *Crime, Surveillance, and Communities*, 40 FORDHAM URB. L.J. 959, 989 (2013). For a discussion of the moral injuries when police cause indignities and abuse, see Eric J. Miller, *The Moral Burdens of Police Wrongdoing*, 97 RES PHILOSOPHICA (2020).

6. *See, e.g.*, Antoaneta Roussi, *Resisting the Rise of Facial Recognition*, 587 NATURE 350, 352 (2020) (quoting Woodrow Hartzog, who described facial recognition technology as the "most dangerous ever to be invented"); Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-sanfrancisco [https://perma.cc/858W-&M6N] (quoting ACLU attorney Matt Cagle, praising the ban as "forward-looking and looks to prevent the unleashing of this dangerous technology against the public"); Matthew Guariglia, *Geofence Warrants and Reverse Keyword Warrants Are So Invasive, Even Big Tech Wants to Ban Them*, ELEC. FRONTIER FOUND. (May 13, 2022), https://www.eff.org/deeplinks/2022/05/geofence-warrants-and-reverse-keyword-warrants-are-so-invasive-even-big-tech-wants [https://perma.cc/VG22-ENMH].

7. Undeterred crime is oppressive and unequal, too. JAMES FORMAN JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA 96–99 (2018); Alexandra Natapoff, *Underenforcement*, 75

Nevertheless, even if filtered dragnets detect crime and nothing else, they pose serious social risks that Fourth Amendment law and scholarship are ill equipped to handle: What happens to Fourth Amendment theory and the practice of criminal justice if nearly every crime could be detected?

In the late 1990s, Larry Lessig asked this very question.[8] He anticipated that digital technologies may create a wedge between the privacy and anti-authoritarian rationales for criminal procedure. But most Fourth Amendment scholars do not even recognize a schism between privacy and anti-authoritarian goals. Instead, they continue to focus on privacy as the key constraint on any police activity that leverages large amounts of personal data. The scholars who have recognized liberty and anti-authoritarianism as a Fourth Amendment lodestar have insisted that all technology-assisted surveillance is a tool of abusive state power *per se*.[9] As a result, Fourth Amendment scholars lump filtered dragnets with all other surveillance and advocate for the strictest access controls, guaranteeing the continuation of a low rate of criminal detection.

This is the wrong course. The threat from filtered dragnets is tyranny, and the Fourth Amendment will be more effective and coherent if we recognize that. Filtered dragnets will dramatically increase the detection of crime, and this will intensify existing pathologies in American criminal justice that have little to do with privacy. Namely, we have too many crimes, too much punishment, and too much police and prosecutorial discretion. These problems jointly produce the risk of authoritarian power. An overly expansive criminal code paired with harsh penalties ensures that nearly everybody could be subjected to incarceration.[10] When the state also has

FORDHAM L. REV. 1715, 1715 (2006).

8. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 18 (1999) ("This difference complicates the constitutional question. The [technology's] behavior is like a generalized search in that it is a search without suspicion, but it is unlike the paradigm case of a generalized search in that it creates no disruption of ordinary life and finds only contraband. . . . Is [it] constitutional? That depends on your conception of what the Fourth Amendment protects. . . . The paradigm case cited by the framers does not distinguish between these two very different protections. It is *we*, instead, who must choose.").

9. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L. J. 1309, 1334–38, 1346 (declaring that considerations of power seem to be "the amendment's essence, not merely a proxy for something deeper," but then equating abuses of state power with the ability to solve crimes faster); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1120 (2014) (advocating for Fourth Amendment protection against any electronic surveillance that fails to leave a sphere of refuge or autonomy for the individual); Andrew Guthrie Ferguson, *Surveillance and the Tyrant Test*, 110 GEORGETOWN L. J. 205, 266 (2021). *But see* Richard M. Re, *Imagining Perfect Surveillance*, 64 UCLA L. REV. DISCOURSE 264, 274–276, 281–285 (2016). Re's essay, set in the year 2026 and describing a fictitious tool of perfect surveillance and crime reporting, anticipates the need for courts to shift the focus of Fourth Amendment law to the substance of criminal law.

10. Glenn Harlan Reynolds, *Ham Sandwich Nation: Due Process When Everything Is a Crime*, 113 COLUM. L. REV. SIDEBAR 102, 103–04 (2013). *See generally* HARVEY A. SILVERGATE, THREE FELONIES A DAY: HOW THE FEDS TARGET THE INNOCENT (2011).

unchecked power to choose where and when to investigate within the ocean of criminal-but-typically-ignored conduct, the populace is at the mercy of the state's will.[11]

Today, the criminal justice equilibrium rests on an unspoken compromise. The state has broad substantive law, harsh punishment, and unchecked discretion, it is true, but the populace has privacy rights that nearly guarantee low detection, even when police are highly motivated. When filtered dragnets give police near-perfect detection, the bargain has to be renegotiated.

This Article proposes a new grand bargain for Fourth Amendment law: the Supreme Court should recognize filtered dragnets as a legitimate and even desirable tool for criminal investigations. But constitutional rules should guarantee that the substance of American criminal law will be limited to conduct that is commonly recognized as heinous, that the severity of the punishment fits the reprehensibility of the crime, and that the enforcement of criminal laws is equitable and nonarbitrary.[12] Without *these* civil rights, if the substance of criminal law is left as broad and vague as it is today,[13] and if penalties and the impact of prison are as debilitating as they are now, filtered dragnets would give the government the means of exercising tyrannical control through the omnipresent threat of criminal enforcement and the power of discretionary clemency.

This Article proceeds as follows: Part I describes some filtered dragnets that are already in use and lays out the essential features that distinguish them from other investigation tools.

Part II describes the potential social benefits that can be gained from the responsible use of filtered dragnets.

Part III describes the scholarship and caselaw challenging the constitutionality of filtered dragnets on privacy grounds and disagrees with it. By most common-sense meanings of privacy, filtered dragnets are in fact *much more* private than the sorts of investigations that routinely occur.

11. Filtered dragnets, like any tool that cheaply and accurately finds evidence of crime, will not necessarily *cause* the state to abuse its power, but it will certainly give legislatures, police, and prosecutors a mechanism to abuse power more efficiently if they so choose.

12. In other words, as described in detail *infra* Part III, reversing *Smith v. Maryland*, 442 U.S. 735 (1979) and the third party doctrine will be of minimal relevance to the just use of filtered dragnets. Instead, cases that permit carceral arrest for minor misconduct (*Atwater v. City of Lago Vista*, 532 U.S. 318 (2001)) and that give police unfettered discretion in investigation and enforcement decisions (*Whren v. United States*, 517 U.S. 806 (1996)) are of much greater consequence. *See infra* Part V.

13. On vagueness and overbreadth, see SILVERGATE, *supra* note 10, at XI–XVI. *See generally* RISA GOLUBOFF, VAGRANT NATION (2016); Kiel Brennan-Marquez, *Extremely Broad Laws*, 61 ARIZ. L. REV. 641 (2019).

Part IV shows that the threat of filtered dragnets comes not in the form of privacy but in the form of tyranny. Perfect detection of crime in a system where criminal statutes are sprawling and criminal penalties are harsh will either create a country of convicts or will give government too much power to engage in selective leniency.

Part V reinterprets the Fourth Amendment prohibition of unreasonable searches and seizures to fit the criminal justice problems that emerging surveillance technologies will cause. The reasonableness of a seizure should depend on whether the defendant's conduct truly warrants criminal liability and penalties. The reasonableness of a search should depend on both expectations of privacy *and* on evenhanded investigation practices.

Part VI explains why the Constitution, and the Fourth Amendment in particular, are well suited to carry out this shift even though it would mark a departure from twentieth century precedent.

The agenda laid out in this Article is ambitious—almost embarrassingly so. What I propose here would require a seismic shift in Fourth Amendment principles that would cross the procedural/substantive divide.[14] Given that, I take comfort in the fact that I am not painting on blank canvas. This project is a remix of themes developed by Bill Stuntz,[15] Bennett Capers,[16] Elizabeth Joh,[17] Bernard Harcourt and Tracey Meares,[18] Chris Slobogin,[19] Mark Kleiman,[20] and many others. Even so, it is awfully presumptuous to suggest courts might start invalidating criminal laws or sentencing rules using a new-fangled conception of the Fourth Amendment. But I will suggest it anyway because it is the only desirable and realistic option. The criminal justice system needs to be transformed in a manner that accepts much greater levels of detection in exchange for many fewer criminal prohibitions and punishments. It is a trade that has to be executed simultaneously in order to

14. Other scholars have advocated for a Fourth Amendment theoretical inquiry that breaks out of a purely procedural lane. Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 200 (1993) ("The fragmentation of constitutional theory in law school curricula and academic scholarship is nowhere more evident than in the isolation of the fourth amendment from broad currents of contemporary jurisprudence. . . . This isolation has impoverished both fourth amendment theory and general constitutional theory alike."); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 393–411 (1995).

15. WILLIAM J. STUNTZ, THE COLLAPSE OF AMERICAN CRIMINAL JUSTICE (2011).

16. Capers, *supra* note 5.

17. Elizabeth E. Joh, *Discretionless Policing: Technology and the Fourth Amendment*, 95 CALIF. L. REV. 199 (2007).

18. Bernard E. Harcourt & Tracey L. Meares, *Randomization and the Fourth Amendment*, 78 U. CHI. L. REV. 809 (2011).

19. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008).

20. MARK A. R. KLEIMAN, WHEN BRUTE FORCE FAILS (2009).

avoid disastrous consequences.[21] No legislative or local government process could pull off a massive rights horse trade of the sort that is required. It can only be accomplished through the style of landmark constitutional cases that, every generation or so, help realign Fourth Amendment operational rules with the ultimate purpose of Fourth Amendment protection.[22]

I. WHAT ARE FILTERED DRAGNETS?

The progenitors of filtered dragnets have been around for a while. Fingerprinting analysis is a well-known and time-honored method of backwards investigation where the facts from the scene of a crime (the fingerprint markings) are cross-checked against a large stockpile of information in order to make a fairly confident match to a particular suspect.[23] Police dogs are another example.[24] We know that the mind-boggling sensitivity of a dog's nose is such that, if it could talk, it could reveal vast amounts of information about a person—what is inside their bag, how their health is, whether they've been in recent contact with other people—that are unobservable to we mere humans. In some sense, the mind of a police dog is a treasure trove of personal information that remains inaccessible to police most of the time. But when they are trained to alert to contraband or to specific scents sampled from a crime scene, the dog and the training combine to create a "binary search"—a mechanism that tells the police nothing unless there is probable cause that a crime is being committed.[25]

These crime-driven, quasi-filtered investigations are the outliers in a system of police investigation that relies much more heavily on witnesses, confessions, and physical searches.[26] But we can expect the practice to rapidly expand because of the greater amounts and variability of data available for cross-checking the facts of a crime against data from the population of potential suspects.

21. Criminal liability and sentencing cannot be reduced unless and until the detection of serious crimes is improved. Otherwise, the inevitable crime wave will turn on the backlash machinery of increased sentences and bloated criminal codes. On the other hand, unleashing filtered dragnet technologies without fixing existing statutes and sentences will expose many more people to criminal liability than is justified and will create too many opportunities for biased or opportunistic enforcement. *See infra* Part V.

22. I am referring here to the transition the Fourth Amendment made from a protection of property interests to a protection of privacy following *Katz v. United States*, 389 U.S. 347 (1967). See discussion *infra* Part V.

23. Davis v. Mississippi, 394 U.S. 721, 727 (1969).

24. Illinois v. Caballes, 543 U.S. 405, 409 (2005).

25. Jane Bambauer, *Defending the Dog*, 91 ORE. L. REV. 1203, 1203 (2013).

26. Throughout this article, I will distinguish suspect-driven investigations from crime-driven searches. *See* Slobogin, *supra* note 19, at 322–23 (using the term "event-driven"); Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 208 (2015) (using the term "crime-out").

This Part lays out the two required features of filtered dragnets that will cause an unprecedented shock to Fourth Amendment theory. We will then visit examples of techniques that are already in use that either already satisfy the definition of filtered dragnets or soon will.

A. REQUIRED ELEMENTS TO QUALIFY AS A FILTERED DRAGNET

Filtered dragnets provide a suspect's data to police only if (a) their data matches uniquely criminal details such that there is a high probability they have engaged in criminal conduct; and (b) their data has been pared down to provide only relevant details about the suspected crime to the police. When combined, these features make filtered dragnets a qualitatively different style of police investigation.[27]

1. Automated Matching of Uniquely Criminal Details

Filtered dragnet investigations will trawl through and process large amounts of data. There is no doubt that they are a dragnet. But to qualify as a filtered dragnet, the *filter* of the dragnet must constrain the system's ability to leak information. A filtered dragnet must be programmed to alert police only if an individual's data matches a unique fingerprint of a crime.[28] In other words, the system blinds the police until at least probable cause (and hopefully more suspicion) is established.

Filtered dragnets are a subset of the category of investigations that Christopher Slobogin calls "suspectless searches."[29] But they are a narrow subset. Very few of the suspectless searches that Slobogin analyzes (many of which I describe below) have the potential to become filtered dragnets. As they are practiced today, they will not meet the heightened standards for filtered dragnets because they do not use *unique* signatures of criminal behavior. For example, geofencing and familial DNA-matching procedures often allow police today to access data about a handful of individuals, all but one of whom are necessarily innocent, in order to help the police create leads for traditional follow-up investigation. To find the Golden State Killer, the FBI found a genetic match to a family member, and then used traditional

27. Jack Balkin bristles when scholars describe "essential features" of a technology. Jack B. Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. CIR. 45, 45 (2015). Suffice it to say that I am defining here a techno-social application of data collection and processing. The same technology can be used in other ways, of course, but then those uses would not meet my definition of a "filtered dragnet."

28. David H. Kaye, *Identification, Individualization and Uniqueness: What's the Difference?*, 8 L. PROBABILITY & RISK 85, 92 (2009).

29. Christopher Slobogin, *Suspectless Searches*, 83 OHIO STATE L.J. 953, 954 (2022) [hereinafter Slobogin, *Suspectless Searches*]; *see* CHRISTOPHER SLOBOGIN, VIRTUAL SEARCHES 127–48 (2022) [hereinafter SLOBOGIN, VIRTUAL SEARCHES]. Slobogin describes many of the same techniques that I do here, but his analysis has less futurism and is more interested in the way the Fourth Amendment should handle suspectless searches right now, when many cannot or do not match to uniquely criminal profiles.

genealogy to trace from that family member to the suspect.[30] The revelation of that family member's identity would not qualify as matching to "uniquely criminal detail."

Slobogin argues that even when a small number of people, some of whom are guaranteed *not* to be the perpetrator (such as somebody whose DNA only partially matches that of the sample from a crime scene), are identified to the police, the intrusion into privacy is fairly minimal and should be handled through Fourth Amendment doctrines that allow for warrantless searches and seizures, like checkpoints.[31] I agree with nearly all of Slobogin's proposals about how courts should interpret the Fourth Amendment with respect to these examples. But they still do not meet the criteria I am setting—criteria that, when met, challenge the most basic conceptions of Fourth Amendment privacy. To meet the definition of a filtered dragnet for my purposes, police will remain ignorant to details and identities until there is a high probability that the information identifies and pertains to the perpetrators and no one else.

2. Nondisclosure of Irrelevant Details

The first requirement on its own ensures that filtered dragnets are analogous to "binary searches" like drug-sniffing dogs—the sort that alert only if there is probable cause of a crime. But there is an additional affordance that should be exploited: filtered dragnets must refine the information that is ultimately disclosed to police by filtering out personal, irrelevant details *even about a suspect*. This is equivalent to a drug-sniffing dog that could magically produce a suspect's drugs without any of the rifling through cars and pockets that are necessary today. Thus, the suspect will retain privacy over details that are not relevant to the criminal investigation at hand.

To be clear, neither of these requirements are meant to be absolute guarantees. All systems have error, and even if police are able to set very demanding thresholds for false positives, police will occasionally access licit, irrelevant details when a filtered dragnet falsely identifies a suspect who is then subjected to an arrest or probable cause–based search. But the requirements for disclosure in a filtered dragnet system can be calibrated to fit societal needs and expectations: the chance of false accusation error can be driven down to practically zero if we would like, if we are willing to tolerate the consequences that there will be more false negatives (more

30. Paige St. John, *The Untold Story of How the Golden State Killer Was Found: A Covert Operation and Private DNA*, L.A. TIMES (Dec. 8, 2020), https://www.latimes.com/california/story/2020-12-08/man-in-the-window [https://perma.cc/7LZU-9JGQ].

31. Slobogin, *Suspectless Searches*, *supra* note 29, at 955–56.

crimes that are not detected) *or* that police departments will need to access more data in order to maintain the same level of detection.

B. EXAMPLES

Next, we will visit a set of backwards investigation techniques that are in use today. These use the particularities of a crime to lead police to a suspect. While most cannot meet the demanding definition of "filtered dragnet" formalized above, with time and additional data resources, they will surely get there.

1. DNA Matching

DNA-matching investigations use parts (non-revelatory portions) of a DNA sequence produced from a sample collected at a crime scene or from a crime victim in order to identify a suspect using DNA databases. They are an obvious extension of fingerprinting analyses with some souped-up features. First, DNA matching can set a very high threshold of statistical probability of true match (or, in other words, a very low probability of a false match) because each DNA sequence has a large amount of data.[32] Second, they can make use of popular commercial and ancestry databases for cross-checking and are therefore not limited to identifying individuals who have a history with the criminal justice system.

Third, familial or partial DNA matches are very useful for police investigations in a way that partial fingerprint matching is not. In familial DNA-matching investigations, such as the one that eventually led to the arrest of the Golden State Killer, police departments recover the identity not of the suspect but of one or more of the suspect's genetic relatives.[33] This raises privacy concerns for the relatives whose identities are revealed to law enforcement in the course of finding the perpetrator.[34] So, as practiced today, familial DNA searches do not fit the definition of a filtered dragnet. They fail the second element (filtering out innocent and irrelevant details) by revealing identities and information about family members who are

32. With enough of a sequence for matching, the investigator can have extremely high confidence that the combination of DNA markers will be unique to a single individual. Fingerprint analysis, by contrast, contains a natural limit on how confident an analyst can be that the patterns from prints left at a crime scene would be produced by just one person. Nevertheless, there are still opportunities for DNA matching to produce erroneous results. ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA 29–83 (2015).

33. David Lazer & Michelle N. Meyer, *DNA and the Criminal Justice System: Consensus and Debate*, in DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 907–08 (David Lazer ed., 2004) (describing "low-stringency" searches on DNA databases that will return results of individuals who are likely to be related to the person whose DNA was sequenced for the crime scene sample).

34. Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 STAN. L. REV. 751, 791 (2011).

definitely *not* the perpetrator of the crime.[35] However, it is conceivable that in the future, if multiple databases are able to be accessed and triangulated, familial DNA matching can be part of a filtered dragnet system that automatically finds a familial match, trawls other data sources in order to identify the correct relative of familial match (based on, e.g., age, location, or personal history of the relatives), and discloses the identity of the suspect and the relevant details only when and if there is sufficient confidence that the correct suspect has been identified.[36] All of this can be automated.

DNA evidence holds an esteemed place in criminal justice and public perception. DNA evidence is durable (as long as it is handled properly) and judges and juries can justifiably place a high degree of confidence in the reliability of DNA-matching investigations.[37] Other types of data beyond DNA can have these qualities, too, but they provoke much more suspicion and dissent. Distinguishing them from DNA matching will become increasingly untenable.

2. Facial Recognition

Facial recognition uses large databases of identified photographs (often scraped from the public Internet) to discover the identity of a person who would otherwise be anonymous.[38] The technology can be used as a filtered dragnet when police departments deploy facial recognition on photographic evidence from the scene of the crime.[39] For example, law enforcement has used facial recognition to pin identities to individuals who appeared in surveillance footage from the Capitol on January 6, 2021, as well as to robberies and street crimes.[40] Although facial recognition algorithms are less

35. One might think these are relatively minor privacy intrusions (equivalent to a witness saying "the murderer was Moe's cousin").

36. This is not far-fetched: police already use statistical packages like a service called "What Are the Odds" in order to understand the closeness of the blood relationship between the suspect and the person whose DNA created a familial match, and then they use traditional methods of genealogy research (e.g., cross-checking with Census records and other public records) to find the suspect. Ellen M. Greytak, CeCe Moore & Steven L. Armentrout, *Genetic Genealogy for Cold Case and Active Investigations*, 299 FORENSIC SCI. INT'L. 103, 103–04, 107 (2019).

37. Lazer & Meyer, *supra* note 33, at 880–81.

38. The procedure works by converting images of faces into "face prints"—maps of the contours of an individual's face—and then cross-checking the maps against each other. Natasha Singer, *Never Forgetting a Face*, N.Y. TIMES (May 18, 2014), https://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face [https://perma.cc/L2PZ-DWL3].

39. Facial recognition can also be used when police have already sought and received a warrant for a person's arrest based on probable cause from other sources and are attempting to locate the suspect. This would also constitute a filtered dragnet.

40. Kashmir Hill, *Your Face Is Not Your Own*, N.Y. TIMES MAG. (Mar. 18, 2021), https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai [https://perma.cc/A2CC-GXGG].

accurate for female and non-white faces,[41] industry members claim this is not the case for top-performing algorithms in active use.[42]

3. Automated CSAM Detection

Last year, Apple unveiled a program that would automatically scan iPhoto images and cross-check them against a library of known child pornography when the images were uploaded to the iCloud. Apple had planned to use a hashing technique to check all files sent from Apple devices to be stored on iCloud servers. Essentially, every image received by an Apple phone is converted to a code that corresponds to the visual image.[43] When a person's iPhoto images produce ten matches, Apple employees would automatically be alerted and would share the information with authorities. Thus, while *every* image would be hashed and cross-checked against child pornography, only the images that matched could lead to a disclosure to law enforcement. Apple has since abandoned its plans in response to criticism,[44] but the technological capability still exists.

4. Geofences and Other Reverse Searches

In 2019, a spate of arsons involving vehicles parked in commercial lots was committed in short succession.[45] Based on the locations, surveillance footage, and similar modi operandi, police had reason to believe that a single set of co-conspirators was involved in all six arsons. When federal investigators requested that the court issue a warrant requiring Google to search its time-logged geolocation records for cellphones that were at or near the scenes of the arsons during the times that they were committed, a U.S.

41. PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS AND TECH., NISTIR 8280, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 48 (2019).

42. Jake Parker & David Ray, *What Science Really Says About Facial Recognition Accuracy and Bias Concerns*, SEC. INDUS. ASS'N (July 23, 2022), https://www.securityindustry.org/2022/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns [https://perma.cc/Z2Z2-ZZN6]; Hoan Ton-That, *The Myth of Facial Recognition Bias*, CLEARVIEW AI (Nov 28, 2022), https://www.clearview.ai/post/the-myth-of-facial-recognition-bias [https://perma.cc/4WXT-65Y6].

43. The hash is a 1:1 transform, meaning that the hash function would convert an image into just one particular string of numbers, and conversely a single code (or string of numbers) would translate into one particular image. This allows Apple to check the hash of every image against a library of hashes that represent known child sexual abuse material ("CSAM") in order to detect child pornography. However, those who traffic in CSAM would be alert to this and could make minor changes to the image to avoid exact matches. To prevent circumvention, Apple uses a form of perceptual hashing (called NeuralHash) that uses fuzzy matching to detect and alert to images that do not match exactly but are very likely depicting the same image. APPLE, CSAM DETECTION: TECHNICAL SUMMARY 4 (2021).

44. Lily Hay Newman, *Apple Kills Its Plan to Scan Your Photos for CSAM. Here's What's Next*, WIRED (Dec. 7, 2022, 11:11 PM) https://www.wired.com/story/apple-photo-scanning-csam-communication-safety-messages [https://perma.cc/G8SL-RE53].

45. *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 351 (N.D. Ill. 2020).

magistrate judge complied.[46] This type of process—where police start with the location, approximate time, and other details of a crime and ask service-providers to find a matching account—is known as a "geofence warrant," and magistrate judges have issued orders authorizing their use under certain conditions. Judges have refused to issue warrants (without deciding whether warrants are actually necessary) when the request cast too wide a net—that is, if too many devices are likely to be identified as matching the search criteria.[47] For example, if police are investigating a crime that took place during a Beyoncé concert, even a geofence with a small radius, during a fairly precise window of time, will draw in too many false matches—too many phones of innocent bystanders. But this concern falls away if police can use multiple details or the intersection of several geofences in order to create a search criteria that will be unique to the perpetrator.[48] For example, in one recent case, a perpetrator who was suspected to have cased the location of a murder on the day before he committed it was identified using overlapping geofences from the day before and the day of the murder.[49] License plate readers, drone footage, Internet of Things data, and satellite surveillance imaging could also be sources of geolocation information in the likely circumstance that criminals begin to leave their devices at home.[50]

Geolocation data can be combined with other types of information, too, to form a signature of crime that is more likely to be unique. As an illustration, US intelligence agencies located Osama bin Laden in part by looking for locations where they would expect to find Internet and cell service but in fact found none.[51] There are data sources outside of location data that can create a signature for reverse searching. For example, while investigating an arson case, the Denver police department sought and received a "keyword warrant"—a court order requiring Google to reveal the account information of users who had recently searched for the address of the arson during a fifteen-day period leading up to the crime.[52]

46. *Id.* at 364.

47. *E.g.*, *In re* Matter of Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 733 (N.D. Ill. 2020).

48. The arson case would have been an ideal investigation to use intersecting geofences. Unfortunately, the government did not request records in that way, and the court did not address the difference between the union and intersection of geofences in its opinion. *In re Search Warrant Application*, 497 F. Supp. 3d at 345.

49. Slobogin, *Suspectless Searches*, *supra* note 29, at 954 (citing Tyler Dukes, *To Find Suspects, Raleigh Police Quietly Turn to Google*, WRAL NEWS (July 13, 2018, 11:07 AM), https://www.wral.com/to-find-suspects-police-quietly-turn-to-google/17377435 [https://perma.cc/BU4W-2Z4Q]).

50. *Id.* at 954–55; Eldar Haber, *The Wiretapping of Things*, 53 UC DAVIS L. REV. 733, 736 (2019).

51. Peter Bergen, *Did Torture Help Lead to Bin Laden?*, CNN (Dec. 10, 2014, 12:26 PM), https://www.cnn.com/2014/12/10/opinion/bergen-torture-path-to-bin-laden/index.html [https://perma.cc/EJV6-FV6W].

52. Celes Keene, *Reverse Keyword Searches and Crime*, LEXOLOGY (Aug. 11, 2022), https://

Cyberstalking, child pornography, and many other online crimes have used forms of reverse searches in order to identify the accounts associated with IP addresses that were used to engage in those crimes.[53]

5. Scanners, Sensors, Cameras, and Microphones

Red light cameras were one of the first ventures into automated policing and were also much despised.[54] These systems used sensors to detect if a car entered an intersection after the light had turned red, took a photograph of the car, and later used the image of the car (and its license plate) to track down the owner and mail a ticket. These systems are not dragnets *per se* (they do not make use of pre-existing collections of data), but they set the stage for Automatic License Plate Readers that *do* capture an abundant amount of data in case some particular parts of it are useful later, as when police are searching for a stolen vehicle.[55]

Patterns that are highly suggestive of crime can also be automatically detected using recording devices with cameras, microphones, or sensors that operate in "always on" mode.[56] One example in use today is ShotSpotter microphones that are constantly "listening" in a public setting but alert the police and save data long term only when the noises captured by the shot-spotter match the sounds of gunshots.[57] In theory, Alexa, which also constantly records to respond to watchwords like "Hey Alexa,"[58] could be designed to detect sounds that are particular to domestic violence or home invasion and automatically alert the authorities.

Other sensitive devices like terahertz scanners can detect when naturally occurring radiation is blocked by metal objects. When the blocking metal objects are gun shaped, the scanners can be programmed to alert.[59] But

www.lexology.com/library/detail.aspx?g=de2f5b21-a9b1-4650-a911-31dd1f39e671 [https://perma.cc/T8HH-RREJ].

53. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 505 (9th Cir. 2008); United States v. Hood, 920 F.3d 87, 89 (1st Cir. 2019); United States v. Contreras, 905 F.3d 853, 855–56 (5th Cir. 2018).

54. Erin Mulvaney & Dug Begley, *Opposition Putting a Stop to Red Light Cameras*, HOUS. CHRON. (Apr. 25, 2013, 9:19 AM), https://www.houstonchronicle.com/news/houston-texas/houston/article/opposition-putting-a-stop-to-red-light-cameras-4461447.php [https://web.archive.org/web/20220708020423/https://www.houstonchronicle.com/news/houston-texas/houston/article/Opposition-putting-a-stop-to-red-light-cameras-4461447.php].

55. Slobogin, *Suspectless Searches*, *supra* note 29, at 955. Similarly, short-range communications technologies can reveal a car's speed. Joh, *supra* note 17, at 200.

56. Haber, *supra* note 50, at 735.

57. SHOTSPOTTER, *ShotSpotter Frequently Asked Questions* (2018), https://www.shotspotter.com/system/content-uploads/SST_FAQ_January_2018.pdf [https://perma.cc/3SD4-B2JU].

58. AMAZON, *How Alexa Works: Wake Word* (last visited Feb. 25, 2024), https://www.amazon.com/b?ie=UTF8&node=23608571011 [https://perma.cc/JXB3-246D].

59. I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1275–77 (2017) (arguing that these tools can lead us to "*real* reasonable suspicion").

this is nothing compared to what quantum magnetometry will be able to do in the near future.[60] Quantum sensing is so sensitive to minute differences in magnetic fields that the sensors will be able to detect trace amounts of chemicals, even when they are concealed behind walls. So, Justice Brennan's nightmare scenario is here: we will soon have contraband detection devices.

This survey of suspicionless searches and backwards investigations demonstrates that there is increasing viability and interest in using these types of techniques. The practices currently in use do not usually meet the two formal requirements for "filtered dragnets," but it is useful to assume they eventually will. By assuming investigations will eventually meet the demanding definition of filtered dragnets, we will be able to state with more rigor precisely why it is we are nervous about these law enforcement technologies, and what the policy or constitutional response should be.

II. THE ADVANTAGES OF FILTERED DRAGNETS

This Article will eventually explain why filtered dragnets impose serious risks on society that are not adequately (or even nominally) addressed in Fourth Amendment theory. But first, we will explore reasons to embrace, rather than resist, the integration of filtered dragnets into policing.

Filtered dragnets offer several advantages over the investigation practices in common use.[61] These include decreased exposure of innocent details, increased accuracy and efficacy of criminal investigations, increased detection and deterrence of crime, decreased discretion for suspect selection, and decreased risk to witnesses and victims. In combination, these advantages contribute such compelling benefits to society that courts and attorneys should feel a moral obligation to harness their powers as much as possible.

A. DECREASED EXPOSURE OF INNOCENT AND IRRELEVANT DETAILS

Filtered dragnets protect the privacy of innocent individuals, as well as the innocent-and-irrelevant details of a suspect. They protect innocent individuals whose data is scanned in the process by allowing police and courts to set a high standard for false match error. That is, filtered dragnets can be programmed to alert and reveal personal information only when the statistical probability that the person has engaged in crime is greater than

60. Dmitry Budker & Michael Romalis, *Optical Magnetometry*, 3 NATURE PHYSICS 227, 227 (2007).

61. A police investigation strategy cannot be judged without comparison to its next best alternatives. *See* Tal Z. Zarsky, *Governmental Data Mining and Its Alternatives*, 116 PENN. ST. L. REV. 285 (2011).

50%, or 80%, or 99%. This would ensure that the number of innocent individuals who are initially approached and investigated will be only a fraction of the number of criminals who are found.[62]

Moreover, filtered dragnets limit the type of information that is revealed even about the proper subjects of investigation who have committed a crime. This is a game-changer. If police could have searched a house or a car in a manner that blinded them to everything *except* contraband or criminal evidence, the text and interpretation of the Constitution would probably differ from what we have today. The closest analogy we have to filtered dragnets, as I have mentioned before, are drug-sniffing dogs. Police dogs are allowed to sniff and alert based on the (mostly defensible) assumption that they will be trained well enough to have a low error rate.[63] The dog sniff and subsequent alert are, controversially, treated as a non-search in Fourth Amendment law unless the dog has trespassed into the home or curtilage of a resident.[64] But once the dog alerts, the police have probable cause to perform an entire human-conducted unfiltered search of a person's vehicle, home, or effects, thereby revealing intimate and innocent details while they look for contraband. Filtered surveillance is more privacy-protective than drug-sniffing dogs because it can restrict the sort of data that is revealed even as police are verifying that the alert is accurate.

I do not mean to suggest that filtered dragnets avoid all revelations about innocent people or activities. Relevant data disclosed to police as a result of a high probability match will frequently, maybe even usually, reveal information that is not directly tied to wrongdoing. For example, if in the future the police used a system that combines familial DNA matching with other records to identify a sexual assault offender, police may see and use the identity of the family member in order to confirm that the identification is sound and to show how the case was solved to a jury. This could reveal the identity of estranged parents or children of the suspect or could uncover paternity that was not previously known.[65] But this is a consequence of the fact that all successful investigations impose some irreducible privacy costs on the innocent. Even using traditional strategies, police will occasionally and appropriately question a spouse in a manner that reveals the suspect is having an affair or may make other similar sensitive revelations. If the revelations are in service of pursuing a probable cause–backed investigation,

62. I have called this "hassle"—the imposition of searches, seizures, or even the stress of becoming a person-of-interest, experienced by an innocent person who is targeted based on probable cause. Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461, 461 (2015).

63. Florida v. Harris, 568 U.S. 237, 238 (2013).

64. Florida v. Jardines, 569 U.S. 1, 6–7 (2013).

65. NEIL RICHARDS, WHY PRIVACY MATTERS 99 (2021).

these will be innocent-but-relevant details.[66] The advantage I describe here pertains to the shielding of innocent-and-irrelevant information.

B. INCREASED ACCURACY

By definition, filtered dragnets identify suspects and reveal information only when there is a high probability of crime. This is a form of increased accuracy—a reduction in false positive error. (In the next subsection, I will discuss the other form of increased accuracy—the reduction in false negative error—which would allow filtered dragnets, if deployed consistently, to solve more crimes and increase clearance rates.)

If filtered dragnets are held to higher probability standards than standard investigation techniques, they will cause proportionally fewer false starts and erroneous arrests and searches along the way.[67] In time, a shift toward filtered dragnets should decrease the dangers and anxiety that come from false suspicion and conviction at every stage of criminal investigation. Indeed, facial recognition systems that identify a suspect based on photographs or surveillance footage from a crime already outperform the accuracy rates of average eyewitnesses and PC-based warranted searches by a large margin.[68]

66. Thus, I disagree with scholars like Neil Richards who suggest that familial DNA matching inevitably presents a risk of a free-for-all where police will routinely learn about paternity or about the genetic propensity for disease. *See id.*

67. Ram, *supra* note 34, at 788 (identifying the potential for exoneration as a reason to adopt familial DNA matching). Similarly, a more accurate criminal justice system also reduces the potential for abuse, too, because it denies state agents the ability to credibly threaten the innocent. Dhammika Dharmapala, Nuno Garoupa & Richard H. McAdams, *Punitive Police? Agency Costs, Law Enforcement, and Criminal Procedure*, 45 J. LEG. STUD. 105, 111 (2016) (citing Keith N. Hylton & Vikramaditya S. Khanna, *A Public Choice Theory of Criminal Procedure*, 15 SUP. CT. ECON. REV. 61 (2007)).

68. False match error rates for facial recognition algorithms are now under 1% in ideal conditions and under 10% when used in the field, and facial recognition services recommend law enforcement use a threshold of 95% confidence. William Crumpler, *How Accurate Are Facial Recognition Systems—and Why Does It Matter?*, CTR. STRATEGIC & INT'L STUD. (Apr. 14, 2020), https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it [https://perma.cc/3YQS-UM7C]. By comparison, eyewitness identification during a lineup has error rates of 20% or more. Gary L. Wells & John W. Turtle, *Eyewitness Identification: The Importance of Lineup Models*, 99 PSYCH. BULLETIN 320, 320 (1986). The same is true for racial differences in error rates: while some facial recognition technologies were, at least for a time, more likely to produce false matches for photographs of Black faces, the gap in false match error has already been reduced. Stewart Baker, *The Flawed Claims About Bias in Facial Recognition*, LAWFARE (Feb. 2, 2022, 12:57 PM), https://www.lawfaremedia.org/article/flawed-claims-about-bias-facial-recognition [https://perma.cc/E8TC-HV8A]. In any event, even if gaps persist, those gaps may be less bad than the differences in false match error from human systems of suspect identification. And unlike traditional policing methods, facial recognition technology can be calibrated to only produce a match when the risk of a false match is below a certain threshold regardless of the target's constraining alerts, in other words, to ensure equal false positive rates by race. Setting the false match rate to be equal is equivalent to ensuring that "probable cause" for Black suspects means the same thing it does for whites. For a full articulation of race-conscious analyses of error, see Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218 (2019).

Skeptics will have at least two critiques of my optimistic prediction: all systems have *some* error, and the sort of error that comes from a highly technical and data-driven system might be particularly worrisome since a falsely accused defendant will have to go up against a trusted and more accurate system.[69]

It is true that no investigation tool is free from error, and it is also possible that police, prosecutors, and juries could be at risk of reflexively trusting the results of a filtered dragnet system because they are so reliable. But the premise of the critique might be plain wrong. When a filtered dragnet produces a spurious result, the error could very well be *easier* to catch than when an informant or witness makes a spurious identification. For example, when a man named Michael Usry was the target of an investigation based on his father's partial genetic match to crime scene DNA, Usry was cleared as soon as his own DNA sample was collected and analyzed because it did not match the sample collected at the scene of the crime.[70] This should generalize: the more independent sources of data there are, the more protection there should be for innocent.[71] A person wrongly identified by facial recognition is more likely to have a credible digital alibi (e.g., geolocation data that puts them in an entirely different state at the time of a crime) than a wrongly identified person who was accused by a confidential informant.

The facts of *United States v. Chatrie*[72] illustrate the propensity for the erroneous targets of filtered dragnets to be cleared earlier and easier than erroneous targets in traditional investigations. In that case, police used a geofence warrant to access the deidentified location data of individuals who were near the scene of a bank robbery during the hour that the crime took place.[73] The geofence produced the deidentified location records of nineteen individuals, only one of whom was the perpetrator.[74] These facts do not fit the requirements of a filtered dragnet because law enforcement accessed and manually examined information related to the eighteen individuals who were not the perpetrator, but we can think of these eighteen as stand-ins for those

69. *See* Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1281 (2016) (describing the "seduction of quantification" in machine processes).

70. Jim Mustian, *New Orleans Filmmaker Cleared in Cold-Case Murder; False Positive Highlights Limitations of Familial DNA Searching*, NOLA.COM (Mar. 12, 2015), https://www.nola.com/article_d58a3d17-c89b-543f-8365-a2619719f6f0.html?mode=comments [https://perma.cc/S3GZ-59DY]; Natalie Ram, Christi J. Guerrini & Amy L. McGuire, *Genealogy Databases and the Future of Criminal Investigations: The Police Can Access Your Online Family-Tree Search and Use It to Investigate Your Relatives*, 360 SCIENCE 1078, 1078 (2018).

71. *See* Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014).

72. United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022).

73. *Id.* at 917–22.

74. *Id.* at 920–21.

who are wrongly targeted by filtered dragnet. One hour of anonymous geolocation data conclusively ruled out sixteen of them, and an additional hour ruled out the other two. None of the eighteen were identified (by name or other direct identifier) to the police, and none were questioned.[75] By contrast, consider the experiences of two individuals who were briefly implicated in the investigation *before* the FBI used geofence technologies. Using traditional policing methods, the FBI first investigated the ex-boyfriend of a woman who saw news reports about the bank robbery and called the police to offer a false tip. They also investigated somebody who owned the same kind of car that was used as the getaway vehicle when a bank employee reported the possible tip, but that, too, was a dead end.[76] It is not clear from the opinion what sorts of encounters and information-gathering the police used to rule out these two, but I suspect the anxiety and privacy burden absorbed by them was greater, by almost any measure, than the burden to the eighteen individuals whose approximate movements in public during one to two hours were disclosed in deidentified form. If this case is representative, the geofence warrant process should be a method of first resort, rather than last resort, because it is likely to lead more quickly to both the identification of the right suspect and the elimination of wrong ones.

A second skeptical critique is that I am describing the positive qualities of filtered dragnets under the assumption that the systems will be deployed as intended and will not be manipulated or tampered with. This is a legitimate concern to which the long history of flaws in forensic labs can attest.[77] But as a comparative matter, data-driven techniques of this sort might be more accountable and auditable than old-school forms of criminal investigation. When the same level of scrutiny and doubt is applied to traditional investigations that would have to continue in the absence of new technologies—the risks of error and manipulation present in eyewitness testimonies, suspect interrogation, or warrant affidavits[78]—the prediction

75. *Id.* at 921.

76. *Id.* at 917.

77. MURPHY, *supra* note 32, at 29–83; John Solomon, *More Wrongdoing Found at FBI Crime Lab*, MIDLAND DAILY NEWS (Apr. 14, 2013), https://www.ourmidland.com/news/article/More-Wrongdoing-Found-at-FBI-Crime-Lab-7133820.php [https://perma.cc/D43V-8T9L]. The FBI has acknowledged that flawed forensics have affected dozens of death penalty cases. *FBI Admits Flawed Forensic Testimony Affected at Least 32 Death Penalty Cases*, EQUAL JUST. INITIATIVE (Apr. 29, 2015), https://eji.org/news/fbi-admits-flawed-forensic-testimony-in-32-death-penalty-cases/#:~:text=These%20FBI%20examiners%20trained%20500,those%20defendants%20have%20been%20executed [https://perma.cc/RNX9-KZTH].

78. Lazer & Meyer, *supra* note 33, at 917. The Innocence Project found that half of the cases that they selected as being likely to be a false conviction did indeed lead to exoneration once DNA evidence was tested. How did they select these cases? By looking for convictions that were based on the traditional (and highly faulty) forms of evidence that are noisy signals of guilt: testimony from jailhouse snitches and eyewitnesses, the defendants' confessions, and pseudo-scientific evidence (e.g., hair analysis). *Id.* at 898–99. Other factors include incompetent defense counsel and police or prosecutorial misconduct.

that filtered dragnets will be *more* corrupt and error-prone is hard to believe.[79]

C. INCREASED DETECTION AND DETERRENCE

The accuracy and efficiency of filtered dragnets can help tackle longstanding social problems of chronically unsolved crime, assuming filtered dragnets are used regularly.[80] About twenty-five million Americans—8% of the population—suffer from a violent felony or a felony-level theft each year.[81] These events are of course disproportionately likely to beset low-income households. While violent crime rates today are still down compared to the high-water marks in the 1980s and early 1990s,[82] the statistics are still grim, particularly for communities of color. In the U.S., about five people in every 100,000 are murdered each year.[83] For African-Americans, the rate is above six per 100,000.[84] (By comparison, the rates in France and Italy are 1.28 and 0.52 per 100,000, respectively.)[85] In addition

79. For example, one study found that more than 25% of sexual assault suspects are exonerated when DNA re-analysis becomes available. PETER NEUFELD & BARRY C. SCHECK, CONVICTED BY JURIES, EXONERATED BY SCIENCE: CASE STUDIES IN THE USE OF DNA EVIDENCE TO ESTABLISH INNOCENCE AFTER TRIAL xxviii (1996). If this sample is typical, the findings imply that the quality of traditional police investigations leading to investigation, arrest, and conviction is rather shoddy.

80. Ram, *supra* note 34, at 788 (describing increased crime solving as an argument in favor of familial DNA searching).

81. ALEXANDRA THOMPSON & SUSANNAH N. TAPP, U.S. DEP'T. OF JUST., NCJ 305101, CRIMINAL VICTIMIZATION, 2021 2–3 (2022).

82. In the U.S., crime rates are quite low in historical terms. Violent crimes have dropped by at least half since the early 1990s, and property crimes have dropped even more dramatically. John Gramlich, *What the Data Says (and Doesn't Say) About Crime in the United States*, PEW RSCH. CTR. (Nov. 20, 2020), https://www.pewresearch.org/short-reads/2020/11/20/facts-about-crime-in-the-u-s [https://perma.cc/R9A8-SDUH]; RACHEL E. MORGAN & BARBARA A. OUDEKERK, U.S. DEP'T. OF JUST., NCJ 253043, CRIMINAL VICTIMIZATION, 2018 1 (2019). Although crimes of all sorts (particularly murder) have skyrocketed during the COVID-19 pandemic, the pandemic-related stress on social and economic wellbeing make the recent data difficult to interpret. *Compare* Paul G. Cassell, *Explaining the Recent Homicide Spikes in U.S. Cities: The "Minneapolis Effect" and the Decline in Proactive Policing*, 33 FED. SENT'G REP. 83 (2020) (finding under-policing and under-deterrence as a main cause), *with* Jeffrey Fagan & Daniel Richman, *Understanding Recent Spikes and Longer Trends in American Murders*, 117 COLUM. L. REV. 1235 (2017), *and* German Lopez, *The Rise in Murders in the U.S., Explained*, VOX (Dec. 2, 2020, 10:35 AM), https://www.vox.com/2020/8/3/21334149/murders-crime-shootings-protests-riots-trump-biden [https://perma.cc/9NZR-HBHC] (suggesting pandemic-related shocks are the primary driver of higher homicide rates).

83. *FBI Uniform Crime Report*, *Crime in the United States 2013, Expanded Homicide Data Table 6*, U.S. DEP'T JUST., FED. BUREAU INVESTIGATION (2013), https://ucr.fbi.gov/crime-in-the-u.s/2013/crime-in-the-u.s.-2013/offenses-known-to-law-enforcement/expanded-homicide/expanded_homicide_data_table_6_murder_race_and_sex_of_vicitm_by_race_and_sex_of_offender_2013.xls [https://perma.cc/W9H4-64BB].

84. *Id.*

85. *Id.* The United States, even in its lowest crime period, is still far more crime-ridden than other developed nations. For example, 5.4 out of every 100,000 Americans were killed by homicide in 2016, whereas in France the rate was 1.4 out of every 100,000. *See Victims of Intentional Homicide, 1990–2018*, UNITED NATIONS OFF. ON DRUGS AND CRIME, https://dataunodc.un.org/content/data/homicide/homicide-rate [https://perma.cc/NLL4-FNLL].

to the trauma and losses to crime victims, society also absorbs a range of economic costs and psychological distress in the course of guarding against crime.[86] It is all too easy for scholars, lawmakers, and others who live in safe neighborhoods to forget: serious crime is just awful.

Crime clearance rates (that is, the proportion of crimes actually reported to the police that have led to an arrest or otherwise been considered solved) for violent crime is 42%, and the rate is under 15% for property crimes.[87] Only about half of violent crimes and one-third of property crimes are ever reported to the police, and many arrests and convictions are erroneous. The low likelihood of reporting a crime, the low clearance rates, and the somewhat sizable chance of false arrest altogether mean that the probability a criminal will be prosecuted for any particular violent crime is probably under 20%.[88]

Clearance rates in black neighborhoods are even worse. The events over the last decade validate Bill Stuntz's observation that "poor black neighborhoods see too little of the kinds of policing and criminal punishment that do the most good, and too much of the kinds that do the most harm."[89] Dampening crime in lower income black communities is a civil rights goal of longstanding stature.[90] Bennett Capers described underenforcement as the criminal justice problem that gets short shrift,[91] and that was before George Floyd's murder made police violence and over-policing problems an issue of pressing global salience. There is some squeamishness today in discussing crime in black neighborhoods (and certainly in referring to that crime as "black on black"), but it is foolish to expect criminal justice reform to be

86. *See*, *e.g.*, David Anderson, *The Aggregate Burden of Crime*, 42 J.L. & Econ 611, 629–30 (1999); Aaron Chalfin & Justin McCrary, *Are U.S. Cities Under-Policed? Theory and Evidence*, 100 REV. ECON. & STAT. 167, 167 (2018); Kathryn E. McCollister, Michael T. French & Hai Fang, *The Cost of Crime to Society: New Crime-Specific Estimates for Policy and Program Evaluation*, 108 DRUG & ALCOHOL DEPEND. 98, 98 (2010).

87. *Crime Clearance Rate in the United States in 2020, by Type*, STATISTA, https://www.statista.com/statistics/194213/crime-clearance-rate-by-type-in-the-us [https://perma.cc/XT5F-EHCQ]; *Most Violent and Property Crimes in the U.S. Go Unsolved*, PEW RSCH. CTR. (2017) [hereinafter *Pew Property Crimes*], https://www.pewresearch.org/fact-tank/2017/03/01/most-violent-and-property-crimes-in-the-u-s-go-unsolved [https://perma.cc/XG8E-6FQ8]; *What the Data Says (and Doesn't Say) About Crime in the United States*, PEW RSCH. CTR. (2020), https://www.pewresearch.org/fact-tank/2020/11/20/facts-about-crime-in-the-u-s [https://perma.cc/92VY-8CGL].

88. STATISTA, *supra* note 87. The figure for property crime is 7%. *Pew Property Crimes*, *supra* note 87.

89. STUNTZ, *supra* note 15, at 497; *see also* RANDALL KENNEDY, RACE, CRIME, AND THE LAW 19, 158–60 (1997).

90. FORMAN, *supra* note 7, at 11 ("African Americans have *always* viewed the protection of black lives as a civil rights issue, whether the threat comes from police officers or street criminals."), 61 (recounting the editorials in journals that served black D.C. neighborhoods that demanded more law enforcement to ensure that black neighborhoods stay peaceful), 128.

91. Capers, *Techno-Policing*, *supra* note 5, at 497.

lasting and meaningful if it does not tackle *both* of the scourges of inner-city policing: harsh policing *and* civilian violence.

The most obvious and natural way to curb future violent crime is to increase the detection of very serious crimes today.[92] Some scholars, Tom Tyler chief among them, have made the case that in the long run, law-abiding behavior has less to do with criminal law enforcement tactics than with cultural, economic, community, and norms-based factors.[93] Occasionally, this insight has been oversimplified and distorted to leave the impression that law enforcement detection rates have nothing to do with crime rates.[94] This is a mischaracterization of the evidence.[95] While there are multiple "root causes" of crime,[96] data and common sense confirm that holding other factors steady, criminal behavior is sensitive to the probability of law enforcement detection. The relevant criminology studies consistently find evidence that detection reduces the incidence of future crime.[97] There is also some evidence that the swiftness of enforcement—the "celerity"—makes a difference.[98]

Increased detection of crime not only reduces crime rates, but also improves other measures of social mobility and security as well. Greater crime detection increases the likelihood that offenders will seek and find

92. Mark Kleiman's work catalogued a set of "dynamic concentration" probation and drug treatment programs that were unusually successful at recidivism reduction. KLEIMAN, *supra* note 20, at 34–65. They depended on good detection. *Id.* at 164. Kleiman pointed out that predatory crimes—those that terrorize and corrupt communities the most—are also the hardest to observe. *Id.* at 165. I am suggesting here that technology may give us the opportunity to run Kleiman-style compassionate crime control programs at a much more ambitious scale.

93. TOM TYLER, WHY PEOPLE OBEY THE LAW 171 (2006).

94. Shaila Dewan, *Refund the Police? Why It Might Not Reduce Crime*, N.Y. TIMES (Nov. 8, 2021), https://www.nytimes.com/2021/11/08/us/police-crime.html [https://perma.cc/U56T-8EPP].

95. Even Tyler's work demonstrates that belief that lawbreakers will be caught and punished has a sizable and statistically significant impact on behavior. TYLER, *supra* note 93, at 59.

96. Crime rates are the result of many social and economic factors that fall outside the realm of criminal law enforcement, such as population demographics (when the population is disproportionately young, there is more crime), fluctuations in the black market for drugs and other vices, environmental toxins (some criminologists have associated lead poisoning to impulsive and criminal behavior), and changes in the access to guns. FORMAN, *supra* note 7, at 50.

97. *See*, *e.g.*, Aaron Chalfin & Justin McCrary, *Criminal Deterrence: A Review of the Literature*, 55 J. ECON. LIT. 5, 13–15, 23–29 (2017) (finding abundant evidence that crime is reduced when police manpower and redeployments increase, and much less consensus in the literature on severe punishment); Steven N. Durlauf & Daniel S. Nagin, *Imprisonment and Crime: Can Both Be Reduced?*, 10 CRIM. & PUB. POL'Y 9, 17 (2011); Daniel S. Nagin, *Deterrence in the Twenty-First Century*, 42 CRIME & JUST. 199, 201 (2013); Daniel S. Nagin, *Deterrence: A Review of the Evidence by a Criminologist for Economists*, 5 ANN. REV. ECON. 83, 88 (2013); Jeffrey Grogger, *Certainty vs. Severity of Punishment*, 29 ECON. INQUIRY 297, 307–09 (1991); KLEIMAN, *supra* note 20, at 74–78; Jennifer L. Doleac, How Do State Crime Policies Affect Other States? The Externalities of State DNA Database Laws 1–3 (Dec. 2016) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2892046 [https://perma.cc/2KP5-7FHJ].

98. Chalfin & McCrary, *supra* note 97, at 10.

employment, enroll in education, and live in a stable family environment, and it reduces school absenteeism in the community.[99] Indeed, given how dramatic the impact of detection is on increasing pro-social behavior, it is not at all clear that law enforcement should even be distinguished from the so-called "root causes" of crime. Fear that crime will not be well controlled is a root of many of the root causes of crime.[100]

So, an enduring and well-documented fact is that an increased likelihood of detection and enforcement drives crime rates down. This is much less true, and possibly not true *at all*, for the severity of punishment, where increasing the length of prison sentences is found to have no impact or even criminogenic effects.[101] Thus, the state's essential duty to protect its constituents from the violence and exploitation of others is well served by good detection. Unfortunately, crime rates are currently under the management of the American criminal justice system's haphazard style of enforcement: occasional, error-prone, and harsh.[102]

D. DECREASED DISCRETION FOR SUSPECT SELECTION

Filtered dragnets are crime-driven rather than suspect-driven. In suspect-driven investigations, police have developed suspicion—or a hunch—around a particular individual and focus their observations in an attempt to develop a case.[103] Suspect-driven investigations are propelled by the theories of police officers and proceed within their discretionary control. Police also have some control over filtered dragnet investigations (e.g., over where and when to deploy them), but once they are put into service, police lose control over the results. If facial recognition or reverse searches identify

99. Anne Sofie Tegner Anker, Jennifer L. Doleac & Rasmus Landersø, *The Effects of DNA Databases on the Deterrence and Detection of Offenders*, 13 AM. ECON. J. APPLIED ECON. 194, 195 (2021).

100. "Safe streets are a necessary platform for neighborhood growth and prosperity. . . . [T]he notion that poverty is the mother of crime has been turned on its head." Philip J. Cook, *Assessing Urban Crime and Its Control: An Overview* 3 (Nat'l Bureau of Econ. Rsch., Working Paper No. 13781, 2008). To be clear, there are plenty of independent reasons to endorse or adopt the rehabilitative programs that criminologists and criminal justice scholars propose. See, e.g., RACHEL ELISE BARKOW, PRISONERS OF POLITICS 76–77 (2019), for an example of an argument in favor of focusing on rehabilitative programs. But scholars like Barkow do not discuss the possibility that greater detection of crime can reduce crime rates and reduce net punishment.

101. Chalfin & McCrary, *supra* note 97, at 23–29.

102. This critique, it should be noted, dates back to the eighteenth-century work of Jeremy Bentham and Cesare Beccaria. *See generally* Raymond Paternoster, *How Much Do We Really Know About Criminal Deterrence?*, 100 J. CRIM. L. & CRIMINOLOGY 765 (2010).

103. Slobogin, *supra* note 19, at 322–23. Even Big Data–assisted suspect-driven investigations appear to perform poorly in identifying criminals who may have committed a crime. JOHN S. HOLLYWOOD, KENNETH N. MCKAY, DULANI WOODS & DENIS AGNIEL, RAND CORP., REAL-TIME CRIME CENTERS IN CHICAGO: EVALUATION OF THE CHICAGO POLICE DEPARTMENT'S STRATEGIC DECISION SUPPORT CENTERS 36 (2019).

a wealthy or politically connected individual as the suspect of a crime, it will be much more difficult for police and prosecutors to avoid pursuing investigation and prosecution, as compared to cases where police use informants or witnesses as the main source of identification.

In later Parts, this Article describes the ways in which police *can* still exercise too much discretion by, for instance, using a filtered dragnet tool preferentially to solve some crimes and not using it on others that are substantially similar. But we should not lose sight of the ways filtered dragnets *do* constrain discretion. One of the greatest risks from mass surveillance (that is, dragnets) is its potential to create a resource for selecting the suspect first and then finding a crime, or for using legal but sensitive information to discredit political enemies and personal foes.[104] Police cannot exert this type of control over filtered dragnets.[105]

The Supreme Court caselaw that has found fault with Big Data policing has involved digital searches in which the police first selected their target and then accessed long histories of their target's whereabouts without a warrant.[106] The Court is right to constrain investigations that permit police to access sensitive and detailed information without any justification or checking mechanism. Even when police have developed suspicion against a target, the low-tech factors that go into building up suspicion about a particular individual (e.g., testimony from an informant or presence in a "high crime neighborhood") can impose an indirect racial tax on innocent minorities that could mostly be avoided with filtered surveillance programs that have very low error.[107]

104. For example, the NSA's strategy of revealing the pornography viewing habits of religious radical critics of the U.S. government. Conor Fridersdorf, *The NSA's Porn-Surveillance Program: Not Safe for Democracy*, THE ATLANTIC (Nov. 27, 2013), https://theatlantic.com/politics/archive/2013/11/the-nsas-porn-surveillance-program-not-safe-for-democracy/281914 [http://web.archive.org/web/20230323142324/https://www.theatlantic.com/politics/archive/2013/11/the-nsas-porn-surveillance-program-not-safe-for-democracy/281914].

105. At least, they cannot exert control so easily. In Section IV.B, I will discuss how police units could still tamper with the process through the selection of crimes to solve or by avoiding or removing the analysis of a subset of constituents' data.

106. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) (accessing several days' worth of geolocation data of a specific target); United States v. Jones, 565 U.S. 400, 403 (2012) (involving GPS tracking of a specific target).

107. KENNEDY, *supra* note 89, at 159; IAN AYRES & JONATHAN BOROWSKY, ACLU OF SO. CAL., A STUDY OF RACIALLY DISPARATE OUTCOMES IN THE LOS ANGELES POLICE DEPARTMENT 27 (Oct. 2008), https://www.aclusocal.org/sites/default/files/wp-content/uploads/2015/09/11837125-LAPD-Racial-Profiling-Report-ACLU.pdf [https://perma.cc/U9GK-7BTU]; Floyd v. City of New York, 959 F. Supp. 2d 540, 556, 584 (S.D.N.Y. 2013). NYPD data showed that a substantial portion of the *Terry* stops (a.k.a. "stop-and-frisk") had a predictably low chance of actually leading to the discovery of contraband based on the factors the police claimed were present. Sharad Goel, Maya Perelman, Ravi Shroff & David Alan Sklansky, *Combatting Police Discrimination in the Age of Big Data*, 20 NEW CRIM. L. REV. 181, 213 (2017).

Not all agree with this assessment. Kiel Brennan-Marquez has argued that "nothing about the logic or practice of data-driven law enforcement makes [] redistributive impulses necessary. On the contrary, they will be hard fought—and particularly in our current political climate, unlikely."[108] I share a certain degree of Brennan-Marquez's cynicism (I have wondered, for example, if law enforcement's sloth-like speed in adopting crime-driven investigation practices rather than suspect-based practices are related to the loss of control over defining the pool of suspects),[109] but he goes too far. There already is some evidence that data-driven policing has redistributed the costs of law enforcement and will continue to do so. DNA-based exonerations, for example, have proven the innocence of disproportionately more minority convicts than whites.[110] This suggests that, going forward, DNA-based investigations will shift police focus not only toward the guilty, but also away from wrongfully accused Black and minority suspects.

E. DECREASED RISK TO VICTIMS, WITNESSES, AND SUSPECTS

Police investigations cause a range of problems that are not captured in the variables I have discussed so far—privacy intrusions, erroneous arrest, et cetera. When police have to rely on old school methods of case investigation, the system necessarily puts victims, witnesses, and suspects at risk of physical or economic harm.

Let us start with crime victims and witnesses. Cooperating with the government is a perilous activity for these individuals, as captured by the saying "snitches get stitches."[111] By one theory, clearance rates for serious crimes are low in the U.S. because proving homicide or robbery cases requires victims and witnesses to testify and put themselves at risk.[112] Bill Stuntz hypothesized that police forces increased their focus on drug and gun

108. Brennan-Marquez, *supra* note 2, at 490.

109. Police use most of these tools as a last resort, perhaps because self-preservation of police discretionary power and popular (if ill-conceived) public resentment toward big data policing happen to push in the same direction.

110. Edwin Grimsley, *What Wrongful Convictions Teach Us About Racial Inequality*, INNOCENCE PROJECT (Sept. 26, 2012), https://innocenceproject.org/what-wrongful-convictions-teach-us-about-racial-inequality [https://perma.cc/V3U6-R4FQ].

111. STUNTZ, *supra* note 15, at 4, 79–80. Drug and gun charges, by contrast, can be proven using physical evidence without any cooperating witnesses. On "snitches get stitches," see *Snitches Get Stitches—Meaning*, *Origin and Usage*, ENGLISH GRAMMAR LESSONS (Dec. 12, 2021), https://english-grammar-lessons.com/snitches-get-stitches-meaning [https://perma.cc/C242-MRDN].

112. In Washington, D.C., residents reported gunshots to 911 or police only 12% of the time as compared with the gunfire incidents detected by ShotSpotter technologies. The study found that crime is disproportionately underreported, and thus under-investigated, in minority and low-income neighborhoods. JILLIAN B. CARR & JENNIFER L. DOLEAC, BROOKINGS INST., THE GEOGRAPHY, INCIDENCE, AND UNDERREPORTING OF GUN VIOLENCE: NEW EVIDENCE USING SHOTSPOTTER DATA 2 (Apr. 2016), https://www.brookings.edu/wp-content/uploads/2016/07/Carr_Doleac_gunfire_underreporting.pdf [https://perma.cc/G7P6-3JBU].

possession charges because these crimes were "self-proving" once contraband was discovered, and therefore did not necessitate the cooperation of a victim or witness.[113] As a result, more serious crimes were harder to clear than low-level crimes. But, of course, those are the crimes that are more damaging to the community. If reverse searches, facial recognition, and other filtered dragnets could allow police to prove cases independently, without exposing victims and witnesses to the risk of social stigma and retaliation, they would contribute benefits to society that are not accounted for in the usual privacy-versus-security debates.

As for the suspects, the manner in which traditional policing builds up cases leave much to be desired. Police stops and searches are often vectors for bias and disrespect where swearing, insults, unwarranted accusations and suspicion, and unjustified physical contact lead to demoralization and distrust.[114] Traditional investigations are costly in terms of time, fear, property damage, and general unpleasantness. A person who is pulled over for a secondary inspection when a police dog alerts to her car may very well have no recourse when the police slash open the seats of her car to try to find drugs. Home searches and interrogations cause additional physical, emotional, and economic strain to suspects, irrespective of what sorts of private information is revealed. These costs will become more obvious and more salient when technology obviates the need for a government agent to tear open the upholstery of a suspect's car, dishevel a dresser, and "grope[] and grab[] our children" at the airport.[115]

***

In combination, these factors show that filtered dragnets should be part of any responsible law enforcement program. They extend the "pareto frontier" by allowing privacy *and* crime detection to increase at the same time.[116] It would be counterproductive for law to prohibit their use based on a formalistic or expansive notion of Fourth Amendment protection. And yet, as the next Part shows, there is some risk that courts and lawmakers may do just that.

113. STUNTZ, *supra* note 15, at 4.

114. Capers, *supra* note 59, at 1243–44 (referring to "hard surveillance" and distinguishing it from soft forms); FORMAN, *supra* note 7, at 171.

115. As Senator Ron Paul colorfully puts it. Capers, *supra* note 59, at 1286.

116. As Part IV argues, the fact that filtered dragnets can rapidly increase crime detection is also the source of its risk.

III. FILTERED DRAGNETS AND PRIVACY

Most of the courts, scholars, and civil society organizations that have considered the societal impact of filtered dragnets such as geofencing and reverse keyword searches have concluded that they pose serious threats to privacy.[117] Putting aside for a moment whether filtered dragnets are consistent with the full set of Fourth Amendment principles, this Part argues that filtered dragnets pose almost no threat to Fourth Amendment privacy. What I mean is, among all of the meanings and purposes that the right to privacy is meant to capture, the only ones that are meaningfully violated by filtered dragnets are related to abuses of power. The privacy expectations of the non-offender, which are the ones that predominate Fourth Amendment analysis, suffer at most a technical violation. If we separate out the anti-authoritarian goals of privacy, nothing is left of the privacy critique of filtered dragnets.

This does not mean that filtered dragnets are harmless—to the contrary, as Part V will argue, they pose significant dangers to civil liberties. But by ruling out *privacy* as the vector of abuse, courts can harvest the benefits of analytical precision and adjust Fourth Amendment law to better match the problems. This Part describes how courts and scholars have responded to filtered dragnets so far and then explains why Fourth Amendment principles are so poorly suited to address the negative reactions.

A. JUDICIAL REACTIONS TO FILTERED DRAGNETS

Courts are not prepared for the challenges that filtered surveillance pose to Fourth Amendment jurisprudence. Indeed, they are struggling as it is to find principled limits in more common and straightforward digital dragnet cases.[118]

So far, lower court opinions are surprisingly unfriendly to technologies and practices that will be the predicates to filtered dragnets. For example, Baltimore tried to set up a program called Aerial Investigation Research ("AIR") in which its police department collected and retained 45 days' worth of aerial surveillance footage, but would not be allowed to access the footage unless a violent crime occurred and was likely to be caught on camera.[119] Civil liberties organizations successfully challenged the program, arguing

117. *See*, *e.g.*, Guariglia, *supra* note 6.

118. For example, *Carpenter v. United States*, 138 S. Ct. 2206 (2018), wherein the Supreme Court considered the government's access to seven days' worth of cell site geolocation data and reached a holding without a rule. The access to records constituted a search requiring a warrant and probable cause, but the Court refused to say whether accessing data for a more limited amount of time would also be treated as a search. *Id.* at *11 n.3.

119. Slobogin, *Suspectless Searches*, *supra* note 29, at 962.

that the Fourth Amendment should constrain the government from amassing data that can be used for longitudinal location tracking no matter how constrained the Baltimore Police Department's access and use of the data might be.[120] The Fourth Circuit used the theoretical possibility of government access to information as a sufficient reason to find that a Fourth Amendment search on *all* Baltimore residents took place, regardless of the design, practice, and risk of abuse for the program.[121] If this reasoning is adopted throughout the judiciary, law enforcement will not be able to collect their own information for filtered dragnets and will have to rely on data that is collected and held by private industry.

Many courts have expressed similar reservations when the government asks a private company like Google to trawl through its data to conduct reverse searches, too.[122] But these opinions suggest that a warrant process that is sufficiently narrow and "particularized" so as to avoid disclosing data of innocent bystanders to the police would satisfy Fourth Amendment requirements.[123] This leaves an opening for filtered surveillance. It suggests that the automated scan that Google or another third party would perform of all its data in the process of identifying responsive records would *not* be a search in and of itself. In other words, the focus of the courts that have analyzed geofence warrants is not on the data that is scanned at all, but on the data that is ultimately revealed to police.

Courts might begin to clamp down on third-party scanning for law enforcement purposes following the logic of the Fourth Circuit's decision in the Baltimore AIR case. Many scholars are advocating for this, as I describe next. But it is still not clear that filtered dragnets will be understood to be a search at all given that they are designed to alert only when probable cause of a crime has been established. Even if police use computing technologies to automatically scan through large amounts of personal data, the constitutionally relevant event is the revelation and use of information to the government agents who are making decisions.[124]

120. Leaders of a Beautiful Struggle v. City of Baltimore, 2 F.4th 330, 346 (4th Cir. 2021).

121. *Id.*

122. United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022).

123. *Id.* at 927–32.

124. It is tempting to think the aggregation and accumulation of data for potential eventual use is itself a form of risk or harm. This is the reasoning behind the "mosaic theory," which captured the attention of some courts and scholars. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2011); Priscilla J. Smith, Nabiha Syed, David Thaw & Albert Wong, *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L.J. ONLINE 177, 201 (2011). Orin Kerr, who coined the term, is skeptical that courts can make it work. Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 346–47 (2012). It is worth noting that this theory does not comport with the attitudes of Americans. Matthew B. Kubler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 6 SUP. CT. REV. 205, 248 (2016).

This is best captured by the binary search doctrine—the rule establishing that, for example, a drug dog's alert is not a search under the Fourth Amendment because it reveals *only* the presence of contraband and criminal wrong-doing. There is little reason to believe the Supreme Court will backpedal. The Court has found that a universal fingerprinting database, possibly even one that requires involuntary contributions of fingerprints by individuals who are not yet in the database, could be justified, given that fingerprinting is an "inherently more reliable and effective crime-solving tool than eyewitness identification or confessions."[125] More recently, in *Maryland v. King*, the Supreme Court found that police can forcibly swab an arrestee and cross-check his DNA against the database of DNA samples from unsolved crimes.[126] The opinion focused almost entirely on the physical act of swabbing and took for granted that the cross-checking of a DNA sample to a crime database will not be a search because it reveals either nothing at all or reveals only a high-confidence match to a crime.[127]

That said, some of the Supreme Court decisions in the last ten years written by Justice Scalia incorporated a strong property-based formalism. In *United States v. Jones*, the use of a GPS device was a search not because of the sensitivity of the information gathered, but because of the *touching* of the suspect's car.[128] And in *Florida v. Jardines*, use of a drug-sniffing dog on a front porch was a violation of the Fourth Amendment because the practice involved a trespass with information gathering.[129] The fact that the information gathering was in the form of a binary search did not alleviate the flaw, according to the majority.[130] If Scalia's formalism for real and tangible property is extended to personal data, filtered dragnets could be considered a search of all individuals whose data is mechanically scanned in the process, irrespective of how trivial the invasion to them may be.

Even if courts come to agree that mechanically processing data is a Fourth Amendment search, this would still not guarantee the death of the filtered dragnet. They might be reasonable searches under the special needs or checkpoints doctrines.[131] In the context of checkpoints, bulk searches, and other dragnets, the Supreme Court has articulated the factors that it would use to determine whether the searches are "reasonable" despite a lack of individualized suspicion. These factors include the intrusiveness of the

125. Davis v. Mississippi, 394 U.S. 721, 727–28 (1969).
126. Maryland v. King, 569 U.S. 435, 465 (2012).
127. *See id.* at 445, 461–62.
128. United States v. Jones, 565 U.S. 400, 403 (2012).
129. Florida v. Jardines, 569 U.S. 1, 5–6 (2013).
130. *Id.* at 10–11.
131. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 449–50 (1990); Illinois v. Lidster, 540 U.S. 419, 426–27 (2004).

search, the public and government interest that is served by the dragnet, and the degree of oversight or limitations on discretion that are involved.[132]

Thus, judicial reasoning seems to be on a collision course between (a) cases that are eager to expand the recognition of privacy rights to cover all data subjects in large databases whose information is theoretically accessible to police and (b) cases that find highly probative "binary searches" are outside the ambit of Fourth Amendment prohibition.

B. SCHOLARLY REACTIONS TO FILTERED DRAGNETS

Lawrence Lessig saw this train wreck coming. In *Code*, he pointed out that the Internet and digital information technologies will allow police to identify a perpetrator with high confidence while remaining blind, by design, to the intimate details of the innocent. He explained that this will cause the privacy rationale for Fourth Amendment protection to lose relevance, at least when filtered dragnet investigations are possible. He expected these technologies would force a wedge between privacy and anti-authoritarian justifications for criminal procedure, when in the past, the two types of arguments traveled together.

Fourth Amendment scholars have doubled down on privacy.[133] They have lumped filtered dragnets together with all other digital surveillance in order to hinder police access. Dragnets of every sort, including the filtered sort, still suffer from analytical chaos because of value judgments and predictions that too often stay latent in the scholarship.[134] As a result, scholars are all over the map in terms of the proper treatment of digital dragnets, and none have focused on the right factors.

A few examples. Daphna Renan has argued that the collection, retention, and theoretical capability for law enforcement to access data is alone sufficient to constitute a privacy harm. Consent or a warrant should be required before the government collects any privately held data, and even before they access or request machine scanning of that data by third parties,

132. *See* Christopher Slobogin, *Government Dragnets*, 73 LAW & CONTEMP. PROBS. 107, 107–08, 127 (2010). The Court focused on constraints over agents' ad hoc discretion in *United States v. Martinez-Fuerte*, 428 U.S. 543, 559 (1976) (with respect to the location of a border and customs checkpoint). Justice Brennan, in dissent, pointed out that there remained a lot of agent discretion with respect to whom to focus on during the primary and secondary inspections, further emphasizing the importance of agent discretion. *See id.* at 576 (Brennan, J., dissenting).

133. *See generally* Sklansky, *supra* note 9; Ohm, *supra* note 9 (each arguing for strong and more capacious conceptions of privacy under Fourth Amendment law that will limit access to information no matter how or why it is sought). Even scholars like Andrew Ferguson and Neil Richards, who have focused on tyranny and power, have used those terms synonymously with surveillance capability. Ferguson, *supra* note 9, at 262–63, 266.

134. Christopher Slobogin took stock of the "analytical extremism" over a decade ago, and not much has changed. Slobogin, *supra* note 132, at 109.

irrespective of how limited and careful the readout is.[135] Natalie Ram has approvingly held up Maryland's law prohibiting law enforcement from using genomic databases to solve crimes unless they have received consent from all individuals whose data is in the genomic dataset.[136] More generally, this brand of scholars use access to data, rather than how it is used, as the *sine qua non* for Fourth Amendment analysis and ask why anybody should be under "lifetime surveillance."[137]

Scott Sundby and Nadine Strossen take the more moderate position that dragnets (of any sort) should be used only as a last resort,[138] though it is not clear they would apply their conclusions to *filtered* dragnets in particular. Eldar Haber, in considering how the Internet of Things can become a rich source of police investigatory data for reverse searches, advocates for a warrant requirement that goes beyond the "super-warrant" requirements of the current Wiretap Act to create an "ultra-warrant" requirement.[139] Since the super warrant requires police to exhaust all other means of investigating before securing a wiretap warrant, the effect and objective of Haber's recommendation is similar to Sundby's and Strossen's—to ensure that the criminal justice system strongly disfavors use of Internet of Things data in investigation.[140]

Continuing down the spectrum, some scholars appreciate the potential benefits of filtered dragnets and have advocated for a style of restraint that differs from prohibition or PC-based warrant requirements. Stephen Henderson and Kiel Brennan-Marquez argue that police departments should have a budget for searches and seizures (including digital investigations that, at least right now, operate outside the formal definition of a Fourth

135. Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1042, 1054–55 (2016).

136. Ram et al., *supra* note 70, at 1078–79. She has argued that Americans have a constitutional right, under the *Carpenter* decision, to the privacy of the genomic data held by a private third-party company and that unless consent to a law enforcement search is exhibited in some way, the police should not be able to ask or force the company to identify a match to a criminal sample. Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1366–67 (2019).

137. Lazer & Meyer, *supra* note 33, at 904 (summarizing what other scholars have asked with respect to including juveniles in DNA databases).

138. Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 446 (1988); Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173, 1176, 1197 (1988) (suggesting a challenged investigation should be invalid if there is a less *intrusive* option, and finding mass searches are more intrusive than individualized ones).

139. Haber, *supra* note 50, at 785.

140. 18 U.S.C. § 2518. Haber's reasoning is also consistent with Justice O'Connor's reasoning in a dissenting opinion, in which she argued suspicionless inspections should only be permitted when law enforcement would not be effective using traditional police tactics that build up reasonable suspicion or probable cause before a search takes place. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 674 (1995) (O'Connor, J., dissenting).

Amendment search) so that they are incentivized to use the most efficacious practices rather than the most expedient ones.[141] Christopher Slobogin has explicitly called for a more nuanced understanding of dragnets and suspicionless surveillance. He would allow dragnets that meet a standard of "generalized reasonable suspicion" where their efficacy outweigh the privacy intrusion enough to merit their use in criminal investigations.[142] Jeffrey Bellin recommends locating the Fourth Amendment interest in databases with the owner or holder of data, rather than the subject of the data searches, which would give a company the right to either consent to a search or to demand a warrant.[143] Andrew Ferguson would allow the use of dragnets as long as the legislative branch explicitly authorizes their use.[144]

Reaching the other end of the spectrum, some scholars (myself included), see the use of filtered dragnets as a move toward justice rather than away from it.[145] The prohibition of a highly reliable investigation tool is unethical when the prohibition would push police toward more invasive and less accurate investigation techniques and when serious crime would too often go undeterred. David Kaye and Michael Smith have made this argument with respect to DNA matching.[146]

Where does this leave us? Hopefully with an open mind and a hunger for reasoning from first principles.

C. THE POINTLESSNESS OF FOURTH AMENDMENT PRIVACY

Filtered dragnets will disrupt the equilibrium between the government, criminals, victims, and bystanders. That is obvious enough. Orin Kerr has made the descriptive and normative claim that courts intuitively adjust

141. Keil Brennan-Marquez & Stephen Henderson, *Search and Seizure Budgets*, 13 U.C. IRVINE L. REV. 389, 396–97 (2023). In my opinion, it would make more sense to limit government power by imposing a "prison budget" so that the state is forced to reserve incarceration resources for their most effective uses. *See* KLEIMAN, *supra* note 20, at 785.

142. Slobogin, *supra* note 132, at 139–40. Slobogin measures efficacy using the hit rate—the chance that an investigative technique will reveal relevant criminal evidence. *Id.* at 139. However, it is not entirely clear what he uses as the denominator in a hit rate. If courts are supposed to ask whether a person whose data is disclosed to police by a filtered dragnet is highly likely to be guilty of the investigated crime, filtered dragnets will always have high efficacy because they are defined to meet this standard. If the denominator is comprised of all individuals whose data is mechanically processed to find matches to the "fingerprint" of a crime, none of the filtered dragnets will meet the standard.

143. Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 270–72 (2019) (articulating an openness to considering some types of data and documents as personal to the consumer rather than owned and controlled by the third-party service provider, so context would play a role in edge cases under his proposal).

144. Ferguson, *supra* note 9, at 272.

145. *See generally* Bambauer, *supra* note 26.

146. D.H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413 (2003).

Fourth Amendment rules to strike a new balance between privacy and security whenever the government gains a significant new surveillance capability.[147] Filtered dragnets implicate only a few Fourth Amendment interests, and those few are not well served by the reasonable expectations of privacy test, by the warrant requirement, or even by intuitive adjustments. We are in new terrain in which a technology increases both privacy *and* crime control.

1. Theoretical Dimensions of Fourth Amendment Privacy

Borrowing from a rich literature that catalogues and elucidates the concept of privacy,[148] the following arise most frequently in the context of government intrusions and surveillance:

i. Freedom from Embarrassing Revelations, Social Dislocation, and Harassment

Perhaps the most common and robust form of privacy is the recognition that everybody has some legitimate, pro-social reason to want to keep licit details about their lives away from at least a subset of people.[149] They want the freedom that comes from relative obscurity,[150] where their decisions and behavior are not under the scrutiny and judgment of others.[151] Everybody deserves to be shielded, at least to some degree, from embarrassment over the things they have said or done that did not cause any lasting harm to others and that can be misunderstood.[152]

The scope of this interest ranges from trivial embarrassments (the regrettable hairstyle, the piece of toilet paper stuck to a shoe) to the truly life-changing (the ostracism of an HIV diagnosis, the physical attack carried out with the help of location information).[153] Much of the time, the sensitivity of

147. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 488–89 (2011).

148. Some attempts to organize the privacy discourse uses different stages of the information life cycle. *See generally*, *e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477 (2006); Jane Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205 (2012). For the purposes of this article, I have focused more heavily on articles that discuss the various types of risks and harms that occur when privacy is violated.

149. Sklansky, *supra* note 9, at 1107–10 (using the concept of refuge).

150. *See generally* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343 (2015).

151. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 854 (2022); *see also* Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1, 23 (2018); DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE 55–57 (2022) (describing how governments around the world have used details about licit-but-scandalous love affairs or other sexual secrets to suppress dissent).

152. *See* Citron & Solove, *supra* note 151, at 837 (discussing reputational harms).

153. *See* RICHARDS, *supra* note 65, at 146–51, 157–62.

a piece of information will depend greatly on context,[154] but the point is that "everyone has facts about themselves that they don't want shared, disclosed, or broadcast indiscriminately."[155] When information is permitted to leap from one context to another and to be used in unexpected ways, it will cause harm.[156]

Filtered dragnets relieve, rather than exacerbate, these concerns. By shielding data from police (and everyone else) unless and until they match the fingerprint of a crime, filtered dragnets keep as much information private as practically possible.[157] Indeed, if more police investigations were conducted through filtered dragnets, members of the community would be much more obscure and unknown vis-à-vis the state as compared with programs that involve heavy use of interviews, street patrols, traffic stops, and home searches.

ii. Freedom from Manipulation

An actor can exploit access to another person's data by discovering their vulnerabilities or gaps in rationality and then using those to persuade, cajole, or threaten the data subject into doing something.[158] Again, as with freedom from embarrassment, filtered dragnets present a lower, rather than higher, risk of this sort because law enforcement and other government actors are blinded from nonrelevant information. The only use to which the dragnet data are put involves solving a crime.

iii. Freedom from Indignity

The privacy literature prizes at least two forms of dignity that are not captured in other concepts on this list. First, privacy intrusions sometimes bring about an indignity from being singled out for suspicion.[159] Dragnets, whatever their faults, do not have this intrusion. Nearly everybody suffers the same indignity when bulk data is scanned, just as they do at TSA

154. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010).

155. RICHARDS, *supra* note 65, at 73.

156. *See* Solove, *supra* note 148, at 487–88; Cohen, *supra* note 151, at 1377; RICHARDS, *supra* note 65, at 134, 142–45.

157. Relatedly, filtered dragnets, when used as designed, will mitigate problems related to the dissolving boundaries between the state, private industry, and society by greatly limiting disclosure and use by law enforcement. For a description of dissolving boundaries, see BERNARD E. HARCOURT, EXPOSED 187–216 (2015).

158. *See* RICHARDS, *supra* note 65, at 151; Citron & Solove, *supra* note 151, at 846.

159. One reason that courts have concluded that roadblock-style DUI checkpoints are reasonable under the Fourth Amendment is that all people are treated with equal indignity. This is borne out in public opinion surveys, where checkpoints and roadblocks are consistently rated as being a relatively low intrusion compared with other investigation techniques. *See* Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at 'Understandings Recognized and Permitted by Society'*, 42 DUKE L.J. 727, 738 (1993).

checkpoints and DUI roadblocks.[160] Another form of dignity concerns being treated as a human rather than being processed as a faceless line of data. This has some overlap with the concept of "individualized suspicion," which I will discuss below, and which (in my opinion) filtered dragnets more than adequately should meet. Nonetheless, it is undeniable that filtered dragnets are entirely mechanical up until the point when a limited set of information is disclosed to police. Whether this *should* make a difference in the moral and legal status of filtered dragnets, though, is debatable.[161]

iv. Freedom from Anxiety

A common theme throughout the discourse revolves around the idea of loss of control and the uncertainty and anxiety that arises from it.[162] When the government has personal information about a subject, the subject is uncertain how the information could be used and fears that it may be used against them. This fear is, in and of itself, a social cost. Kiel Brennan-Marquez has argued that new data-gathering technologies create, and to some extent have already created, an omnipresent low-level form of anxiety similar to the feeling one gets when seeing a patrol car in the rear-view mirror and "feeling your pulse quicken; awareness heightened and senses alert, as you try not to break any traffic rules."[163]

A natural follow-up question is: What havoc *can* the government cause with data?[164] The greatest risk posed by filtered dragnets is to offenders, and it is the risk that their offense (and nothing more) will be detected. Thus, for filtered dragnets, freedom from anxiety calls for a freedom from law enforcement itself. It vindicates the rights of the supposedly "guilty" rather than the innocent. Fourth Amendment privacy recognizes no such interest.

160. This may explain why survey research finds that respondents generally do not find roadblocks intrusive; only 24% believed that they violate a reasonable expectation of privacy. James W. Hazel & Christopher Slobogin, *'A World of Difference'? Law Enforcement, Genetic Data, and the Fourth Amendment*, 70 DUKE L.J. 705, 745 (2021).

161. *See generally* FREDERICK SCHAUER, PROFILES, PROBABILITIES, AND STEREOTYPES (2006) (raising doubts about the differences between mechanical profiling and individualized consideration).

162. *See*, *e.g.*, Citron & Solove, *supra* note 151, at 841–42.

163. Brennan-Marquez, *supra* note 2, at 488.

164. Although some would quibble, most privacy scholars at least implicitly recognize (and sometimes explicitly state) that privacy has primarily an instrumental value rather than an intrinsic one. *See* RICHARDS, *supra* note 65, at 6. Richards later claims that "privacy is like other social goods, like public health or the environment," *id.* at 97, but this seems incorrect to me. Personal and environmental health are both intrinsic goods—more of it is an end in itself, and there is no such thing as too much.

2. Routine Compliance with Reasonable Expectations of Privacy

Data-driven policing has inspired a series of gloomy articles that predict the Fourth Amendment's reasonable expectations of privacy test has become irrelevant.[165] As long as the third-party doctrine stands, permitting police to access data held by third-party companies without justification or oversight, privacy will be insufficiently protected. I agree with these scholars.[166] But courts are already addressing this problem. Cases like *Carpenter v. United States*—in which the Supreme Court found that police access to several days' worth of geolocation data constitutes a search that would require a warrant or appropriate warrant exception—have proven that for suspect-driven searches, Fourth Amendment privacy is not yet irrelevant and is becoming more powerful by the day.[167]

Nevertheless, the reasonable expectations of privacy test is very unlikely to impede the adoption of filtered dragnets. That test has repeatedly been interpreted to deny privacy interests of the guilty. "[A]ny interest in possessing contraband cannot be deemed 'legitimate,' and thus government conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest.' "[168] Jed Rubenfeld's synthesis of Fourth Amendment caselaw seems to get it right: the Fourth Amendment aspires to support "a justified belief that if we do not break the law, our personal lives will remain our own."[169] Filtered dragnets pass this test.[170]

To be clear, there are reasons, independent of privacy, to protect law-violators-as-violators. These arguments, which I describe in depth in the next Part, are critical for understanding the threat from filtered dragnets. But they are only loosely related to "privacy" as the term is typically used, and they will not be incorporated into the reasonable expectations of privacy unless that test is changed beyond all recognition.

165. *See*, *e.g.*, Ohm, *supra* note 9, at 1320; Kimberly N. Brown, *Outsourcing, Data Insourcing, and the Irrelevant Constitution*, 49 GA. L. REV. 607, 659–63 (2015).

166. Bambauer, *supra* note 26, at 209.

167. Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018).

168. Illinois v. Caballes, 543 U.S. 405, 408 (2005).

169. Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 129 (2008) (differentiating the Fourth Amendment's guarantee to security from a right to privacy).

170. For binary searches, the reasonable expectations of privacy test adopts the "nothing to hide" attitude that privacy scholars very often condemn. *See* RICHARDS, *supra* note 65, at 134. *See generally* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADE-OFF BETWEEN PRIVACY AND SECURITY (2011). Despite the scholarly criticism, it is an attitude that the general public shares with the Court. Public opinion surveys demonstrate that Americans' taste for privacy is strongly influenced by whether they believe the person being searched has committed a crime or not. *See* Slobogin & Schumacher, *supra* note 159, at 759.

3. The Irrelevance of the Warrant Requirement

In *U.S. v. Chatrie*, the geofence case described earlier, the court suggested it would approve a geofence warrant process if a magistrate or court got to make a probable cause determination before the geolocation data of a target were de-anonymized.[171] Generalizing to other filtered dragnets, law enforcement would seek a warrant after the filtered dragnet system alerts, but before any identifying data is revealed.

This process might be a good component for accountability and oversight, and to ensure that filtered dragnets are performing at or above the expected "hit rate," but it is hard to imagine why a warrant could ever be denied. A warrant is valid as long as it is issued by a neutral judge or magistrate, is based on probable cause, and states with sufficient particularity what is to be searched or seized.[172] The standards for both probable cause and particularization will be met—more than met—given that the definition of filtered dragnets I am using requires them to withhold information until the probability that the target has engaged in the investigated crime meets a high standard. As for particularization, because the filtered dragnet procedure begins with the signatures of a crime and works backwards to find the perpetrator, the profile for matching (what I have been calling the "fingerprint" of the crime) is as particularized to a crime as it can be.[173]

Privacy advocacy groups have argued that warrants issued for reverse searches are tantamount to general warrants because they do not identify (or even anticipate) a particular suspect before they are issued.[174] But the only similarity that geofence warrants have to general warrants from the Colonial Era is the lack of a named suspect. In every other way, geofence warrants restrict the information that is revealed to that which is closely linked to a particular crime. By comparison, general warrants authorized agents of the colonial government to look for stolen or untaxed goods anywhere the agent "[should] think convenient to search."[175] The only manner in which the geofence warrant is unconstrained—by allowing police to discover who the

171. United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022).

172. California v. Acevedo, 500 U.S. 565, 569–72 (1991); Illinois v. Gates, 462 U.S. 213, 230 (1983).

173. Emily Berman argues that one of the purposes of the individualization requirement of the Fourth Amendment is to provide an opportunity for a suspect to challenge the evidence and beliefs of a police officer who thought they had probable cause to make the stop or search. Emily Berman, *Individualized Suspicion in the Age of Big Data*, 105 IOWA L. REV. 463, 467 (2020). In this example, the non-privacy goal can be reconciled and adapted to filtered dragnets by requiring law enforcement to review and understand the data that connect the suspect to a crime.

174. Guariglia, *supra* note 6.

175. Brennan-Marquez & Henderson, *supra* note 141, at 402 (citing WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 233 (2009)).

suspect is rather than requiring police to come with a suspect in mind—is a feature of geofence warrants that should be praised, as it limits the discretion of the police to select their targets in advance. This is the critical distinction between filtered dragnets like geofence warrants or DNA searches and suspect-driven searches—one that scholars and commentators too frequently gloss over.[176]

Thus, a warrant requirement is irrelevant to the adoption of filtered dragnets, apart from the time, resources, and general system friction involved, because they should routinely be granted.

***

Privacy scholars are courting disaster by lumping filtered dragnet techniques in with other types of dragnets and digital searches. Even if there are court victories in the short term, they will be pyrrhic. The very concept of "privacy" will become increasingly vulnerable to the "I have nothing to hide" argument that is loathed by the field (and rightly so).[177] Courts might fail to sufficiently constrain *unfiltered* dragnets and suspect-driven investigations because of the utility and low harm of filtered dragnet techniques that happen to share the same Fourth Amendment bucket.

Arguments against mass surveillance often start with the observation that surveillance fundamentally shifts power from the surveilled to the surveillor.[178] This is true as far as it goes, but if the surveillor is constrained and can only see evidence of a crime, that power shift will often be a desirable one. In fact, assuming that the law is legitimate, the enforcement of a law is one of the most legitimate acts the government can do. The burden is therefore on surveillance scholars to explain why those who have violated the law may have justified interests in being protected from state detention and prosecution, *even when* their law-abiding conduct remains private. There are answers to this challenge, but they sound in tyranny rather than invasions of privacy. There is a virtue to being precise about the problems of filtered dragnets without reliance on capacious notions of privacy that would implicate nearly every law enforcement function.

176. *See generally, e.g.*, Ram, *supra* note 136 (comparing the suspect-driven search in *Carpenter* to the crime-driven searches in the DNA forensic setting without recognizing the categorical differences between the two).

177. *See generally* SOLOVE, *supra* note 170.

178. "Privacy is about more than just keeping human information unknown or unknowable. . . . Put simply, privacy is about power." RICHARDS, *supra* note 65, at 3. Richards goes on to say, "we need to craft reasonable rules and protections so that we can maximize the good things about these technologies and minimize the bad things." *Id.* at 5.

IV. FILTERED DRAGNETS AND TYRANNY

Filtered dragnets will provide a highly concentrated dose of criminal detection. Even though, in theory, the whole point of having law enforcement departments is to detect and prosecute crime, a drastic increase in criminal detection can have toxic effects on society. The dynamics and interaction of other criminal justice factors have come of age in a time of low detection and only make sense if detection continues to be difficult.

This Part begins by revisiting the interests that privacy scholars have identified that *would* be affected by filtered dragnets. Each of them is really an anti-tyranny concern garbed in the language of privacy. If we are more explicit about the goals and analyze the risks of authoritarianism that filtered dragnets may drag along with them, the problems (and, therefore, the remedies) become much more obvious.

The true threats from filtered dragnets are that: (1) many Americans will confront a real risk of criminal liability based on our overbroad criminal codes; (2) prosecutions of those crimes could lead to life-altering detentions in our inhumane prison systems; and (3) without the shield of abysmally low detection rates, the only protection is lenity, which is no protection at all from a government that attempts to exert authoritarian power.

A. PRIVACY AS A STALKING HORSE FOR ANTI-AUTHORITARIANISM

Neil Richards claims that privacy is a necessary bulwark "if we want political freedom against the power of the state."[179] But privacy is inadequate on its own to protect the broad range of liberty and equality interests that arise with abuse of power. Filtered dragnets prove it. They can be used to trample liberties and to serve the public unequally even though the government will not know any irrelevant details about licit activities.

Instead of trying to expand the meaning of "privacy" to tackle every possible state abuse, courts and criminal justice scholars alike should seize the moment and force constitutional theory to shift its focus from privacy to anti-authoritarian constraint. To be sure, courts should continue to refine the conception of Fourth Amendment privacy interests to address unfiltered digital dragnets. But if we have any hope of harnessing the great potential of filtered dragnets without creating a despot's playground, the Supreme Court will need to simultaneously cultivate an anti-authoritarian strand of Fourth Amendment rules.

179. RICHARDS, supra note 65, at 7.

When surveillance scholars use the concept of privacy to curb abuses of power, they are concerned about unnecessary social control and abuses of discretion.[180]

1. Unnecessary Social Control

Law enforcement serves the obvious and highly valued function of social control. As Kiel Brennan-Marquez explains, "we *want* people to worry about breaking the rules"[181]—at least, when the rules are good rules, and when the consequences for breaking rules are proportional and fair. However, Brennan-Marquez is concerned that data-driven policing tools will leave the police "awash in probable cause," allowing them to stop, search, or arrest nearly anybody.[182] This concern gets to the heart of the matter. But it is ultimately a critique of the *substance* of criminal law and the *discretion* of criminal justice decisionmakers. These are the same themes that Bill Stuntz repeatedly raised when he critiqued Fourth Amendment cases and scholars for allowing privacy to be a distraction from more pressing threats.[183]

Let us return for a minute to Brennan-Marquez's metaphorical driver who has just discovered a patrol car in the rearview mirror. If the government had done a massive purge of its penal codes and the only crimes left on the books were murder, rape, arson, armed robbery, and aggravated assault, and if false positive police error was vanishingly small, would the driver feel anxiety? For a time after the change, yes of course. There will be a short-term period of distrust and adjustment when technologies or rules change suddenly and dramatically.[184] But in the long run, anxiety will ebb under the pressure of persistent feedback of non-events and the absence of harm.

Public opinion surveys find that attitudes about privacy are mediated through attitudes about the substantive criminal law that is being enforced: a dog that is sniffing for bombs is perceived as less privacy-invasive than a dog that sniffs for drugs even though the experience is identical for the investigation target (at least, up until the moment that the dog alerts, that is).[185] If assessments of privacy change not because of the revelations or

180. They are also concerned about illegal use of a tool by rogue agents. *See*, *e.g.*, Lazer & Meyer, *supra* note 33, at 906 (misusing DNA databases to extract phenotypes). There is always a risk that the government will use surveillance tools in violation of constitutional rules, statutory restrictions, or their own internal policies, but compared to opportunities of individual officers to abuse warrant or investigation practices in real space, filtered dragnets are more likely to be auditable.

181. Brennan-Marquez, *supra* note 2, at 489.

182. *Id.* at 491.

183. *See generally* STUNTZ, *supra* note 15.

184. People used to feel nervous about Caller ID, and at the advent of electricity, wealthy homeowners used to hire servants to turn on lights. ADAM THIERER, PERMISSIONLESS INNOVATION 70 (2016).

185. Bambauer, *supra* note 25, at 1205. *See also* Slobogin & Schumacher, *supra* note 159, at 767

techniques that are used but because of the *crimes* that are prosecuted, the concept of privacy is standing in for objections to the substance of the law.

The concern about unnecessary social control is better addressed by defining, as best we can, which types of antisocial conduct rise to the level of being worthy of criminal punishment and which do not. And the concern raises important questions about whether criminal violators are treated too harshly. Privacy is a blunt instrument for these purposes. It draws lines that have only a vague relationship to the distinctions we mean to draw.

2. Selective Attention

Another serious concern is that police might make use of a system of surveillance to rifle around for something to use against a specific person or group.[186] Motivations could range from political persecution to racism to personal vengeance to simply wanting to make a quota or appear well in performance metrics within a bureaucratized police department.

As with unjustified social control, the problem of discretion and selective attention is only indirectly related to privacy. Indeed, it is not even clear that privacy has *any* positive influence on police discretion. Privacy steers police toward information sources that disproportionately expose low-income and minority groups: if police cannot bring a drug-sniffing dog to a house, they will bring it to apartments and cars.[187] If police cannot search the full set of government and commercial DNA databases for a match to a crime scene sample, they will just use the government's database of arrestee DNA data.[188] At the same time, police can also engage in selective *inattention* by avoiding leads that could cause problems for friends or powerful people and by failing to give crimes perpetrated against low-status victims the same attention as the ones inflicted on high-status victims. When communities are under-protected, it is a form of *too much* privacy vis-à-vis the government.

The policy antidote to government discretion and bias is to directly limit discretion and bias. Filtered dragnets already do this, to some extent, because once they are employed, police lose control over who will ultimately be identified as a suspect. But law enforcement can still deploy filtered dragnets unfairly when selecting the neighborhoods or cases in which filtered dragnets will be deployed.[189]

(speculating that the dangerousness of the investigated crime could explain some of their survey results).

186. Dan Markel, *Against Mercy*, 88 MINN. L. REV. 1421, 1476–77 (2003); Joh, *supra* note 17, at 200; Brennan-Marquez, *supra* note 2, at 490–92.

187. Bambauer, *supra* note 26, at 246.

188. Ram et al., *supra* note 70, at 1078.

189. This is why Henderson's and Brennan-Marquez's proposal of search and seizure budgets seem inadequate to me: the concept of a budget does not guarantee that the budget will be spent wisely. *See*

Thus, in the context of filtered dragnets, "privacy" concerns are attempting to capture and curb something bigger: too much social control at the discretion of the government.

B. FILTERED DRAGNETS AND THE RISKS OF TYRANNY

An authoritarian regime thrives when it has unlimited discretion to issue stiff punishment based on criminal behavior that has negligible negative consequences (and possibly even positive consequences) to society. This threat is blunted if the state lacks the means to acquire evidence of criminal behavior, but with reliable surveillance mechanisms, law enforcement officials will be able to exert as much social control as they please, because nearly every person can be charged with a crime.[190]

Thus, filtered dragnets present risks that run along three vectors: (1) overbreadth of criminal law; (2) overly harsh punishment of criminals; and (3) overly discretionary investigations and enforcement. If these three forces remain unchecked, filtered dragnets could cause more harm than good. In the wrong hands, filtered dragnets could cause catastrophic risks of the sort that the Constitution is meant to prevent.

1. Overbreadth of Criminal Law

A government that has the capacity to detect criminal behavior at very high rates must come under heightened standards of care when it promulgates or maintains its criminal laws. If we wince at the thought that *everybody* who commits a minor offense will get caught and will be prosecuted if they do not seem to qualify for a privilege or defense, this is a sign that the conduct is a poor fit for criminal law, and legislators must consider alternatives (e.g., warnings, civil fines, or positive incentives for pro-social conduct) instead.[191]

Right now, constitutional case law does very little to constrain the creation of criminal laws. Outside criminal statutes that would intrude upon specific individual liberties recognized in the Bill of Rights, the courts hold legislatures to very low standards of care (the rational basis test).[192] This latitude on substance has a curious relationship with the procedural restrictions imposed by the Fourth Amendment: as long as police have

generally Brennan-Marquez & Henderson, *supra* note 141.

190. KLEIMAN, *supra* note 20, at 172–73.

191. Social stigma also provides a significant source of deterrence and self-control, often better than fear of punishment. STUNTZ, *supra* note 15, at 52–53 (citing Daniel S. Nagin, *Criminal Deterrence at the Outset of the Twenty-First Century*, 23 CRIME & JUST. 1, 4–5 (1998)).

192. *See generally* Jeffrey D. Jackson, *Classical Rational Basis and the Right to Be Free of Arbitrary Legislation*, 14 GEO. J.L. & PUB. POL'Y 493 (2016).

probable cause to believe that a person is violating or has violated a criminal law, police can make an arrest or initiate a search, no matter how trivial the offense. Thus, in *Atwater v. Largo Vista*, the Supreme Court found that the government acted within the bounds of the constitution when a police officer arrested a woman who was driving with two small children for the violation of a seatbelt law.[193]

Even if the Court is reluctant to interfere with legislators' management of criminal codes, common sense dictates that some crimes are much worse than others. The state's attention should focus on conduct that causes serious harm to others. There is a reason, for example, that the states that have regulated familial DNA-matching programs have allowed their use only for serious offenses like murder and rape,[194] and Baltimore's Aerial Investigation Research ("AIR") system, before it was dismantled, was restricted to use in investigating a limited set of very serious crimes.[195] It is the same reason that the federal Wiretap Act permits courts to issue wiretap orders only when there is probable cause to investigate one of the explicitly listed serious criminal offenses.[196] The same impulse explains why there is scholarly criticism and public outrage when a surveillance system adopted for the purpose of detecting one set of serious criminal violations (like smuggling or terrorism) is simultaneously used to detect violations of drug laws.[197] The unstated assumption is that some crimes should be detected as well as possible (terrorism, for instance) and some should not.[198]

The fact that state and federal criminal law has dramatically expanded in quantity and complexity is not in dispute.[199] And yet, curiously, responses to the problem tend to focus on procedural rather than substantive limits.[200] The unchecked growth of substantive criminal law ironically creates a problem for public safety because the fear of prosecution prompts a demand for privacy and law enforcement obstruction.[201]

193. Atwater v. Largo Vista, 532 U.S. 318, 323–24 (2001).
194. Ram, *supra* note 34, at 781.
195. Slobogin, *Suspectless Searches*, *supra* note 29, at 962.
196. 18 U.S.C. § 2516.
197. Renan, *supra* note 135, at 1060–63 (describing slippage between "silos" of law enforcement).
198. Craig Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951, 1019–22 (2003).
199. SILVERGATE, *supra* note 10, at 268. "All of this is to say, of course, that many of those prosecuted are not real criminals who engaged in real crimes defined by clear and reasonable laws." *Id.*
200. *See, e.g.*, Reynolds, *supra* note 10 (advocating for due process constraints on charging decisions).
201. This is, in a nutshell, the reason that Paul Ohm and other privacy scholars use law enforcement efficiency as a measure of Fourth Amendment violations. Ohm, *supra* note 9, at 1346. As Mark Kleiman put it, "improved enforcement of a law that should not have been passed in the first place can be a loss rather than a gain." KLEIMAN, *supra* note 20, at 172.

The first and most obvious reason to place limits on criminal liability is to reduce the opportunity for unnecessary social control. The relationship between the government and the governed changes profoundly when a crime has been committed. The defendant in *Atwater* should have put a seatbelt on her children, and the government has an interest in encouraging, even requiring, that behavior. But not through criminal law.[202] A second reason to constrain the substance of criminal law is to increase compliance with the rules we care about most.[203] Overstuffed criminal codes also bleed into the problems of law enforcement discretion (discussed at greater length below) because the government has too much power to decide which members in the nation of criminals to send to prison.

Consider two examples that illuminate the problem through opposite ideological lenses. First, abortion will be criminalized in many states in light of *Dobbs v. Jackson Women's Health Organization*.[204] Some states are considering criminal liability for women who seek out an abortion.[205] For liberals and progressives, criminal liability for abortion-seekers represents an intolerable overreach of the state. To combat the substance of these laws, organizations such as the ACLU have already issued warnings about the risk that geofence searches could facilitate arrests and prosecutions of a law that a sizable portion of the state's constituents believe is unjust.[206]

202. Josh Bowers has criticized the *Atwater* decision, arguing that the reasonableness requirement of a Fourth Amendment seizure should protect individuals from "pointless indignities." Josh Bowers, *Probable Cause*, *Constitutional Reasonableness*, *and the Unrecognized Point of a 'Pointless Dignity'*, 66 STAN. L. REV. 987, 1010 (2014). Every arrest is an indignity, of course, so the power of Bowers' observation is the *pointlessness* of Atwater's arrest.

203. Bloated criminal codes reduce law-abiding conduct because they cause what Murat Mungan calls "stigma dilution." Murat Mungan, *Stigma Dillution and Over-Criminalization*, 18 AM. L. & ECON REV. 88, 88 (2016). If functional and productive members of society are regularly engaged in violations of the criminal laws, the fact that a person has committed a crime (or has been convicted of it) loses its negative status signal.

204. Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

205. Andy Rose, *Alabama Attorney General Says He Has Right to Prosecute People Who Facilitate Travel for Out-of-State Abortions*, CNN (Aug. 31, 2023, 7:39 AM), https://www.cnn.com/2023/08/31/politics/alabama-attorney-general-abortion-prosecute [https://perma.cc/B7RP-ANNL].

206. Chad Marlow & Jennifer Stisa Granick, *Celebrating an Important Victory in the Ongoing Fight Against Reverse Warrants*, ACLU (Jan. 29, 2024), https://www.aclu.org/news/privacy-technology/fight-against-reverse-warrants-victory [https://perma.cc/C2PB-NGKH].

By contrast, conservatives might be concerned about overzealous enforcement of gun restrictions.[207] Geolocation and credit card transaction data could be used to create a filtered dragnet that finds individuals without a gun license who cross state lines, attend a gun show, make a sizable purchase, and immediately return to their state.

In both cases, perceived flaws in the substance of the law would not be so troubling if the laws carried only modest punishments—warnings or fines, for example, rather than the incarceration and downstream labor and housing problems that inevitably follow conviction.[208] But given the breadth and severity of criminal law, plus the mostly unchecked discretion that police departments have when deciding *which* among an ocean of technical criminal violations to investigate, the prospect of near-perfect detection takes on a more sinister character. Thus, when people have reservations about, for example, Alexa devices being used to detect the sounds of domestic violence, the reservations stem not from the specific use case but the general capabilities. They wonder, for good reason, what mischief can be made from such a technology when the set of conduct that is forbidden and harshly punished is sprawling and unevenly enforced.[209]

Criminal codes are often expanded when the state has not gotten a handle on crimes of violence and property theft. The criminalization of vice (alcohol and drugs) was supported by the community not necessarily out of concerns that the drugs themselves cause to users but because of the "unconscionable violence" that came along with trafficking and addiction.[210] In other words, substantive criminal law is expanded to compensate for deficiencies in the detection and prosecution of crimes that were already on the books so that police could arrest for lower level crimes and (stochastically) reduce the incidence of more serious crimes.[211] If detection of the serious crimes were more functional, this should relieve the need for sprawling criminal codes.

207. Several credit card networks now flag gun transactions automatically. Landon Mion, *Visa Joins Mastercard, AmEx in Specifically Labeling Gun Store Sales*, N.Y. POST (Sept. 11, 2022), https://nypost.com/2022/09/11/visa-joins-mastercard-amex-in-specifically-labeling-gun-store-sales [https://perma.cc/M554-C4L9].

208. *See generally* JAMES B. JACOBS, THE ETERNAL CRIMINAL RECORD (2015).

209. Jessica Bulman-Pozen & David E. Pozen, *Uncivil Obedience*, 115 COLUM. L. REV. 809 (2015) (illustrating that the set of legal rules operating on U.S. residents is often so unrealistic that fastidious obedience to them can annoy and frustrate law enforcement agents).

210. FORMAN, *supra* note 7, at 129 (quoting Carl T. Rowan, *Locking Up Thugs Is Not Vindictive*, WASHINGTON STAR (Apr. 23, 1976)).

211. K. JACK RILEY, NANCY RODRIGUEZ, GREG RIDGEWAY, DIONNE BARNES-PROBY, TERRY FAIN, NELL GRIFFITH FORGE, VINCENT WEBB & LINDA J. DEMAINE, JUST CAUSE OR JUST BECAUSE?: PROSECUTION AND PLEA-BARGAINING RESULTING IN PRISON SENTENCES ON LOW-LEVEL DRUG CHARGES IN CALIFORNIA AND ARIZONA 76 (2005).

Hence the dilemma: better crime detection could help stop the pattern of an upward ratchet, but as long as the criminal codes are already sprawling, there will be resistance to increasing detection.

2. Overly Harsh Punishment

On severity of punishment, the United States stands out among developed nations. We use incarceration intensively. In France and the U.K., a criminal who punches a person in the nose would be sentenced to less than six months in jail.[212] The same conduct in the U.S. would result in a sentence of about three years.[213] Moreover, no outsider would mistake our prisons for institutions of rehabilitation: the entire sentence is usually carried out in a facility that is punishing, with drab quarters, humiliating toilet and bathroom facilities, and rancid food.[214] Once released, the negative consequences continue as the housing and labor markets penalize criminal convicts.[215] Long sentences also create risks of abuse by giving police officers and other state agents leverage to extract bribes, pleas, and false confessions.[216]

The harshness of our sentences is the byproduct of a low detection rate. Communities that at various times have been disfigured from crime waves tend to demand more and harsher criminal penalties.[217] The intuitive appeal of using long prison sentences to make up for low detection rates became the explicit policy of federal and local governments following the landmark work of Gary Becker. Becker modeled crime with a simple formula determined by the probability of conviction and the severity of punishment.[218] Because it is much easier and cheaper for the state to ratchet

212. U.K. PARLIAMENT, COMPARATIVE PRISON SENTENCES IN THE EU, HOUSE OF COMMONS LIBRARY (2015), https://commonslibrary.parliament.uk/research-briefings/cbp-7218 [https://web.archive.org/web/20240510064827/https://commonslibrary.parliament.uk/research-briefings/cbp-7218/.

213. U.S. SENTENCING COMMISSION, SOURCEBOOK OF FEDERAL SENTENCING STATISTICS TABLE 15 (2020), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/annual-reports-and-sourcebooks/2020/Table15.pdf [https://perma.cc/33WN-APC8]. Note, though, that the differences for non-violent offenses like theft appear to be smaller (fewer than 6 months in U.K. compared to a median of 8 months in the U.S.). *Id.*

214. CRAIG HANEY, CRIMINALITY IN CONTEXT 335–44 (2020).

215. FORMAN, *supra* note 7, at 219. *See generally* MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS (2012).

216. Dharmapala et al., *supra* note 67, at 111 (citing David Friedman, *Why Not Hang Them All?: The Virtues of Inefficient Punishment*, 107 J. POL. ECON. S259 (1999)).

217. James Forman Jr.'s book *Locking Up Our Own* documents the set of factors and conditions that led communities of color to make entirely understandable demands for greater punishment, even though the result of those efforts have not had their intended effects. FORMAN, *supra* note 7, at 124.

218. Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POLIT. ECON. 169, 170 (1968). *See also* A. Mitchell Polinsky & Steven Shavell, *The Theory of Public Enforcement of Law*, *in* HANDBOOK OF LAW AND ECONOMICS 421 (2007).

up punishment than to catch more perpetrators, his work persuaded many politicians to manage crime through tough sentencing.[219]

The sparseness of Becker's model for crime rates leaves much to be desired for anybody looking for a comprehensive explanation for crime—crime, of course, has a range of social and economic causes[220]—but as Part II explained, there is little doubt that detection has a significant influence over the amount of crime in a given community.[221] Punishment, by contrast, seems to have a U-shaped relationship to recidivism, where no punishment and long, harsh punishment both tend to increase the odds that a perpetrator will recidivate.[222]

I do not want to overstate the case for reducing prison time. Roughly half of the inmates in prison are individuals with such consistent sociopathic and antisocial behaviors that for *those* inmates, long-term incapacitation has positive externalities. Not only does incapacitation prevent these particular individuals from committing additional crimes (specific deterrence), but their families and particularly children may benefit from having less, rather than more, exposure to them.[223] Nevertheless, the social costs of harsh punishment do not seem to serve deterrence or otherwise be justified outside the context of heinous or repeated criminal activity.

219. Cass R. Sunstein, David Schkade & Daniel Kahneman, *Do People Want Optimal Deterrence?*, 29 J. LEGAL STUDS. 237 (2000).

220. These are the levers most directly under the control of a politically accountable legislators, mayors, police departments, and prosecutors, but there are of course other factors. *See generally* Stephen J. Schoenthaler & Ian D. Bier, *The Effect of Vitamin-Mineral Supplementation on Juvenile Delinquency Among American Schoolchildren: A Randomized, Double-Blind Placebo-Controlled Trial*, 6 J. ALT. & COMPLEMENTARY MED. 7 (2000) (discussing malnutrition as a factor in crime); CIVIC RESEARCH INSTITUTE, THE SCIENCE, TREATMENT, AND PREVENTION OF ANTISOCIAL BEHAVIORS (Diana H. Fishbein ed., 1999) (reviewing evidence of the impact of alcoholism, drug use, sexual abuse, cognitive and genetic factors, and family/gender role factors); CLIFFORD R. SHAW & HENRY D. MCKAY, JUVENILE DELINQUENCY AND URBAN AREAS (1942) (discussing the effect of weakened or disorganized social institutions on crime; this work planted the roots of what would become the "broken windows" theory).

221. EXECUTIVE OFFICE OF THE PRESIDENT, ECONOMIC PERSPECTIVES ON INCARCERATION AND THE CRIMINAL JUSTICE SYSTEM 36–40 (2016) (citing to the empirical literature finding that increased incarceration reduces crime, but less effectively than equivalent increased spending on police); ANDREW VON HIRSCH, DOING JUSTICE: THE CHOICE OF PUNISHMENTS 62–65 (1976). *See generally* Raymond Paternoster, *The Deterrent Effect of the Perceived Certainty and Severity of Punishment: A Review of the Evidence and Issues*, 42 JUST. Q. 173 (1987); Beau Kilmer, Nancy Nicosia, Paul Heaton & Greg Midgette, *Efficacy of Frequent Monitoring with Swift, Certain, and Modest Sanctions for Violations: Insights from South Dakota's 24/7 Sobriety Project*, 103 AM. J. PUB. HEALTH e37 (2013); Lawrence W. Sherman, *Police Crackdowns: Initial and Residual Deterrence*, 12 CRIME & JUST. 1 (1990).

222. Amanda Y. Agan, Jennifer L. Doleac & Anna Harvey, *Misdemeanor Prosecution* (Nat'l Bureau Econ. Rsch., Working Paper No. 28600, 2021).

223. *See generally* Samuel Norris, Matthew Pecenco & Jeffrey Weaver, *The Effects of Parental and Sibling Incarceration: Evidence from Ohio*, 111 AM. ECON. REV. 2926 (2021); Sara R. Jaffee, Terrie E. Moffitt, Avshalom Caspi & Alan Taylor, *Life with (or Without) Father: The Benefits of Living with Two Biological Parents Depends on the Father's Antisocial Behavior*, 74 CHILD DEV. 109 (2003).

Over-punishment and criminal detection are inextricably connected. We cannot expect to find a political will to reduce punishment unless the police have—*and use*—new means to detect and root out crime. Filtered dragnets can jolt and resettle the criminal justice system in a new equilibrium where detection, rather than harsh punishment, is the key mechanism for crime control.

3. Discretionary Application

Once the police have committed to investigating a particular crime, filtered dragnets take discretion away from the police to drive the investigation. But there are other points in time before and after a filtered dragnet may be used when government agents can exert control over the process:

i. Selective Protection

When it comes to serious crimes of violence and theft, American police forces have a troubling history of systematically ignoring the suffering of minority communities. Police once actively conspired to deprive former slaves of their right to protection by joining the murderous mobs.[224] Over the subsequent century, police started to exhibit a more passive form of selection by simply not investigating and pursuing crimes committed against African-Americans as zealously as crimes committed against whites.[225] This is a form of inequality that is not adequately addressed in constitutional caselaw.[226] Thus, courts must prevent police from using filtered dragnets to solve crimes committed against one set of privileged crime victims while failing to use the same tools to solve comparable (and comparably detectable) crimes committed against others.

224. STUNTZ, *supra* note 15, at 104–05.

225. This trend can be seen in studies finding that models predicting enforcement and sentencing often include a large and statistically significant effect for the race of the victim (with white victims receiving better protection). John J. Donohue III, *An Empirical Evaluation of the Connecticut Death Penalty System Since 1973: Are There Unlawful Racial, Gender, and Geographic Disparities?*, 11 J. EMPIRICAL LEGAL STUDS. 637, 640 (2014).

226. In fact, in the context of capital sentencing, the Supreme Court has explicitly said that there is *not* a constitutional guarantee that would prevent discretionary leniency to be executed arbitrarily. McCleskey v. Kemp, 481 U.S. 279, 292 (1987).

ii. Selective Crackdowns

Police also decide which crimes to target,[227] and when and where to focus their resources.[228] For example, police will decide which crime scene images should be subjected to facial recognition. There is no guarantee that they will pursue arrest and prosecution of violent or destructive participants at Black Lives Matter protests or at a pro-Trump rallies with the same vigor.

iii. Controlling the Data

Whether police use government-held data or data held by private companies to operate a filtered dragnet, they can exert some influence over the process if they are allowed to use a subset of available information to run through the filtered dragnet.[229] For example, if the government were able to limit DNA-matching to the data collected from ex-convicts only, or if a geofence warrant could direct a service provider to look for matching records only among customers who live in a certain precinct, the police could do an end run around the discretion-reducing function of filtered dragnets.

iv. Downstream Decisions

After a suspect is identified by a filtered dragnet, police and prosecutors still have unchecked power to use leniency and to simply not pursue the leads that they do not like.[230]

The unifying theme across these decision-making practices is that the Supreme Court has avoided interfering with law enforcement discretion any time it has a plausible connection to judgment about the best use of resources. In *Whren v. United States*, the Supreme Court rejected a constitutional challenge by a criminal defendant who was pulled over for making an illegal U-turn. The defendant argued that the police would not have pulled over a white person, or any person about whom the police did not have a pre-

227. Mila Sohoni, *Crackdowns*, 103 VA. L. REV. 31, 33–34 (2017).

228. *See generally* Jeffrey Fagan, Garth Davies & Adam Carlis, *Race and Selective Enforcement in Public Housing*, 9 J. EMPIRICAL LEGAL STUDS. 697 (2012) (describing selective enforcement of criminal trespass by race or public housing status).

229. Indeed, this is one counterintuitive reason it may be better to have police access data from third-party companies rather than collecting it themselves, so that private industry may serve as a source of public information and whistle blowing. FARHANG HEYDARI, HOOVER INST., AEGIS SERIES PAPER NO. 2106, UNDERSTANDING POLICE RELIANCE ON PRIVATE DATA 6 (2021).

230. Discretion among judges at the point of sentencing seems to reduce racial disparities or, at least, make them no worse. *See Drug Arrests Stayed High Even as Imprisonment Fell From 2009 to 2019*, PEW CHARITABLE TRS. (Feb. 15, 2022) https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2022/02/drug-arrests-stayed-high-even-as-imprisonment-fell-from-2009-to-2019 [https://perma.cc/Z65C-26JF]. It is possible that institutional and cultural influences downstream have started to change the risks of disparate racial impact over time. *See generally* Joshua B. Fischman & Max M. Schanzenbach, *Racial Disparities Under the Federal Sentencing Guidelines: The Role of Judicial Discretion and Mandatory Minimums*, 9 J. EMPIRICAL LEGAL STUDS. 729 (2012).

existing "hunch," under similar circumstances.[231] The court believed that the defendant's theory of unequal enforcement of minor traffic infractions was irrelevant and unworkable.[232] At the time it probably was.[233] But it is not anymore and will be even less so in the future. Today, a defendant bringing a case like *Whren* might have the data, thanks to GPS tracking of police and civilian cars, to demonstrate that police pull over only a small fraction of the illegal U-turns and other traffic infractions that they observe, and that the enforcement disproportionately targets minority drivers (if this is so).[234]

If police are able to use filtered surveillance to solve crimes at minimal expense, there will be even less need for discretion. So, if police have a filtered dragnet, courts must make sure they have an acceptable response to the question: "Why did you enforce the criminal law here and not there?"[235]

In summary, a government that has the capacity to detect criminal behavior at very high rates must come under heightened standards of care with respect to the promulgation of criminal laws, the use of incarceration and punishment, and the application of detection tools.

V. THE ANTI-AUTHORITARIAN FOURTH AMENDMENT

Anti-authoritarianism, rather than privacy, should be the benchmark for the Fourth Amendment when police develop cases using filtered dragnets. What makes facial recognition or a geofence or some other form of filtered dragnet "reasonable" is not that the privacy of the innocent is protected—they will all do that. Rather, an "unreasonable" use of these technologies means the state is misusing its power to punish and control.

The current trajectory of Fourth Amendment caselaw suggests that we are headed for one of two suboptimal endpoints: either the state will be able to use filtered dragnets with little to protect its citizens from the perils of broad criminal laws, harsh criminal sentences, and selective enforcement, or the state will effectively be prohibited from using filtered dragnets, leaving a criminal justice status quo that nobody would devise and few would

231. Whren v. United States, 517 U.S. 806, 809 (1996).

232. *Id.* at 815.

233. In individual cases, it would have been difficult to prove that race was a but-for cause of a police officer's decision to conduct a seizure. However, even at the time, some argued that the fact that race clearly played a role systemically should have been sufficient for the Court to decide that pretextual stops violated the Fourth Amendment. *See* Tracey Maclin, *Race and the Fourth Amendment*, 51 VAND. L. REV. 333, 375 (1998).

234. Christopher Slobogin has characterized law enforcement use of pretextual stops as a species of general warrant. SLOBOGIN, VIRTUAL SEARCHES, *supra* note 29 at 102.

235. *See generally* Harcourt & Meares, *supra* note 18 (recommending that the degree of suspicion and the evenhandedness of a search program should be of utmost Fourth Amendment importance).

defend.[236] But if the courts start to take seriously the fundamental differences between filtered dragnets and other investigation techniques—if they recognize that technology can explode longstanding assumptions about the nature of risk when police increase the detection of crime—courts can harness the disruptive technology and help society land in a better equilibrium.

Thus, the Fourth Amendment must evolve to demand "reasonableness" when detection is easy. The thrust of my proposal is that the phrase "reasonable searches and seizures" should be understood as a more expansive and robust guarantee of reasonableness.[237] Specifically, the requirement of "reasonable" seizures should guarantee that the *consequences* of a seizure (e.g., carceral arrest and a possible prison sentence) are fitting and proportionate to the gravity of the suspected crime. The requirement of "reasonable" searches should guarantee not only that the search is conducted based on probable cause and in line with established warrant requirements, but also that the decision to search or not search is reasonable and non-arbitrary. The former ensures that the criminal law being enforced is serious enough to justify the loss of rights that comes along with an arrest or a long sentence. The latter ensures that criminal detection tools are used in an even-handed manner.

A. REASONABLE SEIZING—RESTRICTING THE SUBSTANTIVE CRIMINAL LAW

The prospect of near-perfect detection requires more care in defining a reasonable seizure. In order for a carceral seizure of a person to be reasonable, state uses of force and coercion involved must be justified by the harm that the arrestee has imposed on society. "Freedom from unreasonable . . . seizures" should be interpreted to protect the interests of individuals who have engaged in conduct that is technically illegal but not morally reprehensible.[238] Thomas Jefferson's unfinished vision laid out in

236. BARKOW, *supra* note 100, at 5 ("One could say our approach to crime is a failed government program on an epic scale, except for the fact it is not a program at all. It is the cumulative effect of many isolated decisions to pursue tough policies without analyzing them to consider whether they work or, even worse, are harmful.").

237. To some extent, this builds on the constitutional case law and scholarship that give the "reasonableness" phrase pride of place in Fourth Amendment interpretation. *See* AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 35 (1997); Miriam H. Baer, *Law Enforcement's* Lochner, 105 MINN. L. REV. 1667, 1730 (2021); Renan, *supra* note 135, at 1044, 1081–82.

238. *See generally* Robert M. Cover, *Violence and the Word*, 95 YALE L.J. 1601, 1608 (1986) (reminding readers that all prison sentences are backed by the credible threat of state violence). Again, my argument is similar to Bill Stuntz's work suggesting the physical intrusion and coercion of the policing process to be the main source of trouble. William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1026 (1995).

the *Declaration of the Rights of Man and of the Citizen* provides the blueprint. Article 4 states, "Liberty consists in the power to do anything that does not injure others"; Article 5 states, "The law has the right to forbid only such actions as are injurious to society"; and Article 8 states, "The law ought to establish only penalties that are strictly and obviously necessary."[239]

A seizure should only be reasonable if the underlying criminal conduct and the resulting punishment are also reasonable. While substantive due process rights and the Eighth Amendment provide some absolute constitutional limits against unreasonable criminal codes or punishments, these rights must be bolstered in the face of near-perfect detection. An analysis of reasonable seizures in light of filtered dragnets has two aspects to it: (1) whether the behavior is sufficiently blameworthy to belong in the criminal code at all, and (2) if so, whether the punishment fits the risks and harms of the crime.

Is the conduct crime-worthy? The first inquiry asks whether the suspect's conduct is bad enough to justify arrest and incarceration at all.[240] This is a threshold issue. Criminal conviction needs to be blameworthy and stigmatizing. Defining what sort of conduct is "blameworthy" raises deep philosophical questions, but there is an aspect of the question that is empirical: it needs to be rare. If the conduct captured by the scope of the criminal codes is commonplace, the actor's community evidently has not incorporated restraint deeply into its moral fabric.[241] In those cases, government intervention short of criminal liability (including expressive law, civil fines, or positive reinforcement for its opposite) should be used.[242]

This is at odds with cases like *Atwater*, where the court refused to second-guess a local government's decision to criminalize a minor driving infraction,[243] but Fourth Amendment case law *does* occasionally break rank with *Atwater* and peeks at the substance of the criminal violation in order to

239. DECLARATION OF THE RIGHTS OF MAN AND OF THE CITIZEN (France 1789), https://avalon.law.yale.edu/18th_century/rightsof.asp [https://perma.cc/VZF7-CZ6G].

240. Given the public interest in having the state intermediate misdemeanor and civil infractions as well, non-carceral short-term seizures should not require judicial scrutiny of the substance of the law. *See* Rachel A. Harmon, *Why Arrest?*, 115 MICH. L. REV. 307, 359 (2016).

241. A useful methodology may be the sort of surveys of past behavior that Tom Tyler relied on in his seminal work, *Why People Obey the Law*. One survey of Chicago residents suggested that there might be a natural breakpoint between minor traffic violations and neighborhood infractions, where survey respondents sometimes engaged in the activity (even if rarely), and the conduct for which over 90% of respondents state they have never engaged in (e.g., theft). TYLER, *supra* note 93, at 41.

242. To increase cultural legitimacy, punishment should rely more on reputation and relationship consequences than on punishment. STUNTZ, *supra* note 15, at 30–31. One broad category of criminal laws that may deserve constitutional scrutiny are laws that criminalize the possession or sale of contraband items to adults. These are acts that are transactional. KLEIMAN, *supra* note 20, at 154–55.

243. Atwater v. Largo Vista, 532 U.S. 318, 323–24 (2001).

gauge the reasonableness of a procedure. For example, when analyzing whether a warrantless traffic checkpoint is constitutional as a reasonable warrantless seizure, the Supreme Court explicitly considers "the gravity of the public concerns served by the seizure" as one of the factors.[244] And the Court has refused to allow exigent circumstances to excuse the failure to secure a warrant for a home search and arrest when the underlying crime is a minor offense.[245] And *Atwater* is ahistorical: a quick tour of the notorious cases the Crown directed against colonists that inspired the Bill of Rights are offensive, in large part, because of the substance of the crimes. These included crimes such as writing or publishing "gross and scandalous reflections and invectives upon his majesty's government" or the crimes of illegal trade and inadequate record-keeping.[246]

Is the punishment too harsh? If the suspect's conduct is reprehensible enough to pass the initial threshold test, a post-conviction seizure could still be unreasonable if the quality and length of detention is disproportionately harsh.[247] The sentences of many crimes, even violent crimes, could probably be reduced to weeks or days, or even converted to non-carceral forms of punishment (like public service or surveillance-enabled supervised release) without increasing crime rates if detection rates were much higher than they currently are. Long-term prison sentences can be reserved for murder, treason, severe sexual assault, severe child abuse, and for the incapacitation of repeat criminals.[248] For other crimes, detection through filtered dragnets, rather than a small chance of very harsh punishment, can be the door jamb that stops the metaphorical revolving door of recidivism.

B. REASONABLE SEARCHING—MINIMIZING DISCRETION

A police department's use of filtered dragnets will be fair if it avoids gaps in the protection from crime as well as gaps in leniency from enforcement.

244. Illinois v. Lidster, 540 U.S. 419, 427 (2004) (quoting Brown v. Texas, 443 U.S. 47, 51 (1979)).

245. Welsh v. Wisconsin, 466 U.S. 740, 750 (1984) (citing McDonald v. United States, 335 U.S. 451, 459–60 (Jackson, J., concurring)).

246. Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1197 (quoting Entick v. Carrington, 19 Howell's State Trials 1029, 1034 (CP 1765)), 1199 (publishing criticism), 1243 (illegal trade and recordkeeping), 1247 (same) (2016). Moreover, Donohue describes the limits in eighteenth century England to the meaning of the term "felon" or "felony," which included only the most morally reprehensible crimes such as murder, theft, suicide, rape, and arson. *Id.* at 1222–23.

247. ANDREW VON HIRSCH, DOING JUSTICE: THE CHOICE OF PUNISHMENTS 66–83 (1976).

248. *See generally* Eric Helland & Alexander Tabarrok, *Does Three Strikes Deter?: A Nonparametric Estimation*, 42 J. HUM. RES. 309 (2007) (finding significant deterrent effect, and not just incapacitation effect, from three strikes laws).

1. Duty to Search

All cases of reported or otherwise known crimes that are equally suitable for filtered dragnets should be investigated.[249] For example, if a police department can use filtered dragnets to detect gun violence or robberies, and it fails to investigate daytime violence and robberies taking place near low-income schools even though it investigates every daytime robbery or assault that takes place near high-income schools,[250] the uneven use of filtered dragnets would render it an unreasonable search. As a practical matter, while it would make more sense for a constitutional challenge to come in the form of a § 1983 claim brought by a resident who is harmed by a detectable or deterrable crime, the challenge is more likely to emerge when a criminal defendant brings a claim similar to the claim brought in *Whren* (arguing that although they committed an offense, the crime is unequally enforced).[251] Courts should be open to a claim and evidentiary proof of this sort.

2. Duty to Cast a Large Dragnet

Law enforcement should not have undue control defining the search pool that will be used by a filtered dragnet. The database that will be used to cross-check against the facts of a crime should include everyone possible whose data is accessible and whose participation in the crime would not be an impossibility. This reduces the risk of arbitrariness or bias that could result if police search for potential leads and matches in one population while ignoring another.

By this standard, facial recognition systems like Clearview AI are more legitimate (in the sense of being less susceptible to bias or discretion, at least) when they match surveillance footage at a crime scene against the largest possible set of publicly available portraits on the open web. Contrast this with DNA filtered dragnets: it is increasingly common and popular to restrict local law enforcement who are running DNA searches to CODIS, the federally maintained database of arrestee or convict DNA samples.[252] Whatever rationale might justify subjecting convicts to greater likelihood of

249. At the very least, they should be investigated randomly rather than haphazardly. *See* Harcourt & Meares, *supra* note 18, at 851–54.

250. FORMAN, *supra* note 7, at 125.

251. Whren v. United States, 517 U.S. 806, 810 (1996).

252. Kaye & Smith, *supra* note 146, at 414–15; Ram, *supra* note 34, at 789 (it is not fair to subject relatives of people who are in the CODIS database to more police scrutiny than relatives of those who are not). Local police departments have expanded their DNA databases by choosing to include "exclusion samples" (that is, DNA samples collected from suspects or victims) and juvenile defendants. Lazer & Meyer, *supra* note 33, at 904.

being caught in their own future crimes, the logic does not follow to arrestees or to individuals whose crimes are detected through familial DNA.[253]

The principle of evenhanded enforcement is consonant with what Bennett Capers meant when he argued that equitable policing may require "redistributing privacy."[254] But it may require courts to enforce subpoenas or issue warrants in order to pierce through corporate policies that resist law enforcement access.[255] These policies are already in place at some companies.[256] Of course, there may be times when law enforcement resources really are constrained so that investigating every trackable crime or casting the widest possible dragnet will not be possible, but the police should be able to offer some reasonable explanation. And an explanation that would *not* be reasonable is that too many individuals would be caught: if the availability of filtered dragnets forces law enforcement to confront the problem that there are too many criminal acts, the proper government response is to revisit and narrow or purge some of the substantive criminal laws.

C. POLICE CULTURE: THE ERA OF THE NERDY POLICE FORCE

The adoption of filtered dragnets will require law enforcement agencies to become more technocratic. Much of the initial investigation work is likely to be centralized, in upper management working at desks, and their compliance with Fourth Amendment restrictions will require competence, if not expertise, in statistical methods and data auditing procedures. To some extent, this change in operations is already happening with the gradual introduction of DNA forensic labs, facial recognition, and now, reverse searches. With clear Fourth Amendment guidance for filtered dragnets, police forces could rapidly adopt filtered dragnets and divest somewhat from traditional techniques. Police operations would shift away from self-initiated patrols and field-based investigation toward data-driven initiation and investigation. This will change who is qualified for and attracted to a policing job. Police investigators who are used to solving cases through interrogations and informants will begin to feel like the baseball scouts who still visit high

253. Lazer & Meyer, *supra* note 33, at 909–11. Commentators have noted the race disparities in likelihood of detection that result from using arrestee DNA only. Ram, *supra* note 34, at 789.

254. Bennett Capers, *supra* note 59, at 1243–45 ("In exchange for a reduction in hard surveillance of people of color, it will require an increase in soft surveillance of everyone.").

255. *See generally* Yan Fang, *Internet Technology Companies as Evidence Intermediaries*, 110 VA. L. REV. (forthcoming 2024).

256. ANCESTRY, *Ancestry Privacy Statement* (Aug. 11, 2020), https://www.ancestry.com/c/legal/privacystatement_2020_8_11#:~:text=In%20the%20interest%20of%20transparency,data%20across%20all%20our%20sites.&text=We%20may%20share%20your%20Personal,(e.g.%2C%20subpoenas%2C%20warrants)%3B [https://perma.cc/Y8NN-FSXJ].

school and college teams looking for "good legs" while their younger, nerdier, and (eventually) better paid colleagues use Bill James-style statistics to prioritize the team's recruiting efforts.[257]

This may prove to be a feature—a way to achieve the reform of police culture by working backwards from shared ends that are appealing to both suburban families and Black Lives Matter activists (lowering crime, reducing false convictions, and achieving even-handed enforcement). The cultural shift can provide counterpressure to a problem that currently plagues police recruitment—that the people most interested in working for law enforcement have stronger-than-average preferences for meting out punishment.[258] All the more reason civil liberties organizations should reconsider their instinctive negative reactions to filtered dragnets.

The criminal defense bar may get transformed, too. Andrew Ferguson has made the case that law enforcement data-collection and data-mining practices can be inverted to discover negligent or abusive practices within police departments.[259] Defendants can make use of "blue data" to prove their cases that, for example, law enforcement had used an unreasonably narrow dragnet.[260] This may offend a police department's sense of agency and self-determination, but this is a reasonable price to pay for the power and efficiency of filtered dragnets.[261]

VI. ADDRESSING FRIENDLY OBJECTIONS

Some readers will no doubt disagree with my description of the looming opportunities and problems that will arise with filtered dragnets, and as a result will reject the policy solutions offered in Part V. I addressed doubts about the upsides of filtered surveillance or the downsides of near-perfect detection as best I can in those earlier Parts. Whatever disagreements about the policy implications remain will have to be aired in other fora. Here, I address some objections that will be raised even by readers who agree that the policies advanced in this Article are sound.

257. *See generally* MICHAEL LEWIS, MONEYBALL (2003).

258. Dharmapala et al., *supra* note 67, at 107.

259. Andrew Guthrie Ferguson, *The Exclusionary Rule in the Age of Blue Data*, 72 VAND. L. REV. 561, 600–08 (2019).

260. *Id.* To be fully effective, blue data investigations may require increased transparency and access to police programs. *See generally* Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CALIF. L. REV. 917 (2021).

261. Some will no doubt be concerned that filtered dragnets are a progression of the sort of bureaucratization of policing that has already caused dysfunction—the Compstat meetings, bulk, assembly-line adjudication, et cetera. STUNTZ, *supra* note 15, at 57. But it is not clear that there are viable alternatives to a bureaucratic police force.

"Friendly" critics will wonder why it is necessary to constitutionalize these policies rather than advocating for a legislative response. The answer, in brief, is that constitutional protections are the only viable tools when several criminal justice rules must be changed at the same time.

Friendly critics may also wonder why the Fourth Amendment is the right vehicle for course correction even if all agree that constitutional law must be pressed into service. On this question, I am more neutral. If the Eighth Amendment and Due Process clauses can be interpreted to reach the same anti-authoritarian objectives, there is little reason to insist on the Fourth Amendment as the primary source of these rights. But since filtered dragnets will inevitably cause seismic activity in Fourth Amendment law, and since highly efficient searches are the reason that the threat of government tyranny will become more pronounced, it is at least fair to say that the Fourth Amendment *could be* the right constitutional source for the anti-authoritarian rights described in Part V.

A. WHY THE COURTS? (OR, WHY NOT THE LEGISLATURE?)

Not every problem in law enforcement needs to be solved through the constitution, but this one does. The political process is exceedingly unlikely to get us out of our criminal justice rut, where low detection rates are messily compensated through criminal liability for minor infractions. Political winds bob from too much lenity to authoritarian severity,[262] and as a result, surveillance restrictions and decriminalization usually rise and fall together depending on whether the mood is pro-rights or anti-crime. Political institutions do not have the tools to break surveillance and substantive criminal law apart and to work out a criminal justice horse trade. But a horse trade is what we need: we simultaneously need the police to detect more violent crime while also ensuring that no person who is caught with a $10 baggie of drugs could ever be in a position to go to prison for the rest of their life.[263]

This trade—reduced criminal liability in exchange for greater detection—can only be accomplished through constitutional adjustment. If criminal liability and punishment are reduced without a simultaneous increase in detection, crime rates will rise and the ballot box consequences for political actors will be harsh. If detection capacity is increased without any change to the criminal codes, the political actors' constituents will be

262. STUNTZ, *supra* note 15, at 34–35.

263. FORMAN, *supra* note 7, at 121 (describing a former client in this position). Even the more probable outcome—a five-year sentence, say, *id.* at 122, is vastly over-punitive compared to the risk of harm posed to the community. *See generally* Jane Bambauer & Andrea Roth, *From Damage Caps to Decarceration: Extending Tort Law Safeguards to Criminal Sentencing*, 101 B.U. L. REV. 1667 (2021).

justifiably nervous about how the newfound power of detection will be used. But if the two reforms happen at the same time—if the state is constrained by constitutional interpretation from detaining or imprisoning individuals based on minor infractions, or from levying long sentences for anything other than the most serious and violent offenses—surveillance is defanged because the threat of *unjust* prosecution is reduced.[264]

Put another way, the political pressure to limit or ban surveillance tools might make sense as a second-best solution if decriminalization and reduced sentencing is politically infeasible, but the risk is that the strategy can lock out the first best solution—the low penalty/high detection solution. Indeed, in the wake of rising murder rates, the decriminalization and police reform movements are already more politically controversial than they were just a couple years ago. If crime rates continue to rise while detection is capped or suppressed through new legal constraints on technology, politically accountable decisionmakers will continue to use mass incarceration to manage crime.

To be fair, many luminaries in the field of criminal justice have seen roughly the same patterns of dysfunction and technological disruption that I have recounted and have recommended solutions in the form of legislation, administrative regulation, and restoring the role of local government. Bill Stuntz, for example, argued that many of the abuses of power in the criminal justice system would be avoided if local governments (rather than states) were the primary promulgators of criminal law and if juries (rather than prosecutors) were the decisionmakers who most often determined whether a defendant should be convicted or serve time.[265] Chris Slobogin, Barry Friedman, Maria Ponomarenko, Catherine Crump, and Andrew Ferguson have argued that legislatures and regulatory agencies should be more active in structuring how (non-filtered) dragnet and surveillance technologies should and should not be used in the field.[266] But they also acknowledge that politically accountable bodies always run the risk that their decisions will disproportionately benefit the politically powerful and will be relatively indifferent to problems of under-protection and prejudiced enforcement.[267]

264. *See generally* Bambauer & Roth, *supra* note 263 (using a new empirical approach to measure just sentences and finding that criminal sentences are disproportionate to the social harm the crimes caused).

265. STUNTZ, *supra* note 15, at 8, 39. *See generally* Wayne A. Logan, *Fourth Amendment Localism*, 93 IND. L.J. 369 (2018).

266. Ferguson, *supra* note 9, at 272. *See generally* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014); Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827 (2015); Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016).

267. Slobogin, *supra* note 132, at 134.

Daphna Renan has argued, convincingly in my opinion, that political processes alone cannot be expected to produce the sort of basic rights and counter-majoritarian protections that the Constitution should guarantee.[268] Our agreement ends there, though, because Renan advocates for a Fourth Amendment superstructure, or set of principles, that would set requirements and boundaries on administrative agencies (such as the Privacy and Civil Liberties Oversight Board) tasked with creating law enforcement surveillance programs.[269] But no board, no matter how independent, could actually make the grand maneuver that I'm asking readers to consider here—where filtered dragnets are permitted, but in exchange for protection from bad laws, harsh punishment, and discretionary application. Renan's proposal may be a good second-best solution, but a dramatic reorientation of constitutional priorities can only be done by the Supreme Court. It is time for constitutional renewal in search of a better equilibrium.[270]

B. WHY THE FOURTH AMENDMENT?

The harder question, and I confess this is where I am on shakier ground, is why the anti-authoritarian principles that I claim are so important during this inflection point are the responsibility of the Fourth Amendment to solve rather than other parts of the Bill of Rights or notions of substantive due process.[271] The case is somewhat easier for the principle that reasonable searching requires evenhandedness. At the founding, the Fourth and Fifth Amendments were meant to prevent the government from being able to rummage through a disfavored target's things looking for evidence of a crime, so equal and non-arbitrary treatment was always a goal.[272]

The case for using the Fourth Amendment to put constraints on substantive criminal law and sentencing is a bit harder. After all, the Supreme Court has repeatedly authorized law enforcement agencies to execute stops, searches, and arrests, no matter how trivial the law-violating behavior may be to overall public safety.[273] As early as *Boyd v. United States*, decided in 1886, the Court found that Fourth Amendment protections do not apply to those who have committed a public offense, and courts have declined to

268. *See generally* Renan, *supra* note 135.

269. *Id.* at 1108–25. Again, Renan is primarily (though not exclusively) analyzing surveillance technologies that are not crime-driven filtered types of tools that I focus on here.

270. JACK M. BALKIN, THE CYCLES OF CONSTITUTIONAL TIME 44–65 (2020) (describing cycles of constitutional "rot," where the accretion of rules and exceptions have permitted authoritarian practices to fester, and "renewal," where constitutional theory and courts correct course).

271. Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH. L. REV. 143, 155 (2015).

272. STUNTZ, *supra* note 15, at 72.

273. See discussion of *Atwater* and *Whren*, *supra* Part V.

second-guess whether the public offense was valid in the course of a Fourth Amendment analysis.[274] And one may reasonably think that if courts are going to invalidate an overly harsh prison sentence on constitutional grounds, as I argue they should under the guise of protecting against unreasonable seizures, they would have already imposed these limits under the Eighth Amendment's cruel and unusual punishment clause.[275]

Perhaps it would make as much sense to make Eighth Amendment or Due Process protections more robust to ensure that criminal liability is not overbroad and sentences aren't overlong.[276] But a long view of the Fourth Amendment can support a shift from the protection of the property, privacy, and autonomy of *non-offenders* to the protection of those same interests of those who are *innocent* in the more platonic sense.

In many ways, the history of Fourth Amendment caselaw shows a faltering and incoherent attempt to get to the main point: to make sure the state does not have too much power to enforce silly crimes and scare its constituents into submission.[277] Silly crimes have been at the center of the original construction of the Fourth Amendment and each of its major reforms. Shortly after the American Revolution, sedition laws motivated creative lawyers like Alexander Hamilton to use procedure in order to correct flaws in the substantive criminal law that were not, at that time, adequately constrained by the First Amendment.[278] In the context of that time, when states had nearly full rein to search for physical evidence and when prosecutions were proved primarily using witnesses, the thought that constitutional protections could get in the way of convicting rapists and murderers would have been preposterous.[279] After all, the founders did not expect the Fourth Amendment to constrain how local law enforcement investigated crimes, and group searches executed without particularized

274. Boyd v. United States, 116 U.S. 616, 630 (1886). The Fourth Amendment protects rights that have "never been forfeited by his conviction of some public offence." *Id.*

275. Harmelin v. Michigan, 501 U.S. 957, 997 (1991) (while the Eighth Amendment prohibits "grossly disproportionate" mandatory sentences, noncapital sentences would almost never be found to be grossly disproportionate).

276. Note, though, that the Court has already stated a reluctance to expand substantive due process if other parts of the Bill of Rights are relevant to the claim. Sacramento v. Lewis, 523 U.S. 833, 842 (1998).

277. Cloud, *supra* note 14, at 202. Cloud also notes that early Fourth Amendment case law was designed to constrain discretion (or "autonomy") of law enforcement and the judiciary. *Id.* at 276–284.

278. STUNTZ, *supra* note 15, at 71–72. It is particularly strange that the attack required procedural rather than substantive challenges because prosecutions for the crime of seditious libel conducted by the British Crown was a major motivating force behind the Bill of Rights. Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 309, 346 (2010).

279. TRACEY MACLIN, THE SUPREME COURT AND THE FOURTH AMENDMENT'S EXCLUSIONARY RULE 83–100 (2013); STUNTZ, *supra* note 15, at 71–72.

warrants were tolerated.[280] Thus, at that time, the buildup of procedure to help protect against crimes of belief and thought had little cost to the control of more conventional crimes.

Courts again increased Fourth Amendment procedural protections during two subsequent periods when the substance of criminal law was directed at questionable, arguably victimless vice crimes like gambling, alcohol (during prohibition), obscenity, and recreational drugs.[281] In the twentieth century, new information technologies changed the nature of police investigation by enabling wiretapping and forms of long-term tracking of suspects without reliance on trespass or witness cooperation. The standard story is that these technologies unsettled the balance between conflicting societal goals related to police investigations, which is true enough. But another important factor is that the test cases involved the detection and enforcement of gambling, bootlegging, and drug distribution crimes. *Katz v. United States*, the Fourth Amendment case that developed the reasonable expectations of privacy test, involved bugging a phone a bookmaker was using.[282] And it followed the logic of Justice Brandeis's dissent in an earlier case, *Olmstead v. United States*,[283] which involved the wiretapping of a bootlegger.[284] *Katz* marked the end of a primarily property-based conception of Fourth Amendment rights and ushered in the privacy phase. When test facts making their way to the Supreme Court involved more serious crimes, like stalking, the Supreme Court avoided finding a privacy violation.[285]

To be clear, there are other reasons, separate from the substance of the criminal law being enforced, that justify a focus on privacy. Twentieth century surveillance capabilities certainly left Americans—criminals and the innocent alike—at greater risk of unwanted observation of licit activities. But there is also a clear pattern: courts have used criminal procedure to frustrate the enforcement of controversial criminal statutes that cover activities in which a sizable proportion of Americans willingly participate.[286] Once

280. SLOBOGIN, VIRTUAL SEARCHES, *supra* note 29 at 103. Prior to the 1960s, state courts interpreted their constitutional guarantees of freedom from unreasonable searches and seizures to be very permissive. The investigation strategies that police departments adopted were generally considered reasonable. STUNTZ, *supra* note 15 at 68–69.

281. STUNTZ, *supra* note 15, at 110.

282. Katz v. United States, 389 U.S. 347, 348 (1967).

283. Olmstead v. United States, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

284. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

285. Smith v. Maryland, 442 U.S. 735, 745–46 (1979). Bill Stuntz critiqued the privacy turn, noting that Fourth Amendment litigation became much too focused on privacy and failed to ameliorate problems of physical security (especially bodily security) when suspects were routinely frisked and thrown to the ground. STUNTZ, *supra* note 15, at 37. *See also* Michael Klarman, *Rethinking the Civil Rights and Civil Liberties Revolutions*, 82 VA. L. REV. 1 (1996).

286. The converse is also true: when crime rates spike among the crimes that are most important to a well-functioning society, such as crimes of violence, Fourth Amendment procedural protections are

privacy posed a significant obstacle to police investigations, procedural rights became the default defense against a tyrannical state. There was less pressing need to press the Constitution into service to challenge whether conduct should even be considered criminal in the first place or whether the police are protecting communities fairly. For better or worse, the Fourth Amendment privacy rule created a tractor beam for public defenders and civil liberties organizations to concentrate their anti-authoritarian efforts.

Scholars have occasionally attempted to refocus the Fourth Amendment on a more general purpose to create a constraint on power.[287] Bill Stuntz faulted Fourth Amendment's turn to privacy because it "tend[ed] to obscure more serious harms that attend police misconduct."[288] More recently, Thomas Crocker has argued that the Fourth Amendment should be understood as a substantive right, not just a procedural one, that follows in the vision of the First, Second, and Ninth Amendments.[289] But ultimately, Crocker advocates for the use of this substantive right to argue for a more thorough protection against surveillance.[290] Naturally, I think this misses the point. A citizen whose government makes nearly all conduct and action illegal will never feel secure no matter how many restrictions on surveillance are in place. And conversely, a government that is rigidly constrained from expanding its criminal laws beyond the conduct that is nearly universally reviled will be limited in its ability to threaten a citizen's sense of liberty no matter *how much* surveillance is in place.

The happenstance of technology provides another reason to prefer the Fourth Amendment over other constitutional sources to redress the problems of overcriminalization and uneven protection. The privacy of the innocent was mediating the clash between American values in freedom and security. Increasing use of filtered dragnets will make this arrangement untenable. If we expect the role of the Fourth Amendment to be meaningful—to be something other than a brief paperwork requirement in the process of securing warrants for filtered dragnets—it is both necessary and appropriate that Fourth Amendment caselaw starts to look for its root function and embrace its *substantive* as well as procedural dimensions.

tuned down. Yale Kamisar, *The Warren Court and Criminal Justice: A Quarter-Century Retrospective*, 31 TULSA L.J. 1, 2–3 (1995).

287. Or to create a "constraint on the power of the sovereign, not merely on some of its agents" Arizona v. Evans, 514 U.S. 1, 18 (1995) (Stevens, J., dissenting). With gratitude to Tom Crocker for highlighting this passage. Crocker, *supra* note 278, at 335 n.188.

288. William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1020 (1995).

289. As well as the Fifth Amendment's takings clause. Crocker, *supra* note 278, at 309–10, 343.

290. *Id.* at 311.

CONCLUSION

In 1967, Alan Westin, a leading light among privacy scholars, said that "the modern totalitarian state relies on secrecy for the regime, but high surveillance and disclosure for all other groups."[291] This is probably a true statement, but highly incomplete. Surveillance is a necessary condition for authoritarian control, but not sufficient on its own. Indeed, *all* modern states need surveillance. Modern systems of taxation, public benefits distribution, medical services, and public health could not function without copious amounts of personal data. Thus, surveillance is necessary for all states, not just despotic ones. Moreover, surveillance is no more unique to totalitarianism than are weapons, prisons, and other tools the state must use to carry out the most basic obligations to support social order and security.

The tools that live *exclusively* in the toolbox of despots are repressive substantive criminal laws, harsh punishment, and discretion to choose when to enforce the law. Even in George Orwell's dark depiction *Nineteen Eighty-Four*, Big Brother was oppressive partly because of the substance of the law: the wrong thought could land a person in jail.[292]

Against this threat of uncontrolled surveillance, many privacy scholars recommend the dismantling of the surveillance apparatus. This Article focused instead on the "uncontrolled" quality of uncontrolled surveillance. Filtered dragnets are a highly controlled dragnet that reveal only criminal violations. Thus, they are only as threatening to society as the criminal statutes that they enforce and the discretion of the government agents who use them. With the right alignment of Fourth Amendment rules to authoritarian threats, the state can be made to heel—to detect crimes fairly without burdening any communities with under-protection or over-punishment. This will require some intrusion of the traditionally *procedural* domain of the Fourth Amendment into the *substantive* realm of criminal law and punishment. If the state can suddenly detect every violation, prison must be reserved for truly awful behavior, and law enforcement should have less latitude to seek out or avoid the investigations of members of certain groups.

These are radical proposals. They go well beyond the privacy framework that has dominated Fourth Amendment theory for over half a century. But they respond to a radical tool that will shock a criminal justice system that is already in crisis and deserves rescue.

291. ALAN WESTIN, PRIVACY AND FREEDOM 23 (1967).

292. *See generally*, GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).