1-1-2020

Secrecy & Evasion in Police Surveillance Technology

Jonathan Manes
University at Buffalo School of Law

SECRECY & EVASION IN POLICE SURVEILLANCE TECHNOLOGY

Jonathan Manes†

ABSTRACT

New technologies are transforming the capabilities of law enforcement. Police agencies now have devices to track our cellphones and software to hack our networks. They have tools to sift the vast quantities of digital silt we leave behind on the Internet. They can deploy "big data" algorithms meant to predict where crimes will occur and who will commit them. They have even transformed the humble closed-circuit video camera—and its more recent companion, the body camera—into biometric tracking devices equipped with artificial intelligence meant to pick faces out of a crowd and, eventually, to mine gigabytes of stored footage to automatically reconstruct the movements of their targets.

These kinds of novel police technologies test the constitutional limits on surveillance and raise profound questions about privacy, personal freedom, and potential abuse. Yet the government shrouds them in secrecy. Even as new surveillance tools transform the relationship between people and the police, the public is often left in the dark about how police use these tools and the rules, if any, that govern them. What justifies this secrecy?

This Article examines the primary argument offered by law enforcement in the United States: that disclosure of police technologies would allow criminals to evade the law. Without secrecy, the argument goes, criminals could circumvent law enforcement's tools, crime would go undetected, and society would suffer the consequences. I call this the anti-circumvention argument for secrecy. This Article is the first to examine it.

The Article contends that the anti-circumvention argument, as currently implemented in law, is producing far more secrecy than it can justify, and that it is doing so at the expense of democratic checks, public accountability, and perhaps law enforcement itself. The Article proposes specific reforms to circumscribe laws that currently authorize excessive secrecy in the name of preventing evasion. The Article also proposes structural changes to require police to publish information about novel technologies for public notice and comment, in order to allow meaningful democratic deliberation as we enter the age of digital policing.

DOI: https://doi.org/10.15779/,Z38NP1WJ7K

† J.D. Yale Law School; M.Sc. London School of Economics; B.A. Columbia University. Associate Professor of Law, University at Buffalo School of Law, State University of New York; Affiliated Fellow, Yale Law School Information Society Project. The author is grateful for detailed feedback on prior drafts from Hannah Bloch-Wehba, Kiel Brennan-Marquez, Hon. Stephen Wm. Smith, Matthew Steilen, and Rebecca Wexler, as well as generous comments from Guyora Binder, Luis Chiesa, Jeremy Epstein, Andrew Ferguson, Jim Gardner, Clare Garvie, Jim Graves, Heidi Kitrosser, Keir Lamont, Laura Moy, Jim Milles, Eduardo Schnadower Mustri, Athena Mutua, Peter Ormerod, Brian Owsley, Christopher Slobogin, David Schulz, Rick Su, Kathy Strandburg, and participants in the Yale Freedom of Expression Scholars Conference, the Privacy Law Scholars Conference, and the University at Buffalo School of Law Faculty Workshop.

TABLE OF CONTENTS

I. INTRODUCTION 504

II. THE LIFE CYCLE OF SECRECY IN LAW ENFORCEMENT TECHNOLOGIES 511

A. THE SAGA OF STINGRAY SECRECY 513
B. THE MYSTERY OF MOBILE X-RAY VANS 520

III. THE PROBLEM WITH SECRET LAW ENFORCEMENT TECHNOLOGIES 524

A. SECRECY IMPEDES THE ABILITY OF COURTS TO ADJUDICATE THE LEGAL LIMITS WITHIN WHICH NEW TECHNOLOGIES MAY BE USED 524
B. ANTI-CIRCUMVENTION ARGUMENTS MILITATE AGAINST LEGISLATIVE ENACTMENTS THAT LIMIT HOW NEW TECHNOLOGIES MAY BE USED 527
C. NEW TECHNOLOGIES AND OLD LAWS PRODUCE UNACCOUNTABLE SELF-REGULATION BY POLICE 529
D. SECRET TECHNOLOGIES RECONFIGURE THE RELATIONSHIP BETWEEN CITIZEN AND STATE 533
E. SECRECY IMPOSES COSTS ON LAW ENFORCEMENT TOO 537

IV. THE LOGIC OF ANTI-CIRCUMVENTION SECRECY 538

V. ANTI-CIRCUMVENTION DOCTRINES 546

A. THE FOIA EXEMPTION FOR LAW ENFORCEMENT "TECHNIQUES AND PROCEDURES" 546
B. THE EVIDENTIARY PRIVILEGE FOR LAW ENFORCEMENT INVESTIGATIVE TECHNIQUES 552

VI. REFORMING THE LAW OF SECRET LAW ENFORCEMENT TEHNOLOGIES 557

A. NARROWING THE SCOPE OF ANTI-CIRCUMVENTION SECRECY 558
B. PUBLIC NOTICE AND COMMENT FOR NOVEL INVESTIGATIVE TECHNOLOGIES 562

VII. CONCLUSION 566

I. INTRODUCTION

Over the last generation, we have seen remarkable innovations in technology that are transforming the investigative powers of the police. The cell phone has radically expanded our communication networks, the Internet has transformed our information infrastructure, social life is increasingly lived

online, and networked computers now operate inside even the most mundane household appliances. These pervasive technologies produce a huge amount of digital information about each of us.

Alongside each of these innovations are parallel developments in law enforcement's ability to conduct investigations and surveillance. The public's mass adoption of digital communication technologies has created enormous new investigative targets. At the same time, police and private vendors have harnessed technological innovations to create new and previously unimaginable investigative tools.

A few examples illustrate the scope and ambition of these technologies. Law enforcement now has ready access to: cell site simulators (aka "Stingrays") that can pinpoint the location of cell phones, log calls, and sometimes even intercept the content of conversations;[1] computer hacking and surveillance software that can surreptitiously hijack and search computers, cell phones, and myriad other Internet-connected devices;[2] automated license plate readers that track vehicle locations over months or years;[3] mobile x-ray vans that scan inside cars and underneath clothing;[4] facial recognition algorithms that promise to automatically identify individuals in photos or videos, allowing police to track people in real time or to mine gigabytes of stored footage captured by closed-circuit television cameras, police body-worn cameras, or other video sources;[5] social media data mining tools that generate associational

1. *See* Stephanie K. Pell & Cristopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy*, 28 HARV. J. LAW & TECH. 1, 8–13 (2014).

2. *See generally* Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards (2017).

3. *See, e.g.*, *Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND. (last visited Mar. 9, 2019), https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/D5L3-T8C6]; Russell Brandom, *Exclusive: ICE is about to start tracking license plates across the US*, VERGE (Jan. 26, 2018), https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions [https://perma.cc/9QJC-QDFC]; *You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements*, ACLU (2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/MBA2-478E].

4. *See, e.g.*, Grabell v. N.Y.C. Police Dep't, 139 A.D.3d 477, 477–79 (N.Y. App. Div. 2016); Michael Grabell, *Drive-by Scanning: Officials Expand Use and Dose of Radiation for Security Screening*, PROPUBLICA (Jan. 27, 2012), https://www.propublica.org/article/drive-by-scanning-officials-expand-use-and-dose-of-radiation-for-security-s [https://perma.cc/JYF3-Y6LF].

5. *See generally* Clare Garvie et al., *The Perpetual Lineup: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/TDP9-S7R8].

graphs, "threat ratings," and myriad other profiles;[6] and "big data" artificial intelligence and machine learning tools that purport to predict crime patterns, recidivism risks, or individual security threats based on analyses of massive data sets.[7] Each of these technologies gives the police new and powerful capabilities to monitor people. Many of these tools raise troubling concerns about personal privacy.[8] Some tools threaten to reinforce or exacerbate existing racial disparities in policing.[9] Most of them operate in secret, without the knowledge or consent of targeted individuals and, often, without the ability to challenge how law enforcement uses them. Indeed, the fruits of tech-enabled surveillance, stored in massive databases, can amount to virtual time machines, allowing the police to reconstruct a person's comings and goings and communications going back months or years.[10] Clearly, these technologies raise profound questions about how law enforcement uses them and how they should be regulated.

---

6. *See, e.g.*, MOHAMMAD A. TAYEBI & UWE GLÄSSER, SOCIAL NETWORK ANALYSIS IN PREDICTIVE POLICING 7–14 (2016); Brent Skorup, *Cops scan social media to help assess your 'threat rating'*, REUTERS: GREAT DEBATE (Dec. 12, 2014), http://blogs.reuters.com/great-debate/2014/12/12/police-data-mining-looks-through-social-media-assigns-you-a-threat-level/ [https://perma.cc/UY3E-ZREK].

7. *See generally* Andrew G. Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012); Elizabeth Joh, *Artificial Intelligence & Policing: First Questions*, 41 SEATTLE U. L. REV. 1139 (2018); Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L & POL'Y 105 (2014); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016); *see also* Ava Kofman, *Taser Will Use Police Body Camera Videos "To Anticipate Criminal Activity"*, INTERCEPT (Apr. 30, 2017), https://theintercept.com/2017/04/30/taser-will-use-police-body-camera-videos-to-anticipate-criminal-activity/ [https://perma.cc/B987-W53U]; Doug Wyllie, *What TASER's acquisition of 2 AI companies means for the future of policing*, POLICE ONE (Feb. 9, 2017), https://www.policeone.com/police-products/less-lethal/TASER/articles/289203006-What-TASERs-acquisition-of-2-AI-companies-means-for-the-future-of-policing/ [https://perma.cc/UTG2-EE75]; Axon Int'l, Law Enforcement Technology Report 21–31 (2017), https://www.documentcloud.org/documents/3679537-Taser-2017-Law-Enforcement-Technology-Report.html [https://perma.cc/3U4V-V5VN].

8. *See, e.g.*, ACLU, COMMUNITY CONTROL OVER POLICE SURVEILLANCE: TECHNOLOGY 101 (2016), https://www.aclu.org/sites/default/files/field_document/tc2-technology101-primer-v02.pdf [https://perma.cc/A6HZ-7DFM].

9. *See, e.g.*, Garvie et al., *supra* note 5; Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/ [https://perma.cc/9BDJ-933Q].

10. *See generally* Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773 (2015). The Supreme Court has recognized the Fourth Amendment concerns raised by technology that allows "the Government [to] travel back in time to retrace a person's whereabouts." Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (holding that collection of seven days of cell-site location information from a wireless carrier is a search under the Fourth Amendment and requires a warrant).

Alarmingly, however, in the United States these new capabilities have proliferated largely in secret. At best, disclosure is significantly delayed with respect to new police technologies, their uptake by particular agencies, the policies governing their use, and the manner in which they are being deployed. These innovations thus threaten to radically reorient the informational balance of power between citizens and the state, giving law enforcement ready access to enormously detailed and intimate data about people's lives, while leaving the public in the dark about the police's capabilities. This secrecy is no accident. In many instances, government agencies have actively and vigorously resisted disclosure of any official information about their new technological capabilities and the rules governing their use.[11]

What explains this degree of secrecy? The principal justification offered by the law enforcement community has been powerful and simple: we must keep our methods secret in order to prevent criminals from circumventing our investigative techniques. Without secrecy, the argument goes, criminals would be able to evade law enforcement's tools, crime would go undetected, and society would suffer the consequences.

I call this the anti-circumvention argument for secrecy. This Article is the first to examine the argument in depth and to analyze the legal doctrines that instantiate it.[12]

---

11. *See infra* Sections II.A–B.

12. The other argument often advanced to keep information about law enforcement technology secret is that disclosure would impair business confidences or trade secrets. At first blush, this rationale seems entirely out of place in the context of public police forces. But the argument arises because, increasingly, law enforcement agencies purchase their advanced investigative tools from private companies. Such companies argue (or the police argue on their behalf) that disclosure of information about the tools would cause competitive harm or impair trade secrets.

Three excellent recent papers focus on the trade secrecy rationale for secrecy of police technologies. *See generally* Natalie Ram, *Innovating Criminal Justice*, 112 NW. L. REV. 659 (2018); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018); Eli Siems & Katherine J. Strandburg, *Trade Secrets and Markets for Evidential Forensic Technology*, (May 14, 2018) (unpublished manuscript) (on file with author). The purchase of private technology by police also raises policy concerns beyond secrecy, including questions about who controls, regulates, and sets policy for use of these technologies. Professors Catherine Crump and Elizabeth Joh, among others, have written incisively about these issues. *See generally* Catherine Crump, *Surveillance Policymaking by Procurement*, 91 WASH. L. REV. 1595 (2016); Elizabeth Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 102 (2017).

While this Article develops a number of anti-secrecy arguments that might be deployed against the business confidentiality/trade secret arguments, I do not engage directly with that issue here. This Article is focused instead on the anti-circumvention rationale for secrecy, which constitutes a separate, little-examined obstacle to transparency and accountability—one that that would persist even if concerns about outsourced technology were overcome.

The anti-circumvention argument begins from the premise that if law enforcement discloses certain information about its technological capabilities or how it uses them, then lawbreakers—particularly terrorists, drug trafficking organizations, and other sophisticated criminals—will learn how to avoid detection, interdiction, and prosecution. Such criminals will be able to exploit the gaps in both the capabilities of law enforcement's technologies and the manner in which they are deployed. They will, as a result, be able to wreak havoc unimpeded and evade apprehension at will.

The Federal Bureau of Investigation (FBI) has made this argument in particularly stark and ominous terms, raising the specter of large numbers of kidnappings and murders going unpunished. A sworn affidavit from the head of its Tracking Technology Unit made the case for secrecy with respect to information about cell-site simulator devices.[13] The FBI official warned, "discussion of the capabilities and use of the equipment . . . could easily lead to the development and employment of countermeasures" and "completely disarm law enforcement's ability to obtain technology-based surveillance data in criminal investigations," thereby "completely prevent[ing] the successful prosecution of a wide variety of criminal cases involving terrorism, kidnappings, murder, and other conspiracies where cellular location is frequently used."[14]

Versions of this anti-circumvention argument have also been made outside the criminal law enforcement context. For example, the Internal Revenue Service (IRS) will not disclose the "checklist used by agents to detect fraudulent tax schemes"[15] or the precise specifications that it uses to automatically flag returns for an audit.[16] Disclosing those flags would give tax fraudsters a roadmap to avoid detection. Similar arguments have been featured prominently in debates regarding the National Security Agency's (NSA) surveillance activities. For instance, the NSA vigorously resisted disclosing the rules governing its treatment of information about "U.S. persons" on the grounds that doing so would imperil "sources and methods" of intelligence.[17]

13. *See* Affidavit of Bradley S. Morrison, Chief, Tracking Technology Unit, FBI (Apr. 11, 2014), https://www.documentcloud.org/documents/1208337-state-foia-affidavit-signed-04112014.html [https://perma.cc/8BCN-KB3R] [hereinafter Morrison Affidavit].

14. *Id.* at 2.

15. Mayer Brown LLP v. Internal Revenue Serv., 562 F.3d 1190, 1192 (D.C. Cir. 2009).

16. *See IRS Audits*, INTERNAL REVENUE SERV. (Nov. 30, 2017), https://www.irs.gov/businesses/small-businesses-self-employed/irs-audits [https://perma.cc/P878-FDNM] (describing in general terms the "random selection and computer screening" process for selecting return to audit based on a "statistical formula").

17. *See, e.g.*, Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1195 (9th Cir. 2007); ACLU v. FBI, 59 F. Supp. 3d 584, 594 (S.D.N.Y. 2014).

But even though this type of argument has become part of the government's ordinary vernacular in discussions of law enforcement—and it has now been litigated in court numerous times—the argument has not been subject to sustained scrutiny in the scholarly literature.

This Article seeks to fill that gap.[18] It is the first to take a close look at the anti-circumvention argument for secret police technologies. In broad outline, the Article defends three claims.

First, I contend that even if the anti-circumvention argument is sound on its own terms, there are powerful countervailing arguments that militate strongly in favor of transparency with respect to law enforcement innovation.[19]

In particular, secrecy undermines institutional checks on the police by other branches of government. Secrecy impedes the ability of the courts to consider and adjudicate compliance with constitutional and statutory limitations because litigants will frequently be unable to mount court challenges to concealed techniques. Secret techniques are also largely immune from legislative oversight and regulation. Even if legislators themselves learn about the police's technologies and the policies that govern them—which is not always a given—oversight is severely weakened in the absence of public disclosure. Indeed, secrecy undermines the accountability of police technologies to the public at large, limiting the ability of citizens to use the levers of democracy to control their law enforcement agencies.[20]

It is cliché to say that information is power, but when police limit the flow of information about their technical capabilities, it does indeed lead to a troubling concentration of authority. Secrecy produces, in effect, a self-regulatory regime in which law enforcement agencies write their own rules, behind closed doors, about how they can deploy technologies. Even if the secrecy surrounding a technology eventually erodes, as it tends to do over time, the rules and practices that law enforcement has developed over time will enjoy all the advantages of incumbency.

Perhaps even more alarmingly, the anti-circumvention rationale for secrecy militates against the adoption of public rules at all. After all, to make public rules governing a technology's use is to disclose limits on how the technology may be used. According to the anti-circumvention argument, the disclosure of such limits is precisely the kind of information that should not be disclosed, lest criminals develop countermeasures. Seen in this light, public rules, statutes,

18. *See supra* note 12 (describing existing literature on secrecy of law enforcement technologies).

19. *See infra* Part III.

20. *See generally* Barry Friedman, UNWARRANTED: POLICING WITHOUT PERMISSION (2017) (offering a vivid and sustained argument for democratic supervision of policing and the crucial role of secrecy in impeding such oversight).

and judicial opinions are the kinds of disclosures that threaten to permit circumvention of novel law enforcement capabilities. The anti-circumvention argument thus tends to favor keeping the governing rules secret, if they even exist at all. This creates a deep tension with basic liberal and democratic commitments against secret law: public rules governing police are a key protection for individuals against the arbitrary exercise of power.[21] Put more strongly, a system in which investigatory powers are governed by secret rules is more characteristic of a police state than a democracy such as ours.[22]

Moreover, keeping technologies secret can, paradoxically, undermine a law enforcement agency's effectiveness. Disclosure permits input and advice from outside experts. It encourages officials to deliberate carefully about how to deploy technologies most effectively. It permits sharing of best practices among separate agencies. It builds trust between the police and the communities they serve. Indeed, public opposition to new police technologies may be attributable as much to the secrecy of such techniques as it is to their intrusiveness. This dynamic is especially the case with modern investigative technologies that can be deployed without any obvious physical footprint and directed against particular individuals without their knowledge. As Chief Justice Burger wrote in another context, "[p]eople in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing."[23]

The upshot of these arguments, and others developed in this Article, is that the anti-circumvention concerns alone hardly settle the question in favor of secrecy. Even if the anti-circumvention argument is sound, accepting it may come at an unacceptable cost.

Second, this Article unpacks the structure of the anti-circumvention argument for secrecy and evaluates its strength.[24] Anti-circumvention arguments rest on empirical claims about the consequences of disclosure that are often simply assumed to be true without meaningful scrutiny. Will disclosure actually impair law enforcement's techniques or procedures? Or will it in fact have little to no effect because of other facts already in the public

21. For example, we do not keep Fourth Amendment law secret because police investigatory methods would be more effective if would-be criminals did not know the constitutional limits that police officers are bound to respect.

22. I elaborate on the idea that secret rules are threats to individual liberty in other work evaluating the phenomenon secret law. *See generally* Jonathan Manes, *Secret Law*, 106 GEO. L.J. 803 (2018). For present purposes, the key point is that adopting the anti-circumvention argument can raise secret law concerns because disclosing (or publicly adopting) laws that limit police techniques may create opportunities for circumvention.

23. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 572 (1980) (holding that the Constitution guarantees the public the right to access criminal court proceedings).

24. *See infra* Part IV.

domain? Will disclosure result in changes in criminal behavior that frustrate enforcement objectives? Or could it instead channel criminal behavior into less socially harmful activities, or deter criminality outright? By taking the argument seriously on its own terms, this Article aims to clarify the internal power and limits of the anti-circumvention argument.

Third, this Article examines the existing legal regimes that empower police to keep their capabilities and techniques secret.[25] I conclude that these doctrines permit far more secrecy than the anti-circumvention argument can justify. In particular, both the Freedom of Information Act's (FOIA) exemption for law enforcement "techniques and procedures" and a common-law evidentiary privilege against disclosure have been interpreted to permit an expansive ambit for secrecy. These sources of law provide law enforcement a shield against disclosure that is much stronger than what is required by the logic of anti-circumvention. And neither source of law takes into consideration the countervailing interests favoring disclosure to the public.

The Article concludes by offering proposals for reform.[26] In particular, I advocate framework legislation that would require public deliberation about new technologies through the legislature *before* police put them into regular use. I also propose doctrinal changes that would rein in expansive warrants for secrecy under the FOIA and the law enforcement privilege.

The Article proceeds in five parts. Part II illustrates the anti-circumvention argument in action by describing two contemporary examples of secret innovation in law enforcement technology: cell-site simulators and mobile x-ray vans. Part III explores the reasons that secrecy regarding techniques and procedures is often unwarranted, even where anti-circumvention concerns may accompany disclosure. Part IV unpacks the anti-circumvention argument on its own terms, probing its analytic and empirical underpinnings. Part V contrasts this analysis of the anti-circumvention rationale with the legal doctrines that have implemented it in overbroad ways. Part VI offers prescriptions for how to tame the anti-circumvention argument and ensure that excessive secrecy does not thwart democratic deliberation over new, intrusive, and potentially transformative police technologies.

II. THE LIFE CYCLE OF SECRECY IN LAW ENFORCEMENT TECHNOLOGIES

In order to understand how the anti-circumvention argument works in practice, it is essential to closely examine particular examples. This Part focuses on Stingrays and mobile x-ray vans. Because of the privacy concerns that both

25. *See infra* Part V.
26. *See infra* Part VI.

of these technologies raise—and the public health concerns raised by the latter—they vividly illustrate what is at stake when police technology is kept secret and insulated from democratic accountability.

Stingrays and x-ray vans also illustrate the secrecy dynamics that typify innovations in police technology. These technologies typically follow an arc: when they first come into use, they are almost completely opaque to the public. Eventually—often after many years or even decades—they generally come to light and are sometimes then subjected to legal regulation by courts and legislatures. The story usually goes something like this: A law enforcement agency adopts a novel technology and shrouds it in a great deal of secrecy. The agency seeks to maintain this secrecy as long as possible. Information about the technology comes into the public domain slowly, in fits and starts, usually by way of investigative work of technical experts, specialist journalists, or criminal defense teams. Efforts by civil society organizations to force official disclosure through the courts are typically met with powerful legal resistance by the government. Until there is a critical mass of public disclosure and public awareness, courts and legislatures generally do not publicly weigh in on the constitutional or statutory limits on the police's use of the novel technology. Consequently, law enforcement will typically have put a novel technology into routine use long before it becomes subject to any consistent, public legal framework governing its operation.

The Stingray and x-ray van examples also illuminate how the government employs the anti-circumvention argument in practice to delay disclosure. The government has several legal tools at its disposal, including the FOIA exemptions[27] and the evidentiary privilege already mentioned.[28] The government also has tools for concealing technologies in the context of criminal prosecutions, including writing warrant applications that obfuscate[29] or affirmatively misrepresent[30] the technology in question; engaging in "parallel

27. 5 U.S.C. § 552(b)(7)(E) (2018). The FOIA exemption is discussed in detail *infra* Section V.A.

28. *See* Stephen Wm. Smith, *Policing Hoover's Ghost: The Privilege for Law Enforcement Techniques*, 54 AM. CRIM. L. REV. 233, 245–46 (2017). The law enforcement privilege is discussed in detail *infra* Section V.B.

29. *See* United States v. Patrick, 842 F.3d 540, 546 (7th Cir. 2016) ("[I]n this case, the government appears to have purposefully concealed the Stingray's use from the issuing magistrate, the district court, defense counsel, and even this court. It ultimately admitted its use of the device only in response to an *amicus curiae* brief filed during this appeal.").

30. *See, e.g.*, *id.* at 548 (local police department used Stingray device after obtaining court order that " '[a]pprove[d] the release of information,' [from telephone service provider] not the use of a device that would allow the [local police] to track [the suspect's] phone on its own"); United States v. Temple, No. 15-CR-230-1 JAR (JMB), 2017 WL 7798109, at *33 (E.D. Mo. Oct. 6, 2017) (assessing an instance where a cell-site simulator was used and the "application and Court Order d[id] not specifically mention the use of a Cell Site Simulator").

construction" to hide a secret method by conducting a parallel, clean investigation that "discovers" evidence already identified with a secret technique;[31] or even dropping criminal charges rather than having to disclose a method and face a challenge to its legality.[32]

Stingrays and x-ray vans vividly illustrate these secrecy dynamics. The story is the same, in broad outline, with respect to computer hacking tools, predictive policing software, automated license plate readers, facial recognition technology, and others. Each finds itself at some point along the uncertain arc from secrecy to public disclosure and democratic regulation. I have chosen these two particular examples because they are both far enough along this path to be able to tell an instructive story.

A. THE SAGA OF STINGRAY SECRECY

Stingrays are portable electronic devices that mimic cell phone towers. They force mobile phones within range to connect to the device, rather than the genuine cell tower.[33] While these devices vary in their capabilities, all such devices are capable of logging the identifying information of cell phones nearby.[34] Police can also use these devices to triangulate the location of devices (and, therefore, their owners) with a great deal of precision. Many models can precisely track a particular cell phone even if the phone is not actively transmitting voice or data.[35] Some models allow users to log details about the calls that each cell phone makes, including the incoming or outgoing phone number and duration of the call. Certain advanced models even permit interception and decryption of the *content* of phone calls and text messages.[36]

For decades, experts have known that Stingrays exist. The devices exploit vulnerabilities in our cell phone networks that have been well known for twenty years, including the fact that phones will connect to any cell tower, even a spoofed tower, without authentication and that communications are

31. *See, e.g.*, Amanda C. Grayson, Note, *Parallel Construction: Constructing the NSA Out of Prosecutorial Records*, 9 HARV. L. & POL'Y REV. S25, S32–33 (2015); Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1042–43 (2014); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants & The Right to Notice*, 54 SANTA CLARA L. REV. 843, 853–64 (2014).

32. *See Patrick*, 842 F.3d at 546 ("Until recently, the government has gone so far as to dismiss cases and withdraw evidence rather than reveal that the technology was used."); *see also infra* notes 43, 51 and accompanying text.

33. This descriptive discussion relies extensively on Stephanie K. Pell & Cristopher Soghoian. *See supra* note 1.

34. The "Stingray" is actually just a trade name of one such device, which are known generically as International Mobile Subscriber Identity (IMSI)-catchers or cell site simulators.

35. Pell & Soghoian, *supra* note 1, at 11–12.

36. *Id.*

protected by weak encryption that is readily cracked.[37] Indeed, over the last decade or so, it has become possible for hobbyists to create rudimentary Stingrays for only a few hundred dollars apiece.[38]

Nevertheless, the government engaged for decades in a concerted, coordinated, and determined effort to resist and oppose any official disclosure of information about police use of Stingray technology. This secrecy campaign has been wide-ranging, extending to state and local law enforcement. I describe the elements of this effort to resist disclosure presently.

The FBI has imposed secrecy obligations on state and local police by exploiting the Federal Communications Commission's (FCC) jurisdiction over the radio frequency spectrum. Manufacturers of Stingrays and similar devices that transmit signals must obtain equipment authorization from the FCC.[39] As a condition of these authorizations, which allowed sales only to police, the FCC directed that "state and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment."[40] The FBI used this condition to require state and local agencies to sign a nondisclosure agreement that forbade them from disclosing any information about the devices to the public.[41] In addition, the federal government designated information about the devices as "Homeland Security Information" pursuant to 6 U.S.C. § 482(e), a statute that purports to preempt state and local laws that

37. *Id.* at 9–10.

38. *Id.* at 5, 47–54.

39. 47 U.S.C. § 301 (2018); 47 C.F.R. § 24.1 (2018); *see also* FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73100176 (Mar. 2, 2012), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=vPxvZeEaq4qhr7N5OMugqw%3D%3D&fcc_id=NK73100176 [https://perma.cc/YAW4-TR9J]; FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73166210 (Mar. 2, 2012), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=S02SFOCotzKlbdYCDPFIlA%3D%3D&fcc_id=NK73166210 [https://perma.cc/P779-HQQH]; FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73092523 (Mar. 2, 2012), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=1qg4iWNE3Ijyqf%2F9UfNNSQ%3D%3D&fcc_id=NK73092523 [https://perma.cc/EN6C-7X5N].

40. *See* FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73100176, *supra* note 39; FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73166210, *supra* note 39; FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73092523, *supra* note 39.

41. *See* U.S. Dep't of Justice, Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations (June 29, 2012), https://www.documentcloud.org/documents/1727748-nondisclosure-agreement.html [https://perma.cc/PYU7-2XHR]; Adam Bates, *Stingray: A New Frontier in Police Surveillance*, 809 CATO INSTITUTE POLICY ANALYSIS 1 (2017), https://www.cato.org/publications/policy-analysis/stingray-new-frontier-police-surveillance [https://perma.cc/BLA7-EYC6].

might otherwise require disclosure.[42]

Because of these nondisclosure agreements, states and localities have assiduously concealed the use of Stingray devices in criminal prosecutions. They have operated on the understanding that merely disclosing the existence and use of such a device would violate the federal nondisclosure requirement. In cases where it has appeared that the criminal prosecution may result in compelled disclosure of information about the device, prosecutors have sometimes dropped charges rather than permit disclosure.[43]

Law enforcement has also resorted to other measures in an effort to conceal the use of a Stingray and, therefore, to avoid disclosure and challenges to the lawfulness of the technique. In many cases, it appears that when law enforcement obtains a court order or warrant meant to authorize the use of a Stingray, law enforcement omits any mention of the Stingray in the application or court order.[44] In some instances, the application and court order affirmatively misrepresent that police will obtain information from the telephone company when in fact police mean to bypass the telephone company by deploying a Stingray.[45] In such cases, the criminal defendant is unlikely to learn that a Stingray has been deployed—and therefore will be unable to challenge its use—unless there are other indicia of the Stingray's use and defense counsel is alert to the possibility.[46] This secrecy tactic may account for the small number (and recent vintage) of reported decisions assessing the legality of a Stingray's use.[47]

---

42. Pell & Soghoian, *supra* note 1, at 38.

43. *See, e.g.*, Ellen Nakashima, *FBI Clarifies Rules on Secretive Cellphone–Tracking Devices*, WASH. POST, May 14, 2015, https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html?utm_term=.047c571e87fc [https://perma.cc/26NF-TABB]; Robert Patrick, *Controversial Secret Phone Tracker Figured in Dropped St. Louis Case*, ST. LOUIS POST-DISPATCH (Apr. 19, 2015), http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html [https://perma.cc/RXA7-MBTP].

44. *See, e.g.*, United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016); *id.* at 548 (Wood, C.J., dissenting); United States v. Ellis, 270 F. Supp. 3d 1134, 1158–59 (N.D. Cal. 2017); United States v. Temple, No. 15-CR-230-1 JAR (JMB), 2017 WL 7798109, at *33 (E.D. Mo. Oct. 6, 2017); *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 748–49 (S.D. Tex. 2012).

45. *See, e.g.*, *Patrick*, 842 F.3d at 545; *id.* at 548 (Wood, C.J., dissenting); *Ellis*, 270 F. Supp. 3d at 1147.

46. Fourth Amend. Ctr., Nat'l Ass'n of Criminal Def. Lawyers, *Cell Site Simulators*, 2016 NAT'L ASS'N. CRIM. DEF. LAW. FOURTH AMEND. CTR. 1 https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-4-28_Cell-Site-Simulator-Primer_Final.pdf [https://perma.cc/ZE3U-27CY].

47. The first public judicial decision assessing the legal parameters governing law enforcement use of Stingrays was issued sua sponte by Magistrate Judge Brian Owsley in

Law enforcement agencies may also have concealed the use of Stingrays from criminal defendants and courts using a tactic known as "parallel construction." This is the practice of conducting a second, parallel investigation designed to "discover" evidence that was previously identified using the secret technology.[48] When the government presents the evidence to the defendant or the court, it is only the second, "clean" investigation that is disclosed. This serves to avoid both exposure and adjudication of the novel technique in the context of a suppression motion. It appears that the FBI encouraged state and local law enforcement to engage in this tactic.[49]

In 2015, in response to media reports about the sweeping federal secrecy mandate imposed upon state and local law enforcement, the FBI clarified its policy, explaining that states and localities were no longer prohibited from disclosing the mere *existence* of a Stingray and the fact of its use.[50] The FBI thus acknowledged that law enforcement could tell a criminal defendant that police had used the device. The FBI continues to maintain, however, that states and localities must resist, by all means necessary, compelled disclosure of information regarding the capabilities of such devices and the methods by which they are used—even requiring prosecutors to dismiss indictments.[51]

The FBI has explicitly invoked the anti-circumvention argument as its justification for these extraordinary efforts to conceal the use of Stingray devices by law enforcement at all levels of government. A 2014 affidavit from a senior FBI official contended, "information concerning this equipment, if

response to an ex parte application by the local U.S. Attorney's Office seeking authorization to use the device. *See In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 747. The next challenge was raised by a pro se criminal defendant who managed to discover the secret use of a Stingray device while imprisoned facing criminal charges. *See* United States v. Rigmaiden, No. 08-cr-814, 2013 WL 1932800 (D. Ariz. May 8, 2013); *infra* notes 232–236 and accompanying text.

48. *See generally* HUMAN RIGHTS WATCH, DARK SIDE: SECRET ORIGINS OF EVIDENCE IN U.S. CRIMINAL CASES (2018); Grayson, *supra* note 31; *see also* Fairfield & Luna, *supra* note 31, at 1042–43; Toomey & Kaufman, *supra* note 31, at 863–64.

49. *See, e.g.*, Jenna McLaughlin, *FBI Told Cops To Recreate Evidence from Secret Cell-Phone Trackers*, INTERCEPT (May 5, 2016), https://theintercept.com/2016/05/05/fbi-told-cops-to-recreate-evidence-from-secret-cell-phone-trackers/ [https://perma.cc/X8ZU-8Y4K]; John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS, Aug. 5, 2013, http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805 [https://perma.cc/NZ4K-ZZYL]; HUMAN RIGHTS WATCH, *supra* note 48, at 18.

50. *See* DEP'T OF JUSTICE POLICY GUIDANCE, *Use of Cell-Site Simulator Technology* (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/A7JL-PRMA] [hereinafter DOJ Guidance].

51. *See* e-mail from Christopher M. Allan, FBI, to Cyrus Farivar, ArsTechnica (May 15, 2015, 17:59), https://www.documentcloud.org/documents/2082240-urgent-copy-of-Stingray-statement.html [https://perma.cc/9BQK-8ERZ].

made public, could easily impair the use of this investigative method."[52] The affidavit predicted that disclosure would permit the perpetrators in "criminal cases involving terrorism, kidnappings, murder, and other conspiracies" to evade detection and go unprosecuted. What the affidavit did not acknowledge, however, is that Stingray technology was by then available in the public domain and known to anyone who cared to investigate. It also did not grapple with the fact that there was common knowledge among criminals that police had various means to track the location of cell phones.[53]

Public defender offices and civil liberties organizations, like the American Civil Liberties Union and the Electronic Privacy Information Center, have mounted a transparency campaign to try to force disclosure of information about police use of Stingrays. These groups and likeminded individuals have filed and litigated FOIA requests directed at both federal government[54] and state and local law enforcement.[55] These organizations have also sought to unseal records from cases in which it appears that the use of Stingrays may have been at issue.[56]

Unsurprisingly, the government has opposed these efforts vigorously. In response to the FOIA lawsuits, the government has argued—among other things—that information about Stingrays may be withheld from the public pursuant to the FOIA exemption for law enforcement "techniques and

52. Morrison Affidavit, *supra* note 13, at 2; *see* Fred Clasen-Kelly, *Charlotte Police Investigators Secretly Track Cellphones*, CHARLOTTE OBSERVER (Oct. 18, 2014), http://www.charlotteobserver.com/news/local/article9203591.html [https://perma.cc/2E8H-LVBW].

53. *See generally The Wire* (HBO television broadcast 2002–2008).

54. *See, e.g.*, Elec. Privacy Info. Ctr. v. FBI, 80 F. Supp. 3d 149 (D.D.C. 2015); ACLU of N. Cal. v. Dep't of Justice, 70 F. Supp. 3d 1018 (N.D. Cal. 2014), *aff'd in part, rev'd in part*, 880 F.3d 473 (9th Cir. 2018); Soghoian v. U.S. Dep't of Justice, 885 F. Supp. 2d 62 (D.D.C. 2012); ACLU of N. Cal. v. Dep't of Justice, No. 13-CV-03127-MEJ, 2015 WL 3793496 (N.D. Cal. June 17, 2015), *modified upon reconsideration*, 2015 WL 393496 (N.D. Cal. June 17, 2015); ACLU of N. Cal. v. Dep't of Justice, No. 12-cv-04008-MEJ, 2014 WL 4954121 (N.D. Cal. Sept. 30, 2014).

55. *See* Hodai v. City of Tucson, 365 P.3d 959 (Az. Ct. App. 2016) (accepting argument that disclosure of certain training manuals and other information regarding Stingrays could be withheld); Martinez v. Cook Cty. State's Attorney's Office, 103 N.E.3d 351 (Ill. App. Ct. 2018) (rejecting request for records about use of cell-site simulators because request was defective); Rudenberg v. Chief Deputy Attorney Gen. of Del. Dep't of Justice, No. N16A-02-006(RRC), 2016 WL 7494900, at *4–10 (Del. Sup. Ct. Dec. 30, 2016) (determining extent to which court would consider "statement of interest" filed by the United States opposing disclosure of records about Stingrays pursuant to Delaware Freedom of Information Act), *subsequent determination* 2017 WL 7000854 (Del. Sup. Ct. Dec. 8, 2017); N.Y. Civil Liberties Union v. Erie Cty. Sheriff's Office, No. 2014/000206, 2015 WL 1295966 (N.Y. Sup. Ct. Mar. 17, 2015) (ordering disclosure of various withheld records concerning cell-site simulators).

56. *See ACLU of N. Cal.*, 2014 WL 4954121, at *4–5.

procedures."[57] The federal government has also sought to participate in litigation under *state* open records laws to enforce the confidentiality requirements it has imposed on state and local law enforcement.[58] A small number of courts have been skeptical of these arguments and rejected them.[59] But where courts have ordered disclosure, it has only been because a significant amount of information about Stingrays was already available in the public record and the government failed to demonstrate that disclosure of additional records would have revealed more granular details about the technique.[60]

Because of these multi-pronged transparency efforts, we have learned more about the capabilities of these devices and the circumstances in which law enforcement believes it can use them. Still, some agencies continue to oppose disclosure of even the most basic information—like the cost of the devices and the number purchased—let alone information about the capabilities of the devices and guidelines governing their use.[61]

In parallel with the transparency campaign, advocates have undertaken efforts to establish legal standards about how this surveillance technology should be used. Before the concerted transparency effort around Stingrays kicked off, the rules governing their use were either shrouded in secrecy or nonexistent. It appears that many jurisdictions used Stingrays at will, without any prior judicial authorization,[62] notwithstanding that a number of sources of law—including potentially state wiretap laws and Fourth Amendment limits—seem very likely to apply to most uses of the devices.

Now that Stingrays have begun to come out of the shadows, there has been movement toward legal oversight of the technology's use. At least four state appellate courts have now held that a warrant based upon probable cause is required in order to deploy a Stingray.[63] Since 2015, at least five states have

57. *See supra* note 54 (collecting federal FOIA cases).

58. *See, e.g.*, *Rudenberg*, 2016 WL 7494900; *N.Y. Civil Liberties Union*, 2015 WL 1295966.

59. *See, e.g.*, *ACLU of N. Cal.*, 70 F. Supp. 3d 1018, *Rudenberg*, 2016 WL 7494900; *N.Y. Civil Liberties Union*, 2015 WL 1295966, at *11–13. *But see Soghoian*, 885 F. Supp. 2d at 74–75.

60. *See* ACLU of N. Cal. v. Dep't of Justice, 880 F.3d 473 (9th Cir. 2018), *aff'g in relevant part* 70 F. Supp. 3d 1018 (N.D. Cal. 2014). *But see Soghoian*, 885 F. Supp. 2d at 74–75.

61. *See, e.g.*, FOIL Request from N.Y. Civil Liberties Union to N.Y. Police Dep't (Apr. 13, 2015), https://www.nyclu.org/sites/default/files/20150413_FOIL_request_NYPD_stingrays_web.pdf [https://perma.cc/5NR3-QBZ4]; Response to FOIL Request from N.Y. Police Dep't to N.Y. Civil Liberties Union (Oct. 30, 2015), https://www.nyclu.org/sites/default/files/20151030_FOIL_response_NYPD_stingrays_web.pdf [https://perma.cc/YQZ2-S3QM].

62. *See, e.g.*, *Stingrays*, N.Y. CIV. LIBERTIES UNION (last updated May 2016) https://www.nyclu.org/en/Stingrays [https://perma.cc/F7HJ-N8D8] (describing policies of various jurisdictions in New York).

63. *See* Jones v. United States, 168 A.3d 703, 711–17 (D.C. 2017) (finding that the use of a cell-site simulator to locate an individual is a search and requires a warrant based on probable

enacted laws requiring a warrant before a Stingray can be used to determine a person's location.[64] Moreover, at least four federal district courts have considered the Fourth Amendment limits on use of Stingrays.[65] Still, no federal appellate court has yet considered whether use of a Stingray even constitutes a "search" for purposes of the Fourth Amendment.[66] Meanwhile, the Department of Justice (DOJ) has made a voluntary policy change—perhaps in order to mitigate litigation risk and avoid binding precedent—that now requires the FBI to obtain a warrant to use a Stingray device unless one of two exceptions applies.[67] Other agencies have also now adopted internal policies.[68] But it is unclear how closely such policies are being followed, even within DOJ.[69]

---

cause); State v. Andrews, 134 A.3d 324, 371–99 (Md. Ct. Spec. App. 2016) (finding the same); Tracey v. Florida, 152 So. 3d 504, 526 (Fla. 2014) (suppressing evidence obtained from a warrantless use of an IMSI catcher); State v. Tate, 357 Wis. 2d 172, 201 (Wis. 2014) (holding that a warrant was required to use cell-site simulator).

64. *See* CAL. PENAL CODE § 1546 (West 2015); 725 ILL. COMP. STAT. 137 (West 2016); UTAH CODE ANN. § 77-23c-102 (West 2016); VA. CODE ANN. § 19.2-70.3 (2016); WASH. REV. CODE § 9.73.260 (2015).

65. *See* United States v. Ellis, 270 F. Supp. 3d 1134, 1140 (N.D. Cal. 2017) (finding that the use of cell-site simulator is a search under the Fourth Amendment and requires probable clause); United States v. Lambis, 197 F. Supp. 3d 606, 610–11 (S.D.N.Y. 2016) (finding the same); United States v. Temple, No. 15-CR-230-1 JAR(JMB), 2017 WL 7798109, at *30–36 (E.D. Mo. Oct. 6, 2017) (finding that a court order founded upon probable cause was sufficient to authorize use of a cell-site simulator); *In re* Application of the United States for an Order Relating to Telephones Used by Suppressed, No. 15-M-0021, 2015 WL 6871289, at *3–4 (N.D. Ill. Nov. 9, 2015) (setting out Fourth Amendment requirements to minimize collection of innocent third party information when using cell-site simulator).

66. *See* United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016) (declining to determine whether use of a Stingray is a "search"); *id.* at 546 (Wood, J., dissenting) ("This is the first court of appeals case to discuss the use of a cell-site simulator, trade name 'Stingray.' ").

67. *See* DOJ Guidance, *supra* note 50, at 3–5 (explaining that a warrant is required unless there are "exigent circumstances" or other unspecified "exceptional circumstances where the law does not require a warrant").

68. *See generally* COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHNOLOGIES: PRIVACY CONCERNS AND RECOMMENDATIONS 23–27 (Dec. 19, 2016), https://assets.documentcloud.org/documents/3242927/The-FINAL-Bipartisan-Cell-Site-Simulator-Report.pdf [https://perma.cc/9DMH-CRDJ] (describing and comparing the policies adopted by several federal agencies, including the Department of Homeland Security, the Internal Revenue Service, and the Treasury Inspector General for Tax Administration, as well as a number of local jurisdictions).

69. According to a discussion with a public defender at the Legal Aid Services of New York, the U.S. Marshals Service, working in cooperation with the New York Police Department (NYPD), deployed a Stingray without obtaining a warrant but instead on the basis of a court order that did not require probable case. This alleged use of the Stingray by the Marshals Service, which is part of the DOJ, post-dated the DOJ's policy change.

B. THE MYSTERY OF MOBILE X-RAY VANS

Mobile x-ray vans present another archetypical example of innovative technology that police keep firmly under wraps. As with Stingrays, police have justified this secrecy as a measure to protect against circumvention. But, in practice, secrecy has ended up impeding any meaningful legislative, judicial, or public oversight.[70]

According to the promotional material of the mobile x-ray van's manufacturer (which is freely available online), the vans operate by "directing a sweeping beam of x-rays at the object under examination, and then measuring and plotting the intensity of the scattered x-rays . . . ."[71] The result is an image that clearly depicts organic material—drugs, explosives, and people—in silhouette.[72] The promotional materials promise that police can use the vans on the streets even while in motion, at speeds up to six miles per hour, scanning cars and other objects that pass alongside and "provid[ing] a complete field of view of vehicles of all heights, including the tires."[73]

The vans use the same x-ray backscatter technology that was at one point deployed in airports to conduct body scans. Those devices were criticized because of concerns about privacy: the devices' ability to see through clothes produced what some called "virtual strip searches."[74] There were also significant health concerns because the devices emit ionizing radiation.[75] The Transportation Security Administration ultimately removed the x-ray devices from airports in favor of devices that rely on "millimeter waves" and emit no

70. More than a decade ago, NYPD acquired this kind of mobile van equipped with x-ray technology. According to accounts by reporters embedded with the NYPD bomb squad, the vans have been used by NYPD since at least 2004. *See* RICHARD ESPOSITO & TED GERSTEIN, BOMB SQUAD: A YEAR INSIDE THE NATION'S MOST EXCLUSIVE POLICE UNIT (Hyperion Books 2017); Grabell, *supra* note 4. The NYPD Commissioner has acknowledged that NYPD has such vans. *See* Yoav Gonen & Shawn Cohen, *NYPD has super-secret X-ray vans*, N.Y. POST, Oct. 13, 2015, http://nypost.com/2015/10/13/nypd-has-secret-x-ray-vans/ [https://perma.cc/9K8C-W842].

71. *Z Backscatter Technology Was Pioneered By AS&E*, AS&E, http://as-e.com/resource-center/technology/z-backscatter/ [https://perma.cc/7VTP-JTU9].

72. *Id.*

73. *Mobile Z Backscatter Cargo and Vehicle Screening System*, AS&E, https://www.rapiscan-ase.com/products/mobile/product/zbv [https://perma.cc/9996-UCXR].

74. *See* Competitive Enter. Inst. v. Dep't of Homeland Sec., No. 16-1135, 688 F. App'x 20, 2017 U.S. App. LEXIS 9324 (D.C. Cir. May 26, 2017); *Backgrounder on Body Scanners and "Virtual Strip Searches"*, ACLU, https://www.aclu.org/aclu-backgrounder-body-scanners-and-virtual-strip-searches [https://perma.cc/RD47-EV8X].

75. *See* Markham Heid, *You Asked: Are Airport Body Scanners Safe?*, TIME (Aug. 23, 2017), http://time.com/4909615/airport-body-scanners-safe/ [https://perma.cc/Y9YY-E7CM].

radiation.[76]

The vans raise similar health and privacy concerns. With respect to the health concerns, the manufacturer of the device contends that radiation doses are well below specified limits. Advertising material states that one scan of an object at a distance of five feet, conducted while the van is travelling at three miles per hour, delivers a radiation dose of 0.1 microsieverts, "equivalent to flying 2 minutes at altitude."[77] But the exposure depends entirely on how the device is used by the police. If the device is closer to a target or if a particular location is repeatedly or continuously scanned, exposure levels would be higher.

The device also raises obvious privacy concerns. The specified purpose of the vans is to see inside vehicles and, perhaps, buildings, in order to identify objects not otherwise visible, including at least the silhouette of a person's body beneath their clothes. Unlike airport scanners, x-ray vans can operate surreptitiously, without the subject's knowledge or consent.

In many likely applications, the mobile x-ray vans will implicate the Fourth Amendment. For instance, the Fourth Amendment generally permits warrantless searches inside vehicles only if "probable cause exists to believe it contains contraband."[78] In some limited circumstances, it may be permissible to conduct a suspicionless administrative search—for example, at the international border[79]—but in ordinary policing, probable cause is required. The vans, however, are designed to be readily used to conduct indiscriminate searches. As the promotional material suggests, the van can scan vehicles on the streets as it drives by.[80] One can also easily imagine the van scanning all vehicles passing a particular traffic chokepoint (like, for example, the entrance to a bridge or tunnel).

There is little information about how broadly mobile x-ray vans are in use by police across the country, and what rules govern them. The New York Police Department (NYPD), which is one of the few departments known to have this technology, has disclosed neither what position it takes with respect to these Fourth Amendment concerns nor whether it uses the vans in ways that raise significant constitutional questions.

---

76. *See* Mike M. Ahlers, *TSA removes body scanners criticized as too revealing*, CNN (May 30, 2013), http://www.cnn.com/2013/05/29/travel/tsa-backscatter/ [https://perma.cc/3AP8-7B3Q].

77. *ZBV Cargo and Vehicle X-ray Screening System,* AS&E, https://www.rapiscan-ase.com/uploads/documents/ZBV_Privacy_and_Safety_Assured.pdf [https://perma.cc/Q255-TP97].

78. Pennsylvania v. Lebron, 518 U.S. 938, 940 (1996).

79. *See* United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004).

80. *See supra* note 73.

To the contrary, NYPD has made determined efforts to keep secret essentially all information about the vans, their capabilities, when and how they are used, and any policies or practices meant to address privacy and health concerns.[81] There do not appear to be any reported criminal cases in which law enforcement has disclosed that an x-ray van was used in the course of an investigation. To the extent that police are using the devices to investigate, law enforcement appears to be either obscuring their role or declining to bring prosecutions where their use may become subject to discovery.

NYPD has also vigorously resisted efforts to pry loose information about the vans using the Freedom of Information laws (FOIL). ProPublica reporter Michael Grabell filed a Freedom of Information request with NYPD seeking information about the specifications of the vans, procurement costs, health and privacy policies, and information about how the police had used them in the past. NYPD refused to turn over any information at all.

Grabell sued to enforce the FOIL request. In response, NYPD argued that all of the information sought was exempt because it would disclose "techniques or procedures."[82] The NYPD's submissions explicitly invoked the anti-circumvention rationale, focusing in particular on the notion that disclosure could allow terrorists to evade detection.[83] NYPD argued that disclosing even basic information about the cost or number of vans could allow terrorists to deduce information that would permit circumvention.[84] NYPD likewise refused to turn over any information about health, safety, and privacy because it could permit circumvention.[85]

The trial court judge largely rejected these arguments and ordered significant disclosure after taking an unusually detailed, fact-intensive approach to the determination about whether disclosure could lead to circumvention.[86] In particular, the court found that NYPD could only withhold documents disclosing when and in what particular circumstances the vans may *not* be used.[87] The court reasoned that disclosure of such information "would extend a free pass from detection by the Van(s)" in such circumstances.[88] On the other hand, the court did order disclosure of information regarding (1) the locations where the vans had *previously* been used, (2) general policies, procedures, and

81. *See infra* notes 82–85.

82. Grabell v. N.Y.C. Police Dep't, 996 N.Y.S.2d 893, 896 (Sup. Ct. 2014).

83. *Id.* at 210–15 (discussing Affidavit of Richard Daddario, NYPD Dep't Comm. of Counterterrorism in Support of Answer). The author was among counsel for the petitioner in this case.

84. *Id.* at 212.

85. *Id.* at 213.

86. *Id.* at 210–16.

87. *Id.* at 212.

88. *Id.*

training materials (to the extent they did not disclose where vans could not be used), (3) information regarding the cost of the vans, (4) records describing the data retention/privacy policies governing the images taken by the vans, and (5) information regarding health and safety effects regarding their use.[89] With respect to all of these kinds of documents, the court found that NYPD had failed to make a detailed or persuasive showing that disclosure could actually create a substantial risk of circumvention.[90]

On appeal, however, the appellate court was far less searching in its scrutiny of the anti-circumvention arguments presented by NYPD. The court agreed with NYPD's blanket argument that disclosing any information about "the strategies, operational tactics, uses and numbers of the vans would undermine their deterrent effect, hamper NYPD's counterterrorism operations, and increase the likelihood of another terrorist attack."[91] In addition, disclosure of past deployments of the vans "would allow terrorists to infer the inverse, namely, locations and times when NYPD does not use them, and would permit a terrorist to conform his or her conduct accordingly."[92] On this basis, the court allowed NYPD to withhold *all* information about the vans, except "tests or reports regarding the radiation dose or other health and safety effects," which amounted to a single three-page report.[93]

In reaching this ruling, the appellate court was willing to defer to NYPD's high-level speculation about circumvention risk. For example, the court failed entirely to engage with the significant amount of public information already available about the vans, including images of the vans provided by the manufacturer, which would allow any would-be terrorist to identify whether a van is deployed in the immediate vicinity.[94]

As a result of the decision, the public remains in the dark about when NYPD believes it can use the vans and how NYPD handles health and privacy concerns. It is entirely possible, for example, that NYPD uses the vans to perform random spot checks of city blocks. Or perhaps it routinely scans certain locations, regularly exposing pedestrians or an unwitting food vendor to significant doses of radiation. Perhaps it only uses the vans where it has probable cause to believe a vehicle contains contraband. Or maybe NYPD operates the vans without any suspicion at all, perhaps on the view that such searches fall within a controversial "special needs" exception to the Fourth

89. *Id.* at 205–06.

90. *Id.* at 210–16.

91. Grabell v. N.Y.C. Police Dep't, 139 A.D.3d 477, 478–79 (N.Y. App. Div. 2016).

92. *Id.* at 479.

93. *Id.*; Email from Susan Paulson, Senior Counsel New York City Law Department to John Langford and David Schulz, Counsel for Michael Grabell (Jan. 17, 2017) (on file with author).

94. *Grabell*, 139 A.D.3d at 478–79.

Amendment's warrant requirement because they are ostensibly aimed at protecting against terrorism, even if in practice they end up only turning up evidence of ordinary crime.[95]

Not only is the public in the dark but also, importantly, regulation of the use of the vans has been left solely in the hands of the police. In the absence of basic information regarding the police's current practices, it has not been possible to mount court challenges or mobilize legislative efforts to rein in any potential abuses. Citizens and legislators are left to speculate about potential concerns, while the police can now point to a judicial opinion endorsing the notion that it would pose an unacceptable terrorism risk even to make public the non-binding internal guidelines, if any, that currently regulate the use of the vans. The anti-circumvention rationale thus continues not just to prevent transparency, but to postpone or frustrate any meaningful public deliberation or regulation even now, well over a decade after the technology was first acquired.[96]

III. THE PROBLEM WITH SECRET LAW ENFORCEMENT TECHNOLOGIES

This Part examines the democratic costs that anti-circumvention secrecy imposes. In particular, it canvases how secrecy about police technology impairs the constitutional role of courts and legislatures, leading to a self-regulatory regime without meaningful checks on law enforcement. It also explores how anti-circumvention secrecy can upend the relationship between the public and police, to the detriment of both.

A. SECRECY IMPEDES THE ABILITY OF COURTS TO ADJUDICATE THE LEGAL LIMITS WITHIN WHICH NEW TECHNOLOGIES MAY BE USED

As we have already seen, many novel police technologies raise significant constitutional or statutory concerns. Police can use them in ways that press beyond established limits, or at least raise serious questions about their legality. Of course, regulation of the government's investigatory powers is a primary concern of the Constitution; the Bill of Rights contains multiple provisions that limit how the government may go about investigating individuals.[97] The statute books also contain detailed legal regimes meant to regulate investigative

95. *See, e.g.*, MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006) (upholding a suspicionless subway search program under the special needs doctrine on the theory that the programmatic purpose was to prevent terrorist attacks).

96. *See* Michael Grabell, *Split Decision on NYPD's X-ray Vans*, PROPUBLICA (May 10, 2016), https://www.propublica.org/article/split-decision-on-nypds-x-ray-vans [https://perma.cc/75LR-5LFE].

97. *See generally* U.S. CONST. amends. IV, V, VI.

and surveillance techniques.[98] Typically, we rely on the courts to authoritatively adjudicate the meaning of these constitutional and statutory provisions and the protections they do or do not offer in particular circumstances. Secrecy threatens to upend this check on law enforcement.

If techniques and capabilities are secret, then litigation is much more difficult, and perhaps impossible. Affirmative cases challenging such techniques are likely to fail because secrecy puts up threshold barriers to adjudication. For instance, plaintiffs will often be unable to establish standing to challenge a secret technique. The Supreme Court in *Clapper v. Amnesty International* held, with respect to a surveillance program, that plaintiffs lacked standing unless the "threatened injury [is] certainly impending."[99] In particular, the Court required the plaintiffs to demonstrate that they were in fact targeted by the challenged surveillance program.[100] But the details of the program and its operations were a closely guarded secret, so the plaintiffs could not make that case.

Similar concerns thwart efforts to challenge other novel investigative methods—Stingrays, x-ray vans, and the like. Unless and until the police choose to reveal how these devices are used (and that certain individuals have been targeted), it will be difficult for any plaintiff to show that they have suffered an injury sufficient to establish standing. Put differently, the police can often guard against the prospect of affirmative litigation simply by keeping a tight lid on details about where, when, how, or against whom they are using these new technologies.[101]

Of course, constitutional and statutory adjudication may also arise in a defensive context, where a criminal defendant learns that police have used a certain method and the defendant chooses to contest it on a motion to suppress. But, as detailed already, the government has developed tactics, including filing opaque or misleading warrant applications, engaging in "parallel construction," or simply dropping charges, that are designed to avoid

98. *See, e.g.*, Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (regulating wiretaps); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (regulating electronic communications while in transit and at rest, as well as regulation of pen register devices); Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 (1994)) (amending Electronic Communications Privacy Act); USA Patriot Act, tit. II, Pub. L. No. 107-56, 115 Stat. 272 (2001) (amending Electronic Communications Privacy Act and the Foreign Intelligence Surveillance Act); FISA Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436 (2008); USA Freedom Act, Pub. L. No. 114-23, 129 Stat. 268 (2015) (limiting certain surveillance powers).

99. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013).

100. *Id.* at 410–13.

101. *See* Manes, *supra* note 22, at 821–26 (examining various obstacles that secrecy poses to judicial oversight of programs).

adjudication by keeping criminal defendants in the dark that novel techniques have been used.[102]

But even if law enforcement is not completely obscuring its reliance on novel techniques, it may provide defendants and courts with so few details about its techniques as to make constitutional adjudication nearly impossible. In a fairly recent decision of the Seventh Circuit Court of Appeals—the first federal appellate court to encounter the use of Stingrays—Judge Diane Wood elaborated on these problems in a lengthy dissent.[103] In that case, the government "appear[ed] to have purposefully concealed the Stingray's use from the issuing magistrate, district court, and defense counsel."[104] Indeed, the defendant had litigated his motion to suppress "based on the government's representation that the officers tracked his location using information provided by the cell phone service provider."[105] The government admitted the truth—that it had in fact used a Stingray and not records from the phone company—only after the defendant and supporting amici filed their briefs on appeal.[106]

Even after admitting its use, however, the government refused to provide any details about "the way in which the Stingray . . . was configured" or "the extent of its surveillance capabilities."[107] The government refused to say, for example, whether agents used the device solely to determine locations or whether they used it in an even more aggressive manner to "capture the e-mails, texts, contact lists, images, and other data."[108] In the absence of this kind of information, Judge Wood contended that it was impossible for the court to adjudicate whether its use was constitutional or whether it was even authorized by the location-tracking warrant that the magistrate judge had issued in that case. As she lamented, "we must know how it works and how the government used it before we can judge whether it functions in a manner [consistent with] the location-gathering methods specified in the warrant" that was actually obtained.[109]

102. Toomey & Kaufman, *supra* note 31; *see supra* notes 44–46 and accompanying text.

103. United States v. Patrick, 842 F.3d 540, 545–52 (7th Cir. 2016) (Wood, C.J., dissenting).

104. *Id.* at 546.

105. United States v. Patrick, No. 13-CR-234, 2016 U.S. Dist. LEXIS 59933, at *2 (E.D. Wisc. May 5, 2016).

106. *Patrick*, 842 F.3d at 546.

107. *Id.* at 547.

108. *Id.* (internal citations omitted).

109. *Id.* at 546.

Even in cases where the government concedes that it used a novel technology, it can avoid adjudication of constitutional questions by making strategic concessions. Thus, in at least one case, prosecutors conceded, solely for purposes of that particular case, that use of Stingrays was a "search" subject to the Fourth Amendment.[110] By making that concession, the government avoided a judicial ruling on that central constitutional question.[111]

Stingrays are but one example of how secrecy impedes judicial oversight. Twenty years after they came into use, courts are only beginning to grapple with Stingrays' legality. The courts remain completely shut out of the picture with respect to many other novel technologies that have yet to see their moment in the sun. Secrecy, it turns out, does not just shield police technology from the public but also from the courts.

B. ANTI-CIRCUMVENTION ARGUMENTS MILITATE AGAINST LEGISLATIVE ENACTMENTS THAT LIMIT HOW NEW TECHNOLOGIES MAY BE USED

Litigation is only one means we have to regulate law enforcement's use of technology. Legislatures at all levels of government have authority to enact laws imposing requirements upon the use of investigative techniques.[112] Secrecy, however, impedes this kind of democratic oversight and deliberation, as well. Indeed, the anti-circumvention argument specifically militates against the adoption of public rules governing novel technologies, because knowing these rules may create opportunities for circumvention.

Legislative efforts to regulate law enforcement capabilities are very difficult where the methods are secret because there will be no public pressure or electoral rewards for acting. Even if the existence of a technique is public (as with x-ray vans), the absence of information about how police use it will impede efforts to make the case for legislative action. Without vivid stories about how police use or misuse a technique, against whom, and for what purposes, it will be difficult or impossible to mobilize support for oversight.[113] And without pressure from constituents, community groups, advocacy organizations, and the like, it is unlikely there will be a legislative response.

---

110. *See* United States v. Rigmaiden, 844 F. Supp. 2d 982, 995–96 (D. Ariz. 2012); *see generally infra* notes 232–236 and accompanying text.

111. *See Rigmaiden*, 844 F. Supp. 2d at 996 n.6.

112. *See, e.g.*, Electronic Privacy Communication Act, 2015 Stat. Cal. Ch. 651 (codified at Cal. Penal Code §§ 1546–1546.4 (2016)); Biometric Information Privacy Act, Ill. Pub. Acts 95-994 (codified at 740 Ill. Comp. Stat. § 14 (2008)).

113. *See generally* Deborah A. Stone, *Causal Stories and the Formation of Policy Agendas*, 104 POL. SCI. Q. 281 (1989).

The anti-circumvention rationale also discourages legislative oversight and regulation of novel law enforcement techniques for a more fundamental reason: the logic of anti-circumvention itself militates against having public rules or standards governing the use of a technology. The basic idea of anti-circumvention is that disclosing information about methods would give bad actors a roadmap to circumvent or evade them. But these same arguments militate against enacting public rules regarding how and when such techniques may be used. After all, to make rules governing a technology's use is both to confirm its existence and to disclose limits on its use. Anti-circumvention arguments, where accepted, therefore tend to be arguments not just against disclosure by law enforcement but against any kind of public, democratic regulation and control.

This troubling implication of the anti-circumvention argument is particularly acute with respect to contemporary and emerging electronic technologies. This is because the capabilities of a technology (and, therefore, potential vulnerabilities) can be defined either by technological limits or legal limits on its use.[114] Whether a Stingray can intercept the content of text messages is as much a question of the technical capabilities of a particular device as it is a question about whether and in what circumstances the law allows police to use it in this way. Put differently, from the perspective of the hypothetical criminal seeking to circumvent the Stingray, knowing that the Stingray cannot technically intercept the content of text messages provides similar prospects for evasion as knowing that the Stingray cannot be used to intercept text messages unless the police already have probable cause and have obtained a warrant covering a particular cell phone. Thus, when it comes to technology, anti-circumvention arguments often stray from a concern to avoid disclosure of technical information into a concern to avoid disclosure of legal and policy limits.[115]

In practice, secrecy has indeed resulted in legislative action being avoided, misdirected, or delayed. With respect to Stingray devices, former prosecutor Stephanie Pell and technologist Christopher Soghoian have documented that legislatures at every level have for decades refused to engage seriously the possibility of regulating the manner in which law enforcement used these devices.[116] Instead, lawmakers enacted laws limiting the sale of Stingrays in a futile effort to prevent bad actors from obtaining the same capabilities to surveil cell phone networks as police.[117] Legislatures declined to act even

114. *See generally* LAWRENCE LESSIG, CODE 1–9 (2d ed. 2006) (arguing famously that "code is law").

115. *See supra* notes 48–49 and accompanying text.

116. Pell & Soghoian, *supra* note 1, at 2–8.

117. *Id.* at 3–4 & nn.9–10.

though nearly all of the "sensitive" capabilities they aimed to protect were in fact already a matter of public record, well-known among technologists and privacy specialists and also, presumably, among the kind of sophisticated criminals who would take countermeasures to circumvent the devices.[118] It is only now—after Stingrays received significant media attention, after a sustained public education campaign by advocacy organizations, and after a multi-pronged litigation campaign—that legislatures are beginning to pay attention and consider regulating these devices.[119] Efforts to regulate other relatively novel law enforcement techniques have likewise struggled, in large part due to the secrecy under which they currently operate.[120]

C. NEW TECHNOLOGIES AND OLD LAWS PRODUCE UNACCOUNTABLE SELF-REGULATION BY POLICE

Secrecy about police technology also exacerbates a regulatory problem that is familiar within studies of law and technology: old laws, drafted in a particular historical and technological context, tend to be a poor fit with new technologies whose capabilities and operation simply could not have been envisioned by earlier legislators. New technologies are thus often mis-regulated, subject to rules that are too strict, too lenient, or simply ill-formed.

---

118. *Id.* at 6–8.

119. Tim Cushing, *House Oversight Committee Calls for Stingray Device Legislation*, TECHDIRT (Dec. 22, 2016), https://www.techdirt.com/articles/20161219/15052936308/house-oversight-committee-calls-Stingray-device-legislation.shtml [https://perma.cc/K9JE-X7UG]; COMM'N. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHNOLOGIES: PRIVACY CONCERNS AND RECOMMENDATIONS (2016), https://assets.documentcloud.org/documents/3242927/The-FINAL-Bipartisan-Cell-Site-Simulator-Report.pdf [https://perma.cc/JK9P-8G89].

120. For example, facial recognition technology is coming into widespread use by police, yet there are extraordinarily few states with laws governing their use. *See* Garvie et al., *supra* note 5, at 35–36. To take another example, automated license plate reader (ALPR) technology has been available since the 1990's and was in very widespread use by 2012, at which point 71% of law enforcement agencies reported using the devices. *See* Jeremy Hsu, *70 Percent of U.S. Police Departments Use License Plate Readers*, IEEE SPECTRUM (July 8, 2014), https://spectrum.ieee.org/cars-that-think/transportation/sensors/privacy-concerns-grow-as-us-police-departments-turn-to-license-plate-readers [https://perma.cc/YS3C-H6WH]. Nevertheless, only two states had enacted any kind of ALPR legislation by 2012. *See* CAL. VEH. CODE § 2413 (West 2011); ME. REV. STAT. ANN. tit. 29-A § 2117-A (2009). Even today, when the vast majority of police departments have adopted the technology—and use it daily to collect massive quantities of data about the location of private vehicles—only 16 states have any legislation relating to the use of ALPRs or the retention and sharing of data collected with ALPRs. *See* NAT'L CONFERENCE OF STATE LEGISLATURES, *Automated License Plate Readers: State Statutes* (Mar. 15, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx [https://perma.cc/H6GL-P22P].

In the context of law enforcement, however, this problem of regulatory lag has a different valence: secrecy prevents (or at least delays) the development of rules governing novel technologies. As we have seen, the parts of government that typically set rules for policing—the courts and legislatures—simply cannot function properly when the techniques themselves are shrouded in secrecy.[121] Secrecy thus impedes the ability of courts to adapt existing constitutional and statutory frameworks to new technologies, and it prevents legislatures from enacting new legislation. Secrecy, in other words, fosters a system of de facto self-regulation in which police agencies decide for themselves whether and how existing laws apply.

This problem of regulating novel police technologies is a special case of the broader problem—much examined in the literature—about the interaction between new technologies and old laws. Much of the literature centers on the relative merits of technology-neutral laws, which are intended to lay down principles that can be applied no matter how technology evolves, versus technology-specific laws, which govern only a particular kind of technology but do it well, and leave it for future legislators to confront whatever the future might bring.[122]

With respect to novel police capabilities, there can be legislation enacted to address particular forms of technology,[123] as well as general technology-neutral laws governing police—most prominently, the Fourth Amendment to the Constitution.[124] Unfortunately, the anti-circumvention justification for secrecy upends both modes of regulation.

Regulation of technology according to technology-neutral laws relies fundamentally on the existence of an institution that can make the judgments necessary to adapt the broad, neutral language of the law to a particular, novel circumstance. In many cases, that institution is the courts. The Fourth Amendment is a classic example: it has largely been up to the courts to

121. *See supra* Sections III.A–B.

122. *See generally* Brad A. Greenberg, *Rethinking Technology Neutrality*, 100 MINN. L. REV. 1495 (2016); Paul Ohm, *The Argument Against Technology Neutral Surveillance Laws*, 88 TEX. L. REV. 1685, 1687–700 (2010); Lyria B. Moses, *Recurring Dilemmas: The Law's Race to Keep Up With Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239 (2007).

123. For example, new law enforcement tools to hack into servers or plant malware may run up against existing technology-specific laws governing access to stored communications on a "remote computing service" or "electronic communication service." *See* Stored Communications Act of 1996, 28 U.S.C. §§ 2701–2712 (1996).

124. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1015–17 (2010) (describing the "deeply entrenched judicial consensus . . . that technology neutrality is the proper approach to the Fourth Amendment"); *see also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 748 (2005).

elaborate whether and how it regulates novel law enforcement methods.[125] Other institutions can play this updating role, too. For example, the Federal Trade Commission (FTC), an administrative body, shares authority with the courts to adapt technology-neutral protections against "unfair or deceptive acts or practices" to suit contemporary needs.[126] Specifically, the FTC can bring administrative proceedings to enforce these consumer protection standards and, ultimately, sue in court to enforce its determinations. The FTC, with the cooperation of the courts, has used this mechanism to enforce basic privacy and consumer fairness measures online, adapting the century-old provisions of the Federal Trade Commission Act of 1914 to the Internet.[127]

Secrecy regarding novel law enforcement techniques upends this model of technology-neutral regulation. If law enforcement is permitted to keep secret information about the capabilities it has and how they use them, outside institutions that might otherwise be able to determine how old, neutral laws should apply cannot do so. We have already seen an instance of this in the examples of Stingrays and mobile x-ray vans: the courts have been unable to elaborate how Fourth Amendment standards apply to these technologies precisely because of the government's furtiveness, which, in turn, has been justified by supposed anti-circumvention concerns.[128]

The interplay between secrecy and legal regulation is different and perhaps more straightforward when it comes to technology-specific regulation. Secrecy simply delays the adoption of laws that specifically regulate new technologies. As already described in the prior Section, where the details of a technology are secret, they do not attract legislative interest. To the contrary, the anti-circumvention justification for secrecy is itself an argument against enactment

125. Perhaps the most famous example of the courts playing catch-up with technology in the Fourth Amendment context is the Supreme Court's treatment of wiretapping. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that telephone wiretaps did not implicate the Fourth Amendment because they did not involve a physical trespass); *id.* at 471 (Brandeis, J., dissenting); Katz v. United States, 389 U.S. 347, 353–56 (1967) (overruling Olmstead and holding wiretapping is a "search" within the meaning of the Fourth Amendment and requires prior judicial authorization); *see also* United States v. Jones, 565 U.S. 400 (2012) (providing a more recent example of the Court's treatment of GPS tracking devices); Riley v. California, 573 U.S. 373 (2014) (regarding cell phones); Carpenter v. United States, 138 S. Ct. 2206 (2018) (regarding historical cell-site location information).

126. Federal Trade Commission Act of 1914, ch. 311, § 5, 38 Stat. 717 (codified as amended at 15 U.S.C. § 45 (2018)).

127. *Id.*; *see generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 2015 GEO. WASH. L. REV. 2230 (2015); Chris Jay Hoofnagle, *FTC Regulation of Cybersecurity and Surveillance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW (David Gray & Stephen E. Henderson, eds., 2017).

128. *See, e.g.*, United States v. Patrick, 842 F.3d 540, 546 (7th Cir. 2016) (Wood, C.J., dissenting).

of technology-specific regulation because any such regulation would necessarily reveal something about technology and the limitations placed upon its use.

Secrecy thus cuts external institutions out of the loop, hampering the ability of courts and legislatures to update old laws or enact new ones. In fact, secrecy leaves only one institution in a position to determine how old laws should apply to new technologies—law enforcement itself. Rather than having an *outside* institution determine how laws should be adapted, secrecy leads inexorably to a self-regulatory model of policing. Law enforcement agencies themselves decide what limits they must respect. The examples of x-ray vans and Stingrays provided in Part II illustrate the phenomenon: in each case, the agency itself has developed the rules governing their use. In the case of x-ray vans, those rules remain secret and entirely uncertain.[129] In the case of Stingrays, the rules were secret until very recently, when the DOJ, Department of Homeland Security, IRS, and other federal agencies each issued separate guidance about when warrants are required before an investigator can use a Stingray.[130]

One of the principal consequences of this self-regulatory model is that law enforcement will usually opt for the most permissive application of existing laws. Indeed, with respect to Stingrays, recent investigative efforts have revealed that some state and local departments had no policy documents at all regarding when they could use Stingrays.[131] In other instances, the police had misled the public about how it was applying existing laws and told reporters that Stingrays were only used with prior judicial authorization, when in fact the police agency in question only obtained a court order in one out of forty-seven deployments of the Stingray during a three-and-a-half-year period.[132] In short, the consequence of secrecy is under-regulation.[133]

Secrecy impedes the process of law catching up with new technology in one additional and very important way: it can create an entrenchment problem. Because the anti-circumvention justification for secrecy pushes courts,

129. *See supra* Section II.B.

130. *See* COMM'N. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations* (2016), https://assets.documentcloud.org/documents/3242927/The-FINAL-Bipartisan-Cell-Site-Simulator-Report.pdf [https://perma.cc/DY8H-RWWC].

131. *See Stingrays*, N.Y. CIV. LIBERTIES UNION (last updated May 2016) https://www.nyclu.org/Stingrays [https://perma.cc/UBC2-NT8F] (describing findings with respect to New York State Police).

132. *See id.* (describing findings with respect to Erie County Sheriff's Department).

133. The Georgetown Center for Privacy and Technology has documented a similar pattern with respect to police self-regulation of facial recognition technology. *See* Garvie et al., *supra* note 5, at 36–40.

legislatures, and other institutions to the sidelines, it leaves the field open for law enforcement to establish and entrench new practices and policy baselines. Police agencies can roll out a new technology, determine the most advantageous ways to use it, and develop protocols regarding such use in secret. These practices will enjoy the advantages of incumbency; they will become the status quo. By the time the coordinate branches—and the public—enter the field to scrutinize the technology, any departures from the status quo will meet powerful opposition. The law enforcement establishment will be accustomed to acting with a certain freedom. It will presumably be armed with anecdotes or data about the benefits to crime detection and prevention that come from relatively unfettered use of the technology. Correspondingly, there will be anecdotes or data about the threat to public safety that would result from putting additional limits on its use. In the face of these temporal, evidentiary, and rhetorical advantages enjoyed by law enforcement, advocates for greater judicial or legislative regulation of a technology are left trying to roll the proverbial boulder back up the hill. In short, secrecy about novel technologies not only gives law enforcement the preeminent and primary role in regulating that technology but also gives it considerable political and legal power to entrench its preferred regulatory frame in perpetuity.

D. SECRET TECHNOLOGIES RECONFIGURE THE RELATIONSHIP BETWEEN CITIZEN AND STATE

Allowing law enforcement to keep its capabilities and methods secret may also pose a more fundamental challenge. In a liberal democracy such as ours, we are committed to the proposition that individuals enjoy a sphere of freedom from intrusion by the government. One important way that we protect this conception of the relationship between government and individual is to allow the public to know what power the state potentially wields. This means allowing the public to know what investigative tools the government has at its disposal and the limits on their use.

An illustration helps make the point: imagine that the government develops hacking software that permits it to obtain easy access in bulk to all of the microphone and recording capabilities of every smartphone. The government has effectively transformed every smartphone into a listening device. This technology would raise profound privacy concerns. Now imagine that the public did not know the rules that governed when the government could switch the technology on.[134] The threat to civil liberties would be much

134. While it may seem obvious that surreptitiously turning on a recording device would require a warrant founded upon probable cause, one can at least imagine creative arguments that would permit warrantless use of such a device. For example, an enterprising law

worse, and not simply because the new tool might be misused and abused by rogue officials, but also because citizens would be left in a fundamentally vulnerable position, at the mercy of the state's secret decision about how broadly it can cast its net. The situation would be worse still if the very *existence* of this surveillance capability were a secret. In that case, citizens would not even know that the government could exercise these surveillance powers and would have no inkling that they might want to take democratic action to rein in those powers.

In this way, secrets about law enforcement techniques tend to invert the democratic relationship between the individual and government: the government's power expands in ways that are invisible to the citizenry and not subject to its control. Transparency is a fundamental safeguard that protects individuals against such encroachments by the state.[135]

At the same time, surveillance technology, by its nature, expands the stock of information that the government may obtain about citizens. Thus, while the public is in the dark about the scope of the police's investigatory power, the government has access to ever more information about individuals. History suggests that this information asymmetry can readily breed abuse, particularly in the absence of strong external checks.

This type of threat to individual liberties was illustrated most vividly in the United States by the Hoover-era FBI, and its secretive "black bag jobs" and other surveillance. For decades following the Second World War, the FBI engaged in illegal and secret operations involving breaking-and-entering, wiretaps, opening postal mail, and other invasive methods.[136] These operations often targeted political dissenters, activists, protestors, and political leaders.[137] Such activities proliferated precisely because Hoover's FBI was able to keep them secret.[138]

---

enforcement agency might argue that individuals enjoy no expectations of privacy with respect to conversations they have on the street in public, and so no warrant is required in such spaces. *See* 18 U.S.C. § 2510(2) (2018) (defining "oral communication" for purposes of the federal prohibition on warrantless interception to). One may also imagine law enforcement invoking various "special needs" exemptions to the warrant and probable cause requirement. In any case, the point is not to argue that any of these legal theories is plausible, only to show that if the technology and the rules are secret there is significant cause for alarm.

135. *See* Manes, *supra* note 22, at 814–17.

136. *See* ATHAN G. THEOHARIS & JOHN STUART COX, THE BOSS: J. EDGAR HOOVER AND THE GREAT AMERICAN INQUISITION 7–15 (1988); TIM WEINER, ENEMIES: A HISTORY OF THE FBI 191–201, 278–79 (2012).

137. *See* THEOHARIS & COX, *supra* note 136, at 14–15; WEINER, *supra* note 136, at 195–201.

138. *See* THEOHARIS & COX, *supra* note 136, at 361–78; Smith, *supra* note 28, at 245–46.

Indeed, as Judge Stephen Wm. Smith has shown in a fascinating recent article, the current legal doctrines that give the police the right to keep their techniques secret—i.e., the FOIA exemptions and the evidentiary privilege for law enforcement techniques that this Article focuses on—actually trace their roots directly back to Hoover himself.[139] Hoover dreamed up the idea of legal protection for the secrecy of techniques in the wake of *United States v. Coplon*, a high-profile prosecution of an alleged communist spy.[140] That case resulted in two calamities for the FBI. First, the court ordered an unprecedented disclosure of the FBI's illegal wiretapping operations, which showed them to have been approved at the highest levels of the FBI.[141] Second, on appeal, the Second Circuit suppressed the illegally obtained evidence and reversed the conviction.[142] As Judge Smith recounts, the lesson Hoover learned from the embarrassing episode was not to stop his agents from breaking the law, but to do a better job of keeping it secret—whether that meant hiding any paper trail or, alternatively, obtaining legal shields against disclosure.[143] Six years after the botched *Coplon* prosecution, Hoover publicly advocated for the latter course, publishing an article in the Syracuse Law Review proposing that law enforcement should have an evidentiary privilege shielding its techniques from discovery.[144] It was the first time that anybody proposed this kind of privilege.[145] And the idea was plainly motivated by the embarrassment and damage that Hoover's FBI had suffered when its illegal conduct was revealed in the *Coplon* case.[146]

Of course, there may still be *good* reasons to have protection for secret law enforcement techniques, even if such protection has its origins in a desire to perpetuate a system in which law enforcement enjoyed unchecked and oft-abused powers.[147] But the capacity for this particular kind of secrecy to shield wrongdoing and expand the power of the state unchecked has been evident from the start.

The extent to which secrecy is currently shielding illegality or abuses from coming to light is unclear. There is evidence, however, that secrecy is enabling aggressive and troubling uses of novel technologies. For example, there have

139. Smith, *supra* note 28, at 242–46; *see also* John Edgar Hoover, *The Confidential Nature of FBI Reports*, 8 SYRACUSE L. REV. 2 (1956).

140. *Id.* at 9–11; United States v. Coplon, 185 F.2d 629 (2d Cir. 1950).

141. *See* Smith, *supra* note 28, at 234, 237–40.

142. *Coplon*, 185 F.2d at 640.

143. *See* Smith, *supra* note 28, at 242–46.

144. *See* THEOHARIS & COX, *supra* note 136.

145. *See* Smith, *supra* note 28, at 234.

146. *Id.*

147. *See infra* Part IV (examining in detail the arguments for keeping law enforcement techniques secret).

been alarming revelations about the scope of government surveillance powers exercised not just by intelligence agencies like the NSA, but also by federal law enforcement. Prime among these examples is the Drug Enforcement Administration's (DEA) Hemisphere program, in which the DEA compiled a truly massive database of telephone records that logged billions of domestic and international calling records every day.[148] The database apparently includes not just information about who has called whom, but also the locations of callers—something that was omitted even from the NSA's similar domestic call database, made famous by Edward Snowden's disclosures to the press.[149] The DEA's efforts to hide this program, which have included the aggressive use of "parallel construction," suggest that it, like Hoover's FBI, may be just as concerned with evading public scrutiny and legal oversight as it is with protecting the efficacy of a law enforcement technique.[150]

Moreover, because contemporary surveillance tools are often able to sweep up massive quantities of data over extended periods, the threat to individual liberties does not necessarily abate as time passes and technologies become known. To the contrary, as more and more data is stored and made searchable for law enforcement, law enforcement's power to reach back and investigate a particular person grows apace.[151] For example, the swift proliferation of body cameras among police departments has been accompanied by the growth of online services that provide storage and hosting of the recorded videos. These databases store millions of hours of footage taken by on-duty police officers across the nation.[152] As voice-to-text and facial recognition algorithms improve, these video databases are likely to become readily searchable.[153] In a few years, law enforcement may be able to reach back in time and pull out from massive archives of footage anything that matches a

148. *See* Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES, Sept. 1, 2013 (describing the Drug Enforcement Administration's "Hemisphere" program).

149. *See id.*; ACLU v. Clapper, 785 F.3d 787, 794 (2d Cir. 2015) (NSA data included "call-routing information" but not "cell site locational information, which provides a more precise indication of a caller's location than call-routing information does").

150. *See Hemisphere: Law Enforcement's Secret Call Records Deal with AT&T*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/hemisphere [https://perma.cc/P8ZW-67EA].

151. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (discussing this phenomenon with respect to historical cell-site location data).

152. *See, e.g.*, Beryl Lipton, *Shifting from Tasers to AI, Axon wants to use terabytes of data to automate police records and redactions*, MUCKROCK (Feb. 12, 2019), https://www.muckrock.com/news/archives/2019/feb/12/algorithms-ai-task-force/ [https://perma.cc/9YXM-JCF4]; Josh Sanburn, *Storing Body Cam Data is the Next Big Challenge for Police*, TIME (Jan. 25, 2016), http://time.com/4180889/police-body-cameras-vievu-taser/ [https://perma.cc/3AT9-ZU2F].

153. *See* Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1594 (2017).

particular individual.[154] As Professor Elizabeth Joh has written, this kind of "big data" policing could also allow for automated "identification of large numbers of suspicious activities and people by sifting through large quantities of digitized data."[155] Such capabilities could easily transform the power of government to engage in both criminal law enforcement and non-criminal regulation through, for example, the child protection system, immigration enforcement, welfare and social benefits agencies, and other regimes.[156]

Put simply, a world in which police have such vast investigatory capacities would radically reorient the nature of law enforcement and its power to investigate and regulate individuals.[157] If police adopt such technologies in secret, citizens lose a powerful check against abuses and largely surrender the opportunity for meaningful public accountability that lies at the heart of our democratic constitutionalism.

E. SECRECY IMPOSES COSTS ON LAW ENFORCEMENT TOO

Thus far, this Article has focused on the normative costs that secrecy imposes from the point of view of citizens and democratic checks and balances. But there is also reason to believe that secrecy is a two-edged sword for law enforcement. The premise of the anti-circumvention argument is that police must keep secrets in order to preserve their investigative advantage over criminals. But secrecy also imposes costs on the law enforcement agencies in terms of public confidence, public input, and open exchanges of best practices.

For the reasons explored in the prior subsection, secrecy about intrusive police technologies will breed distrust among the public. Citizens who are not otherwise inclined to presume the police's good intentions are likely to regard secrecy with suspicion, cutting against the efforts of police departments to establish cooperative relationships with the communities they serve. Indeed, a major strand of the contemporary discussion around policing focuses on the

154. *See* Zak Doffman, *Facial Recognition is Coming to Police Body-Worn Cameras in 2019*, FORBES (Jan. 10, 2019), https://www.forbes.com/sites/zakdoffman/2019/01/10/body-worn-2-0-how-iot-facial-recognition-is-set-to-change-frontline-policing/#4820caf01ff3 [https://perma.cc/5GWW-LYHR] (discussing the future of real time and systematized facial recognition).

155. Elizabeth Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 19 (2016).

156. *See generally* Jennifer Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327 (2014) (examining the broad powers law enforcement has to regulate people using watchlists and other means that impair an individual's freedom short of incarceration).

157. *See generally* Christina M. Mulligan, *Perfect Enforcement of Law: When To Limit and When To Use Technology*, 14 RICH. J.L. & TECH. 13 (2008) (examining the consequences and normative challenges posed by technology that could permit perfect surveillance or perfect detection of criminal violations).

idea of building trust between law enforcement and citizens.[158] The literature suggests that police-community relations improve when the public regards policing as legitimate.[159] Transparency is one piece of establishing such legitimacy, as part of a broader focus on establishing perceptions of procedural justice in the community.[160]

Transparency also benefits police in another way: it allows the police the benefit of input and advice from experts and laypeople alike. Where technologies or the rules that govern them are secret, police are limited to relying on whatever expertise they have in-house or, more likely, the recommendations of the outside vendor who sold them the technology.[161] Secrecy makes it difficult or impossible for police to open up their practices to constructive input from experts, other law enforcement agencies, or the public itself. This breeds suboptimal practices. Perhaps police will underutilize a technology because police do not realize all of its potential applications. Perhaps police will overuse a technology or use it too haphazardly because officers have not been presented with more efficient (or more legally defensible) means of deploying it. If techniques are public, law enforcement may even be motivated to find more creative—and perhaps more effective—approaches to its investigations that don't rely on secret methods.

In these ways, secrecy throws up obstacles to law enforcement, potentially frustrating efforts to improve police-community relations and impeding the flow of advice, experimentation, and expertise about how to use novel technologies. In some cases, at least, it seems that law enforcement may determine that it is in its own best interests not to forego the potential benefits of transparency in order to try to prevent circumvention at the margins.

IV. THE LOGIC OF ANTI-CIRCUMVENTION SECRECY

The previous Part argued that secrecy justified on anti-circumvention grounds raises serious normative and policy concerns. This Part takes the anti-circumvention rationale seriously on its own terms in order to understand its strengths and its limits. It begins by describing the logic of anti-circumvention:

158. *See, e.g.*, LORAINE MAZEROLLE ET AL., LEGITIMACY IN POLICING 4–5 (U.S. Dept. of Justice, Office of Community Oriented Policing Services, Legitimacy in Policing No. 10 2013); POLICE EXECUTIVE RESEARCH FORUM, OPERATIONAL STRATEGIES TO BUILD POLICE-COMMUNITY TRUST AND REDUCE CRIME IN MINORITY COMMUNITIES: THE MINNEAPOLIS CEDAR-RIVERSIDE EXPLORATORY POLICING STUDY 1–3, 10–12 (2017).

159. *See generally* Tom Tyler, *Procedural Justice and Policing: A Rush to Judgment?*, 13 ANN. REV. L. & SOC. SCI. 29 (2017); Tracy Meares, *The Path Forward: Improving the Dynamics of Community-Police Relationships to Achieve Effective Law Enforcement Policies*, 117 COLUM. L. REV. 1355, 1360 (2017).

160. *See* Meares, *supra* note 159, at 1362–63.

161. *See* Crump, *supra* note 12; Joh, *supra* note 12.

what empirical and analytic claims the anti-circumvention argument for secrecy relies on. It then proceeds to unpack the normative assumptions built into the anti-circumvention argument.

The basic anti-circumvention argument for secrecy is deceptively simple and compelling. The logic proceeds as follows: If law enforcement discloses information about its capabilities (including how they are used or the rules governing their use), those disclosures will increase the stock of information available to the general public, including potential criminals. People planning crimes can use such information in order to devise ways to evade law enforcement's capabilities or to navigate around their limits. The underlying normative premise is that this kind of evasion of law enforcement is always a bad thing because it makes it more difficult to prevent or solve crimes.

This logic was vividly dramatized in one particular scene of Martin Scorsese's classic mobster film *Casino*.[162] The film centers on Sam "Ace" Rothstein (played by Robert DeNiro), who has been tapped by the mob to oversee the Tangiers Casino in Las Vegas. The mob has sent in an enforcer, Nicky Santoro (played by Joe Pesci), to make sure that the casino's profits are being properly skimmed. The FBI is hot on their trail, wiretapping Ace and Nicky's calls. It is getting hard for them to communicate privately.

Ace describes the predicament in an extended voice-over: "[J]ust getting a call from Nicky wasn't easy anymore. Even the [code words] didn't work anymore. So, we figured out another act."[163]

Ace continues narrating, describing his intimate knowledge of the FBI's wiretap minimization rules: "You see, if a phone's tapped, the Feds can only listen in on the stuff involving crimes. So on routine calls, they have to click off after a few minutes."[164]

While Ace is delivering this voice-over, the audience watches Ace and Nicky's wives chat on the phone, planning a supposed shopping trip. Ace and Nicky are waiting impatiently next to them. The shot cuts to a bored FBI agent at a desk with a tape recorder, glancing at his watch. A few beats later, the agent looks at his watch again and clicks off the recording device. Immediately, Ace and Nicky grab the phones from their wives and quickly set a time to meet in the desert outside town. They hand the phones back to their wives who pick up their inane conversation. The FBI agent clicks back on to the line unaware that he just missed his targets.[165]

162. CASINO (Universal Pictures 1995), at 1:52:40.
163. *Id.*
164. *Id.*
165. *Id.*

The scene illustrates exactly what the anti-circumvention rationale is getting at. Ace and Nicky are able to evade law enforcement because they know details about how the FBI carries out its wiretaps; indeed, in this case it is the very laws that govern wiretaps that permit circumvention.[166] Because they know that the FBI has to stop wiretapping routine calls after some time, the FBI misses an important lead and the mobsters are able to meet and make plans undetected. The anti-circumvention argument says that the limits on government wiretaps should have been kept secret in order to prevent Ace and Nicky from evading the FBI.

The scene also illustrates the limitations of the anti-circumvention argument. In particular, it shows how the argument depends crucially on a number of empirical and normative claims.

First, the anti-circumvention argument depends essentially on the idea that there is a sophisticated criminal who gathers technical details about law enforcement's methods and then uses that knowledge to frustrate those methods. No doubt, sophisticated criminals like Ace and Nicky exist in real life. But certainly, they are a small minority. After all, everyone knows that police collect fingerprints at crime scenes, yet people continue to fail to wear gloves when committing crimes. It's no secret that police can track a cell phone, yet people still carry them and leave them turned on when breaking the law.

This observation is important because it highlights the extent to which the anti-circumvention argument is mostly concerned with preserving law enforcement's effectiveness at the margins, in cases involving the behavior of the most sophisticated criminal actors.[167] When we decide that the anti-circumvention rationale should prevail, it is because we are concerned about the potential effect on investigations of a small minority of crimes; in the vast

166. *See, e.g.*, 18 U.S.C. § 2518(5) (2018) ("Every [wiretap] order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter . . . ."); UNITED STATES DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL PROCEDURES AND CASE LAW FORMS 12–14 (2005) (describing minimization requirements for wiretaps) https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf [https://perma.cc/6JSU-XFCN]; *id.* at 134 ("All monitoring will cease when it is determined that the monitored conversation is not criminal in nature."). The government appears to have tried to address the circumvention risk by allowing periodic "spot checks" of minimized calls to determine whether they have turned to criminal matters. *See id.* at 134 (DOJ sample Title III roving wiretap application provides, "If an interception is minimized, monitoring agents all spot check insure that the conversation has not turned to criminal matters").

167. Moreover, for reasons discussed presently, the most sophisticated criminal actors are the ones most likely to have developed countermeasures already.

majority of cases, there will be no difference.

This dynamic also explains why law enforcement, when making the anti-circumvention argument, so often raises the specter of the sophisticated terrorist.[168] The idea of a highly destructive and sophisticated criminal puts the argument on its strongest ground. But if we adopt the anti-circumvention argument because we are concerned about the high-tech terrorist, it means we will keep the public in the dark about how the police use technology even in the vastly more numerous cases where there is no criminal mastermind or grave public safety risk. The specter of terrorism drives secrecy with respect to run-of-the-mill policing.

The scene from *Casino* also illustrates a second key empirical point: the anti-circumvention argument only works if the information that would permit countermeasures is not already in the public domain—whether or not that information came from an official source. Suppose that the FBI's minimization rules for wiretaps were not in any law, court order, or other official document. Instead, imagine that the FBI's practice of not tapping routine calls was leaked to a reporter and published in the newspaper. It wouldn't matter to Ace and Nicky where the information came from, so long as they have the information they need to evade the FBI.

The lesson here is that the anti-circumvention rationale tends to crumble once information has come into the public domain, no matter how it gets there—whether by official disclosure, unauthorized leak, or outright theft. It also matters little whether information about a law enforcement technique is widely known or only available to those who want to find it. Because the anti-circumvention rationale presupposes sophisticated criminals, even relatively obscure knowledge—say, about the wiretapping practices of the FBI or the capabilities of the backscatter x-rays used in mobile vans—is enough to render further efforts to preserve secrecy futile.

Closely related is a third empirical limit on the anti-circumvention rationale: it may be the case that some piece of information is in the public domain that already alerts sophisticated criminals to take the same evasive measures that would be suggested if the police were to disclose secret information about their technique. Take the example of Stingrays. If malefactors already know that the government can surveil the location of cell phones by obtaining the cooperation of cell phone companies, then those would-be criminals already know how to take the appropriate countermeasure—i.e., turning the cell phone off or using a burner phone. But those are the same countermeasures that a criminal would adopt if they knew

168. *See, e.g.*, Grabell v. N.Y.C. Police Dep't, 139 A.D.3d 477, 478–79 (N.Y. App. Div. 2016); Morrison Affidavit, *supra* note 13, at 1–3.

about Stingrays, which simply allow police to track cell phones without involving the cell phone company. In short, information in the public domain may already lead sophisticated criminals to take countermeasures that impede law enforcement's use of a secret technique. In such cases, secrecy serves no anti-circumvention purpose.

The anti-circumvention argument can also fail if disclosure simply does not permit the lawbreaker to learn anything that would assist him in evading law enforcement. Take the *Casino* example of FBI wiretapping again. Suppose that the FBI had rules that require it to dispose of recordings after a certain amount of time when recordings only contain benign, innocent conversations. It is hard to see how this rule could result in circumvention. Unlike the rules about switching off the wiretap that Ace and Nicky exploited, rules about record retention periods do not seem to create any risk of circumvention. The lesson here is that one cannot simply *assume* that disclosure of any and all information about law enforcement's capabilities and techniques will give rise to a threat of circumvention. The case needs to be made that disclosure will be useful to evade police.

Finally, the anti-circumvention argument can fail if the disclosure in question leaves uncertainty about how police will use the technique—and, therefore, how it could be circumvented. Ace and Nicky were able to exploit the FBI's minimization rules either because they knew precisely how much time the FBI agent could listen in before clicking off the call or because they could actually hear the FBI agent disconnecting the wiretap. The FBI could have mitigated the risk of circumvention by tweaking the technology or the rules in question. If the minimization rules prescribed no specific period of time before the wiretap was disconnected (or if the rules permitted random spot checks)[169] and if the wiretap device was completely silent, then there would have been no ready way for Ace and Nicky to evade the FBI. They would have used the phone at their peril, uncertain whether or not the FBI was in fact taping them. The example may generalize; in some cases, the nature of the technology or the rules in question can be difficult to circumvent because they are not sufficiently predictable or detectable.

So much for the empirical premises of the anti-circumvention argument; what about its normative underpinnings? On first blush, they seem unassailable: who in their right mind would want would-be lawbreakers to be able to evade law enforcement? If, as an empirical matter, disclosure would actually permit evasion of law enforcement, then surely it follows uncontroversially that we should oppose disclosure. There are at least two responses—one complicates the normative premise, and the other points out

169. As, indeed, DOJ guidelines currently allow. *See supra* note 166.

that competing normative commitments may swamp concerns to prevent circumvention.

First, there may well be circumstances where we actually do want to allow or even encourage evasion. The idea is that by allowing would-be lawbreakers to evade particular law enforcement techniques, we might channel them into less socially destructive behavior. Imagine, for example, that a city has outfitted its downtown area with technologically sophisticated surveillance cameras, automated license plate readers, perhaps also exotic chemical sensors, listening devices, and the like. Disclosing the capabilities of these devices might allow sophisticated lawbreakers to evade detection by these devices. The standard normative premise is that such evasion is a bad thing, so we should keep the capabilities of the devices secret. But the opposite normative premise may be more compelling: we may want people to know that law enforcement is watching in order to deter certain kinds of crimes or to displace crimes from a certain location.[170]

Along similar lines, let's return to the story of Ace and Nicky. Because they knew the FBI's minimization procedures, they were able to evade the wiretap. But the wiretap nevertheless made it much harder for them to communicate, materially impeding their ability to conspire and giving the police other opportunities to surveil them. Ace and Nicky were forced to undertake elaborate measures in order to speak. Because they could not use the phone for any length of time without being wiretapped, they had to meet in person.[171] In order to do so, they had to try to evade physical surveillance, switching cars multiple times in order to shake the FBI.[172] They could only meet and speak undisturbed in exposed, dusty patches of desert outside town in order to avoid

170. There is mixed evidence about whether surveillance cameras have a deterrent effect on crime. Some studies have found a meaningful deterrent effect while others have not. The evidence is similarly mixed on the question of whether surveillance cameras serve merely to displace crime to unsurveilled locations. *See, e.g.*, Eric L. Piza et al., *Analyzing the Influence of Micro-Level Factors on CCTV Camera Effect*, 30 J. QUANTITATIVE CRIMINOLOGY 237, 238–42 (2013) (reviewing the empirical literature on the deterrent effect of surveillance cameras and concluding that the evidence is mixed); Mikael Priks, *The Effects of Surveillance Cameras on Crime: Evidence from the Stockholm Subway*, 125 ECON. J. 289–91 (2015) (finding that surveillance cameras in subway stations deterred certain pre-planned crimes like pickpocketing, but tended to displace such crime to the immediate vicinity—e.g., outside subway entrances—beyond the view of the surveillance cameras); Joel M. Caplan et al., *Police-Monitored CCTV Cameras in Newark, NJ: A Quasi-Experimental Test of Crime Deterrence*, 7 J. EXPERIMENTAL CRIMINOLOGY 255, 264–71 (2011) (finding reductions in certain crimes in areas within the field-of-view of particular cameras, and finding no evidence that cameras served to displace the location of crimes).

171. *See* CASINO, *supra* note 162, at 1:52:40.

172. *Id.*

the possibility of physical or electronic surveillance.[173] In short, disclosing wiretap rules succeeded in putting the heat on Ace and Nicky, impairing their ability to make plans, even if it didn't succeed in intercepting every conversation.[174]

This approach to policing is a kind of harm-reduction strategy. Police encourage or at least tolerate evasion of law enforcement in order to diminish opportunities for crime or to channel crime in less damaging directions. This approach may have much to say for it. Rather than requiring secrecy, it requires the opposite; the would-be criminal must know that law enforcement may be deploying a certain technique. As a result, it is not fair to assume that in every case evasion of law enforcement techniques will always be a bad thing, or that disclosure will always impair law enforcement objectives.[175]

Second, even when we do actually want to prevent sophisticated criminals from evading law enforcement, we will often simultaneously hold competing normative commitments that move us to oppose secrecy. These competing values were explored in the prior Part: We want our law enforcement agencies to be amenable to democratic oversight and deliberation. We want courts, legislatures, and citizens to vet law enforcement techniques for compliance with the Constitution and other laws. We want to avoid circumstances where abuses proliferate in secret. We want law enforcement to be governed by laws and rules that are public. We want law enforcement to have the benefit of outside input and expert criticism. We want police to maintain trust and credibility with the people they serve. Secrecy impairs these goals. The decision to endorse anti-circumvention thus has major costs.

The upshot is that even if the anti-circumvention argument is sound and empirically justified, it is not conclusive. The decision whether to keep a law enforcement technique secret necessarily involves a value judgment—implicit

173. *Id.*

174. *Id.* ("Ace: The problem was, Nicky was not only bringin' heat on himself, but on me too. The FBI watched every move he made. But he didn't care. He just didn't care.").

175. In one interesting recent example, the New York Police Department threatened to bring legal action against Waze, a mapping app that crowdsources information from users, because the app allowed users to notify fellow drivers about the location of police drunk-driving checkpoints. NYPD argued that the app was allowing drivers to evade checkpoints and thereby impairing law enforcement. *See* Michael Gold, *Google and Waze Must Stop Sharing Drunken-Driving Checkpoints, New York Police Demand*, N.Y. TIMES (Feb. 6, 2019), https://www.nytimes.com/2019/02/06/nyregion/waze-nypd-location.html [https://perma.cc/YB59-VYNH]. Critics, however, pointed out that police checkpoints are more effective at deterring drunk driving if they are visible and public; the app might actually be *amplifying* the police's intended deterrent effect by making checkpoints more public. *See* Hannah Bloch-Wehba, *The NYPD's Misguided War on Waze*, SLATE (Feb. 13, 2019), https://slate.com/technology/2019/02/nypd-waze-dwi-checkpoints-lawsuit-first-amendment.html [https://perma.cc/FL8X-93AC].

or explicit—that anti-evasion concerns are weightier than the rest.

There is good reason to believe that most people do not assign normative priority to anti-circumvention concerns. Consider again Ace and Nicky: a world in which they did not know that the FBI's minimization rules required agents to stop listening to innocent telephone conversations would be a world in which the public was kept in the dark about the scope of the FBI's wiretap powers. In a very real sense, this would be a world of secret law; the rules governing the FBI's conduct would be hidden from the public. The public would not be able to know whether police could lawfully use a wiretap to intercept perfectly innocent conversations. Indeed, the public could not enact public rules to this effect because to do so would tip off mobsters. Of course, few people would be willing to endorse that kind of secrecy. We are simply not willing to accept that wiretapping should be governed by secret law in order to increase the effectiveness of the technique at the margins. To the contrary, we expect law enforcement to absorb any burdens on its investigatory capacity as a basic cost of democracy and rule of law.

Taking the contrary view—i.e., that anti-circumvention concerns generally outweigh competing values—leads to alarming conclusions. If our overriding concern were to prevent circumvention, then we would presumably think it justified to keep a good deal of Fourth Amendment law secret. After all, the Fourth Amendment imposes intricate limits on the police's ability to carry out various techniques. Sophisticated knowledge of Fourth Amendment rules may well allow a person to evade detection. For example, knowing that police cannot search inside a car's glovebox in the absence of consent or probable cause[176] may well allow an individual to avoid an arrest for drug possession. We do not typically lament this consequence. Instead, we accept it as a cost of the rule of law.

A thought experiment further illustrates the point. Imagine a world in which law enforcement has managed to keep *all* of its capabilities and techniques secret. The public does not know about how police can use fingerprints; it does not know about DNA testing; it does not know about wiretaps, etc. In that world, the would-be lawbreaker has no information that would allow him to evade law enforcement. If all we cared about was preventing such evasion, then we would presumably be comfortable with that state of affairs. But I think most of us recoil at the thought of living in a society

176. *See* Carroll v. United States, 267 U.S. 132, 153–54 (1925); California v. Acevedo, 500 U.S. 565, 580 (1991); Evan Levtow, *Locked Glove Compartments: Searchable or Stash Spots?*, 29 TOURO L. REV. 1115 (2013); John P. Besselman, *Locked Containers - An Overview*, FED. L. ENFORCEMENT TRAINING CTR., https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/4th-amendment/lockedcontainers.pdf [https://perma.cc/GF25-RV7J].

like that—one in which we are not allowed to know how the authorities can investigate any of us, lest some of us attempt to evade them.

Of course, in the real world, the public already knows a great deal about law enforcement's methods, and that knowledge cannot be erased from memory. But the question that arises—and the one that this Article grapples with—is how much we should be able to learn about *new* technologies, particularly technologies that can be deployed surreptitiously without revealing themselves to the target. If we would reject a world in which information about existing law enforcement techniques is secret, why do we accept a world in which information about new technologies can remain secret? A desire to prevent evasion of law enforcement does not alone answer the question. Answering in favor of secrecy implies a judgment that the anti-circumvention concern outweighs other considerations including, often, basic commitments to democratic accountability and rule-based governance.

V. ANTI-CIRCUMVENTION DOCTRINES

I now turn away from a theoretical exploration of the anti-circumvention argument in order to explore how the law actually protects the secrecy of law enforcement techniques. The principal sources of law in this area at the federal level are Exemption 7(E) of FOIA and the law enforcement evidentiary privilege.

A. THE FOIA EXEMPTION FOR LAW ENFORCEMENT "TECHNIQUES AND PROCEDURES"

FOIA imposes a presumptive requirement on the government to disclose any records in its possession upon request, including in theory records that might disclose law enforcement capabilities or techniques.[177] Of course, this disclosure mandate is not absolute; FOIA contains exemptions.[178] Key among these is the law enforcement exemption.[179] In particular, Exemption 7(E) permits federal agencies to withhold

> records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk

177. *See* 5 U.S.C. § 552(a)(3)(A) (2018).
178. § 552(b).
179. § 552(b)(7).

circumvention of the law.[180]

The scope of this exemption determines, to a great extent, how much official information the public can obtain about the capabilities of law enforcement technologies and how they are used. Exemption 7(E) is therefore worth examining in some detail.

Exemption 7(E) has been on the books in its current form since 1986,[181] and it is frequently litigated. The case law interpreting the Exemption has given it a fairly broad scope. Courts have found that a wide range of information constitutes "techniques and procedures" or "guidelines" within the meaning of the exemption.[182] Importantly, courts have permitted secrecy upon a modest showing that disclosure of a technique risks circumvention of law.

The D.C. Circuit, for example, has explicitly rejected the argument that the agency "has a high burden to specifically prove how the law will be circumvented."[183] Instead, that court determined that "exemption 7(E) only requires that the [agency] demonstrate logically how the release of the requested information might create a risk of circumvention of the law."[184] On this view, secrecy is justified if the agency is merely able to tell a coherent story about how circumvention "might" result. It is not a particularly high bar and, unsurprisingly, it permits a great deal of secrecy about novel technologies.[185]

Some circuits have required even less. The Second and Ninth Circuits have taken the position that when it comes to information about "techniques and procedures," no showing of risk of circumvention is required at all.[186] These

180. *Id.*; § 552(b)(7)(E).

181. The anti-circumvention rationale is also codified in the privilege for law enforcement investigative techniques, which has been recognized so far by a several circuit. *See* Smith, *supra* note 28, at 258–69 (detailing the development and present state of the law). In this Article, I focus solely on the FOIA exemption; future articles may include discussion of the privilege, as relevant.

182. *See, e.g.*, Blackwell v. FBI, 646 F.3d 37, 42 (D.C. Cir. 2011) (forensic computer examination methods); Hale v. Dep't of Justice, 973 F.2d 894, 902–03 (10th Cir. 1992), *cert. granted, vacated & remanded on other grounds*, 509 U.S. 918 (1993) (information about polygraph examinations); Sheridan v. U.S. Office of Pers. Mgmt., 278 F. Supp. 3d 11, 21 (D.D.C. 2017) (source code and design manual for receiving and vetting security clearance forms); Showing Animals Respect & Kindness v. U.S. Dep't of Interior, 730 F. Supp. 2d 180, 199–200 (D.D.C. 2010) (surveillance methods at wildlife refuge); Mayer Brown LLP v. Internal Revenue Serv., 562 F.3d 1190, 1192–93 (D.C. Cir. 2009) (settlement guidelines for tax audits).

183. *Mayer Brown*, 562 F.3d at 1194.

184. *Id.* (internal quotation and alterations omitted).

185. *See, e.g.*, Soghoian v. U.S. Dep't of Justice, 885 F. Supp. 2d 62, 74–75 (D.D.C. 2012) (determining that information about Stingrays was exempt under Exemption 7(E)).

186. *See* Allard K. Lowenstein Int'l Human Rights Project v. Dep't of Homeland Sec., 626 F.3d 678, 681–82 (2d Cir. 2010); Hamdan v. U.S. Dep't of Justice, 797 F.3d 759, 778 (9th Cir. 2015).

courts have read the language in the exemption regarding the risk of circumvention to apply only to "*guidelines* for law enforcement investigations or prosecutions" and not to the earlier part of the exemption which covers "*techniques and procedures* for law enforcement investigations or prosecutions."[187] The Second Circuit further clarified that "guidelines" in this context refers to "an indication or outline of future policy or conduct" and, specifically, "resource allocation" decisions about how to focus enforcement efforts.[188] "Techniques and procedures," on the other hand, "refers to how law enforcement officials go about investigating a crime."[189] Information about the existence and capabilities of law enforcement technologies may often fall in the latter category. Thus, on the Second Circuit's view, police may be able to withhold information even if there is no plausible risk of circumvention at all.[190]

The only consistent limit that the courts have recognized on the scope of Exemption 7(E) is that it "only exempts investigative techniques not generally known to the public."[191] In other words, information cannot be withheld if a technique is already public. The scope of this limitation, however, is contested

187. *Hamdan*, 797 F.3d at 777–78; *Sheridan*, 278 F. Supp. 3d at 22 (noting disagreement among courts about "whether the 'risk of circumvention' requirement applies to records containing 'techniques and procedures' or only to records containing 'guidelines' "); Pub. Emps. for Envtl. Responsibility v. U.S. Section, Int'l Boundary & Water Comm'n, U.S.-Mex., 740 F.3d 195, 204 n.4 (D.C. Cir. 2014) (same).

188. Allard K. Lowenstein Int'l Human Rights Project, 626 F.3d at 682.

189. *Id.*

190. *Id.* at 681–82. As the D.C. Circuit has noted, however, "given the low bar posed by the 'risk circumvention of the law' requirement, it is not clear that the difference matters much in practice." *Pub. Emps. for Envtl. Responsibility*, 740 F.3d at 204 n.4. It is possible that the Second Circuit's interpretation will be reconsidered in light of recent amendments to FOIA that now permit agencies to withhold information "only if the agency reasonably foresees that disclosure would harm an interest protected by an exemption." FOIA Improvement Act of 2016, Pub. L. No. 114-185, § 2, 130 Stat. 538, 539 (2016) (codified at 5 U.S.C. § 552(a)(8)(A)(i) (2018)). Lower courts are interpreting this amendment to require agencies to identify some *harm* in order to successfully invoke exemptions. *See* Rosenberg v. U.S. Dep't of Def., 342 F. Supp. 3d 62, 77–79 (D.D.C. 2018) (holding that the new foreseeable harm standard imposes an additional burden on the government to justify withholding); Judicial Watch v. U.S. Dep't of Commerce, 375 F. Supp. 3d 93, 100 (D.D.C. 2019) (same). The Second Circuit's categorical approach to excluding "techniques and procedures" irrespective of any risk of circumvention or other articulated harm would probably not survive such an interpretation of the amendment. To date, however, no court has yet considered how amendment interacts with Exemption 7(E).

191. *See* Rosenfeld v. U.S. Dep't of Justice, 57 F.3d 803, 815 (9th Cir. 1995); *accord* Rugiero v. U.S. Dep't of Justice, 257 F.3d 534, 551 (6th Cir. 2001); Davin v. U.S. Dep't of Justice, 60 F.3d 1043, 1064 (3d Cir. 1995); Albuquerque Pub. Co. v. U.S. Dep't of Justice, 726 F. Supp. 851, 857–58 (D.D.C. 1989); Malloy v. U.S. Dep't of Justice, 457 F. Supp. 543, 545 (D.D.C. 1978).

and applied inconsistently by the courts. It generally imposes only a weak constraint because the test only regards "generally known" information as sufficient to overcome secrecy. As a result, the most well-known and obvious techniques are more likely to fall outside Exemption 7(E),[192] while courts are less likely to order disclosure with respect to novel law enforcement technologies at least until significant information about the technique has become public.[193] Indeed, courts have held that law enforcement can withhold even information about well-known techniques if the government contends that disclosure might risk circumvention.[194] In other words, the courts will rarely crack open a window on a police technique much wider than the window has already been opened by other forces.

Cases applying these standards demonstrate significant mismatches between Exemption 7(E) doctrine and the more rigorous explication of the logic of anti-circumvention offered in the prior Part.

For starters, the law does not typically require a strong explanation of the link between disclosure of the information at issue and the potential for circumvention. Where courts demand such an explanation, they only require a "logical" link between disclosure and circumvention.[195] To be sure, some courts have gone out of their way to take a close look at whether disclosure of particular details is likely to risk circumvention.[196] But in many instances, law

192. *See, e.g.*, *Rosenfeld*, 57 F.3d at 815 (holding that the technique of using pretext phone calls was sufficiently well known that it could not be withheld under Exemption 7(E)); *Davin*, 60 F.3d at 1064 ("This exemption . . . may not be asserted to withhold routine techniques and procedures already well-known to the public, such as ballistic tests, fingerprinting, and other scientific tests commonly known.") (internal quotation omitted); *Albuquerque Pub. Co.*, 726 F. Supp. at 857–58 ("[T]he government should avoid burdening the Court with an in-camera inspection of information pertaining to techniques that are commonly described or depicted in movies, popular novels, stories or magazines, or on television. These would include, it would seem to us, techniques such as eavesdropping, wiretapping, and surreptitious tape recording and photographing. Instead, the government should release such information to plaintiff voluntarily.").

193. *See Soghoian*, 885 F. Supp. 2d at 74–75 (refusing to disclose any records regarding Stingrays in 2012). *But see* ACLU of N. Cal. v. Dep't of Justice, 880 F.3d 473, 491–92 (9th Cir. 2018) (finding in 2018 that cell phone tracking technology was sufficiently well-known that certain records about Stingrays could not be withheld).

194. *See, e.g.*, Unidad Latina en Accion v. U.S. Dep't of Homeland Sec., 253 F.R.D. 44, 53–54 (D. Conn. 2008) (weekly immigration arrest reports could be withheld under Exemption 7(E)); Piper v. U.S. Dep't of Justice, 294 F. Supp. 2d 16, 30 (D.D.C. 2003) (finding documents that would disclose unspecified "logistical considerations" regarding polygraph tests could be withheld even though polygraphy is a well-known technique).

195. N.Y. Times v. U.S. Dep't of Justice, 101 F. Supp. 3d 310, 319 (S.D.N.Y. 2015) (quoting Blackwell v. FBI, 646 F.3d 37, 40 (D.C. Cir. 2011)).

196. *See, e.g.*, Allard K. Lowenstein Int'l Human Rights Project v. U.S. Dep't of Homeland Sec., 603 F. Supp. 2d 354, 354–55 (D. Conn. 2009), *aff'd*, 626 F.3d 678 (2d Cir. 2010); ACLU

enforcement can withhold information about "techniques and procedures" without showing any risk of circumvention at all.[197]

The case law generally also takes a crude approach to assessing the effect of existing public-domain information that may render the risk of circumvention illusory. Rather than taking seriously the notion that secrecy may be futile because existing public-domain information already creates identical risks of circumvention, the case law takes the opposite tack: only if a technique is so well known and well publicized that it is common knowledge will secrecy be inappropriate.[198]

Similarly, courts rarely take serious account of the likelihood that disclosure would allow criminals to develop genuinely new countermeasures. It is an unusual case where the court actually identifies potential countermeasures and considers whether such countermeasures would already be obvious based on existing publicly available information.[199]

Courts also lack a nuanced approach to the probabilistic nature of alleged risks of circumvention. Whether disclosure will in fact encourage circumvention is rarely a certainty and usually a matter of conjecture. Rather than weighing the seriousness of the risk against countervailing concerns, courts adjudicating Exemption 7(E) claims simply end the inquiry once they have determined that there is some unspecified (and usually very small) probability of circumvention. There is no balance of the risks and rewards of disclosure.[200]

Perhaps most fundamentally, the existing case law fails to engage with the crosscutting value judgments implicated in secrecy determinations. There is no public interest "override." The only value the exemption explicitly recognizes is law enforcement's interest in confidentiality. The doctrine has no clear space for the weighty concerns about democratic accountability, separation of powers, or rule-based governance.[201] Those values, which otherwise animate FOIA, are often submerged in favor of the anti-circumvention rationale.[202] In

---

of N. Cal. v. Dep't of Justice, 70 F. Supp. 3d 1018, 1036–39 (N.D. Cal. 2014), *aff'd*, 880 F.3d at 492.

197. *See supra* notes 186–190 and accompanying text.

198. *See supra* note 192 (collecting illustrative cases).

199. One outlier in this regard is Northern District of California's decision rejecting the DOJ's argument for withholding information about Stingrays, affirmed in relevant part by the Ninth Circuit. *See ACLU of N. Cal.*, 70 F. Supp. 3d at 1038.

200. *See supra* notes 182–183, 185, 192 (identifying illustrative cases).

201. *See supra* Sections III.A–D.

202. Indeed, in jurisdictions that do not require the government to show a risk of circumvention in order to keep techniques secret, there is not even a clear rationale for disregarding countervailing values: law enforcement gets to keep its techniques secret, whether

perhaps the starkest example of this problem, some courts have allowed the government to withhold records under Exemption 7(E) even if those records constitute the internal law that governs how an agency will operate.[203] Thus, even the public interest in not having secret law has sometimes not been enough to defeat the anti-circumvention argument.[204]

The only true safety valve in the existing case law is the exception for information that is already in the public domain. But this is a crude and somewhat mystifying way of demarcating a line between proper and improper secrets. Whether or not some technique has entered popular culture and become widely familiar does not track whether sophisticated criminals will be able to exploit disclosures to evade detection. It also does not reflect the normative sacrifices involved in permitting secrecy. Just because something is not common knowledge does not mean it should remain secret. To return to a concrete example, the question of whether we should keep x-ray vans secret does not depend, as a normative matter, on the fact that NYPD has been very effective at hiding information about the vans. It depends instead on value judgments about democratic oversight and legal regulation of the public health and privacy issues that the technique implicates. Those concerns have little place in the current legal regime.[205] Instead, by giving law enforcement the

---

or not disclosure would plausibly impair law enforcement's efforts. *See supra* notes 186–190 and accompanying text.

203. *See, e.g.*, ACLU v. U.S. Dep't of Justice, No. 12 CIV. 7412 WHP, 2014 WL 956303, at *1, *8 (S.D.N.Y. Mar. 11, 2014) (holding that government could withhold legal memorandum describing the parameters within which FBI could use unspecified location-tracking techniques even though the memorandum contained "the Government's interpretation of its constitutional obligations" with respect to such techniques); N.Y. Times v. U.S. Dep't of Justice, 101 F. Supp. 3d 310, 322 (S.D.N.Y. 2015) (holding that federal law enforcement agency could withhold emails describing "specific factual scenarios and . . . technical aspects of GPS tracking devices" even though it contained guidance governing use of such devices, which were already publicly known, because release would create unspecified "risk of a circumvention of the law"). *But see* ACLU of N. Cal., 880 F.3d at 492 (finding that Exemption 7(E) did not bar disclosure of documents that "describe the legal authorization necessary for obtaining location information, and describe legal arguments related to that acquisition").

204. *See* Manes, *supra* note 22, at 851–54.

205. Perhaps as a result of this doctrinal paradox, advocates seeking to shine a light on novel police technologies have mounted multi-pronged transparency campaigns in an effort to force disclosure of information. Such campaigns typically involve publicizing whatever information has managed to find its way into the public domain, publishing reports and articles about the technique in question, publicizing any discoveries and disclosures to the press to raise the profile of the issue, raising concerns in Congress, and generally sounding the alarm. Such publicity campaigns may ultimately shift perceptions to a sufficient degree that courts are willing to reject claims that disclosure will reveal a secret technique. *Compare* Soghoian v. U.S. Dep't of Justice, 885 F. Supp. 2d 62, 74–75 (D.D.C. 2012) (refusing disclosure about Stingrays) *with ACLU of N. Cal.*, 880 F.3d at 492 (rejecting arguments against disclosure).

authority to keep techniques secret so long as they remain out of the public eye, the legal regime strongly incentivizes law enforcement to do everything it can to keep its technologies under wraps for as long as possible. In this way, it gives law enforcement significant power to decide when and how to disclose information about the capabilities it possesses and how they are used.

B. THE EVIDENTIARY PRIVILEGE FOR LAW ENFORCEMENT INVESTIGATIVE TECHNIQUES

Historically, law enforcement did not enjoy any evidentiary privilege protecting information about its techniques.[206] Since 1977, however, four federal circuit courts have squarely recognized a common law privilege that covers law enforcement techniques, and many district courts in other circuits have followed suit.[207] In some of these jurisdictions, the privilege for law enforcement techniques is one component of a broader "law enforcement privilege" that, depending on the jurisdiction, serves to protect not just techniques but also investigatory files,[208] "the identity of informer[s],"[209] "witness and law enforcement personnel," "the privacy of individuals involved in an investigation," and "interference with an investigation."[210] The courts have recognized these privileges in an exercise of their common law authority pursuant to Federal Rule of Evidence 501.

The appellate authorities do not elaborate in great detail on the scope of the privilege for law enforcement techniques but suggest that its sweep is similar to that of FOIA Exemption 7(E). Indeed, a number of the decisions explicitly analogize the evidentiary privilege to Exemption 7(E), even while recognizing that the considerations at stake in the FOIA, which is concerned with policing the line between secrecy and disclosure to the general public, are different and less acute than those at stake with the privilege, which can prevent defendants in criminal cases from obtaining evidence for use in their

206. *See* Smith, *supra* note 28, at 233–34.

207. *See* United States v. Pirosko, 787 F.3d 358, 365–67 (6th Cir. 2015) (applying qualified "law enforcement privilege" to law enforcement technique); *In re* Dep't of Investigation of N.Y., 856 F.2d 481, 483–84 (2d Cir. 1988) (recognizing "law enforcement privilege" the purpose of which is "to prevent disclosure of law enforcement techniques and procedures"); United States v. Cintolo, 818 F.2d 980, 1001–03 (1st Cir. 1987) (holding that qualified privilege protects "nature and location of electronic surveillance equipment"); United States v. Van Horn, 789 F.2d 1492, 1507–08 (11th Cir. 1986) (same); Black v. Sheraton Corp. of Am., 564 F.2d 550, 541–47 (D.C. Cir. 1977) (recognizing "law enforcement evidentiary privilege" against "disclosure of documents that would tend to reveal law enforcement investigative techniques or sources").

208. *See, e.g.*, Dellwood Farms v. Cargill, Inc., 128 F.3d 1122, 1125–28 (7th Cir. 1997).

209. *See, e.g.*, Roviaro v. United States, 353 U.S. 53, 60, 66–67 (1957).

210. *See, e.g.*, *In re Dep't of Investigation of N.Y.*, 856 F.2d at 484.

defense.[211]

The Eleventh Circuit has explained the basis for the privilege in perhaps the most explicit terms. In *United States v. Van Horn*, a criminal defendant sought disclosure of information about what type of microphone was used to surveil him and where the microphone had been hidden in a particular room.[212] The case was decided in 1986, at a time when hidden microphones or "bugs" were already well known. Nevertheless, the court held that "the privilege applies equally to the nature and location of electronic surveillance equipment,"[213] on the reasoning that

> [d]isclosing the precise locations where surveillance devices are hidden or their precise specifications will educate criminals regarding how to protect themselves against police surveillance. Electronic surveillance is an important tool of law enforcement, and its effectiveness should not be unnecessarily compromised. Disclosure of such information will also educate persons on how to employ such techniques themselves, in violation of Title III.[214]

The court's reasoning rested entirely on these generalized concerns. It did not provide (or, it appears, demand) any particularized explanation about how disclosure of details about the hidden microphone in question could compromise the effectiveness thereof in a future investigation. It also did not consider whether disclosure would have created any meaningful additional risk of evasion in light of information already in the public domain.[215]

Subsequent decisions in the lower courts apply the privilege broadly to prohibit disclosure of information about all manner of technology, even techniques that are decades old and well known to anyone who has ever watched a police procedural. Thus, courts have withheld information about pen registers,[216] hidden sound and video recording devices,[217] and polygraph

211. *See, e.g.*, *Black*, 564 F.2d at 545–46.

212. *Van Horn*, 789 F.2d at 1507.

213. *Id.* at 1508.

214. *Id.*

215. *See id.*

216. United States v. Garey, No. 5:03-CR-83, 2004 WL 2663023, at *1 (M.D. Ga. Nov. 15, 2004) (privilege covered information about "the nature and details pertaining to the use of the pen register and trap and trace devices").

217. United States v. Alimehmeti, 284 F. Supp. 3d 477, 493 (S.D.N.Y. 2018) (privilege covered "methodology used to facilitate recordings" between undercover officer and suspect); United States v. Djokich, No. CR 08-10346-MLW, 2016 WL 927145, at *5 (D. Mass. Mar. 7, 2016) (privilege covered specific "types of computers, recording devices, and software used by the government" to record telephone conversations); United States v. Farha, No. 8:11-CR-115-T-30MAP, 2012 WL 12964913, at *2–3 (M.D. Fla. Sept. 27, 2012) (privilege likely applies to "the device or devices . . . used in making . . . recordings [of defendant]; the operating

examinations.[218] The privilege has also been successfully invoked to prevent disclosure of information about newer technology including Stingrays[219] and various forms of surveillance software.[220]

In these cases, courts often require little if any demonstration that disclosure of the information sought would create a significant risk of circumvention. In many cases, it is enough simply that the material in question pertains to a law enforcement technique.[221] Similarly, courts rarely inquire whether the technique in question is already well known to the public, or whether information in the public domain already creates the risk of circumvention that the government seeks to avoid.[222] In fact, in one recent case concerning Stingrays, a court found that the privilege prohibited disclosure even while it acknowledged elsewhere in its opinion that the criminal defendant had amassed a treasure trove of detail from public sources regarding the operation of the device.[223] In this respect, the privilege often

manual for these devices including their spec sheets; the batteries" and related equipment); United States v. Little, No. 09-20673-CR, 2010 WL 11570441, at *2–3 (S.D. Fla. Jan. 21, 2010) (privilege covered "inspection of the recording device" used to record defendant); United States v. O'Neill, 52 F. Supp. 2d 954, 963 (E.D. Wis. 1999), *aff'd sub nom.* United States v. Warneke, 199 F.3d 906 (7th Cir. 1999) ("recording and monitoring equipment used to transmit and record [defendant]").

218. Shah v. Dep't of Justice, No. 15-15232, 2017 WL 4812585, at *1 (9th Cir. Oct. 25, 2017) (privilege covered "charts, graphs, and raw data associated with [polygraph] examination" of criminal defendant).

219. United States v. Rigmaiden, 844 F. Supp. 2d 982, 1002 (D. Ariz. 2012) (information about cell-site simulator was held to be privileged).

220. United States v. Matish, 193 F. Supp. 3d 585, 592 (E.D. Va. 2016) (privilege encompasses source code for "network investigative technique" that allowed government to identify a person's computer and location); United States v. Pirosko, 787 F.3d 358, 365 (6th Cir. 2015) (privilege applied to law enforcement software used to investigate illegal file-sharing); United States v. Hoeffener, No. 4:16CR00374 JAR/PLC, 2017 WL 3676141, at *18 (E.D. Mo. Aug. 25, 2017) (privilege covered source code, manuals, and other information regarding software used to conduct investigations on the BitTorrent file-sharing network).

221. *See, e.g.*, *Shah*, 2017 WL 4812585, at *1; *Little*, 2010 WL 11570441, at *2–3; *Garey*, 2004 WL 2663023, at *4. *But see* United States v. Taylor, No. 3:14-00015, 2015 WL 9274934, at *3 (M.D. Tenn. Dec. 18, 2015) (expressing skepticism that information about a GPS tracking device fell within scope of privilege because of the familiarity of the technology and technique involved); Ibrahim v. Dep't of Homeland Sec., No. C 06-00545 WHA, 2013 WL 1703367, at *5 (N.D. Cal. Apr. 19, 2013) ("screening procedures and requirements for being placed on the No-Fly and other watch lists" could be disclosed, despite claim of privilege, pursuant to an "attorney's eyes only" protective order limiting further dissemination).

222. *See, e.g.*, *Matish*, 193 F. Supp. 3d at 601; *Shah*, 2017 WL 4812585, at *1; *Djokich*, 2016 WL 927145, at *5; *Farha*, 2012 WL 12964913, at *2–3; *Little*, 2010 WL 11570441, at *2; *Garey*, 2004 WL 2663023, at *4.

223. *Rigmaiden*, 844 F. Supp. 2d at 999 (noting that defendants' "filings contain extensive technical data regarding cell tower simulation technology [including] product brochures,

mirrors the broadest version of Exemption 7(E), which requires no showing of circumvention risk at all.[224]

Unlike in the FOIA context, however, the evidentiary privilege for law enforcement techniques is not an absolute bar to disclosure but is instead subject to a balancing test that weighs "[t]he public interest in nondisclosure . . . against the need of a particular litigant for access to the privileged information."[225] If a criminal defendant or civil plaintiff can make a strong showing of need, the privilege may be overcome. Courts have established various tests in the civil[226] and criminal[227] contexts to determine whether disclosure is required despite a claim of privilege. In general, however, the privilege will be overcome only upon a showing that evidence is necessary or important to a party's case and that there are no alternative means for the party to make the relevant point or argument.[228]

In principle, the possibility of overcoming a claim of privilege could allay some of the concerns about secrecy that were canvassed above. But, in practice, this safety valve is often stuck closed. Courts have placed a heavy burden on criminal defendants to identify in advance particular arguments they wish to make and to demonstrate that, without disclosure, they would not be able to make them.[229] It is difficult, however, to know in advance which secret facts might support a compelling constitutional or statutory argument. A technology may operate in ways that are opaque to the defendant and yet deeply constitutionally suspect. Moreover, even where it appears that a party will be able to make the requisite showing of need and lack of alternative means, the government can avoid disclosure (and subsequent litigation) by making narrow strategic concessions that obviate the need for disclosure.[230]

---

patent applications, articles, websites, and textbooks [that] show the manner in which cell tower emulation occurs").

224. *See supra* note 186 and accompanying text.

225. *In re* City of New York, 607 F.3d 923, 945 (2d Cir. 2010) (quoting *In re* Sealed Case, 856 F.2d 268, 272 (D.C. Cir. 1988)).

226. *See, e.g.*, *id.* at 945 (party seeking disclosure "must show (1) that its suit is non-frivolous and brought in good faith, (2) that the information sought is [not] available through other discovery or from other sources, and (3) that the information sought is important to the party's case") (internal quotation and alteration omitted).

227. *See, e.g.*, United States v. Cintolo, 818 F.2d 980, 1002 (1st Cir. 1987) (criminal defendant must make "a sufficient showing of need," which "requires a case by case balancing process controlled by the fundamental requirements of fairness") (internal quotations and citations omitted).

228. *See generally* United States v. Alimehmeti, 284 F. Supp. 3d 477, 493–94 (S.D.N.Y. 2018) (synthesizing common elements of tests for overcoming privilege).

229. *See, e.g.*, United States v. Little, No. 09-20673-CR, 2010 WL 11570441, at *2 (S.D. Fla. Jan. 21, 2010); *Alimehmeti* 284 F. Supp. at 494.

230. *See infra* notes 232–236 and accompanying text (discussing *Rigmaiden*, 844 F. Supp. 2d at 982).

Perhaps as a result, there are few reported decisions in which a party succeeded in overcoming the government's claim of privilege.[231]

These concerns were highlighted most vividly in the high-profile case of Daniel Rigmaiden, a criminal defendant charged with making numerous fraudulent tax filings. Rigmaiden managed to piece together evidence strongly suggesting that the government had discovered his location using a Stingray device.[232] Rigmaiden sought discovery of information about the Stingray technology and how it was used. He intended to use that information in support of a suppression motion, which would have tested whether using a Stingray requires a warrant and whether the police's use in his case had exceeded the scope of the judicial authorization they had actually obtained.[233] The case promised to be the first time the federal government would face a Fourth Amendment challenge to its use of a Stingray device.

Ultimately, however, the court held that even Rigmaiden could not demonstrate sufficient "need" to displace the law enforcement privilege, in large part because the government made a number of strategic concessions in order to avoid disclosure.[234] Among other things, the government conceded, solely for purposes of that case, that its investigative actions had constituted a "search" for purposes of the Fourth Amendment; it also conceded certain specific details about how Rigmaiden alleged the device had been used.[235] Having made those concessions, Rigmaiden's "need" for information about the capabilities and deployment of the government's Stingray technology evaporated. By making these strategic concessions, the government avoided any actual disclosures about its capabilities and evaded any judicial

231. *See, e.g.*, State v. Harris, 819 So. 2d 844, 846 (Fla. Dist. Ct. App. 2002) (location from which police surveilled suspect was not privilege because the officer's testimony on the matter was essential to the defense and there was no videotape of the surveillance); United States v. Foster, 986 F.2d 541, 543–44 (D.C. Cir. 1993) (same); United States v. Taylor, No. 3:14-00015, 2015 WL 9274934, at *4 (M.D. Tenn. Dec. 18, 2015) (expressing skepticism that information about a GPS tracking device fell within scope of privilege because of the familiarity of the technology and technique involved); Ibrahim v. Dep't of Homeland Sec., No. C 06-00545 WHA, 2013 WL 1703367, at *5 (N.D. Cal. Apr. 19, 2013) ("screening procedures and requirements for being placed on the No-Fly and other watch lists" could be disclosed, despite claim of privilege, pursuant to an "attorney's eyes only" protective order limiting further dissemination); United States v. Wright, No. 2:08-CR-5-02, 2008 WL 8797841, at *4 (D. Vt. Nov. 3, 2008) (claim of privilege was overcome with respect to "training and certification records that reflect the [drug detection] dog's accuracy and reliability").

232. Cale G. Weissman, *How An Obsessive Recluse Blew the Lid off the Secret Technology Authorities Use to Spy on People's Cellphones*, BUS. INSIDER (June 19, 2015), http://www.businessinsider.com/how-daniel-rigmaiden-discovered-stingray-spying-technology-2015-6 [https://perma.cc/8S9R-X95U].

233. United States v. Rigmaiden, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012).

234. *Id.* at 995–96, 1005.

235. *Id.*

determination on the core Fourth Amendment questions.[236]

Thus, despite vigorous litigation with an extraordinarily dogged and well-prepared criminal defendant, the courts and the public remained in the dark about both the legal boundaries and technical powers of the government's Stingray technology. In the mine run of criminal cases, secret technologies will go undetected or unchallenged because defense lawyers, carrying heavy caseloads, usually have little capacity to piece together the highly technical methods potentially used against their clients and few resources to employ experts, who are generally necessary to build a legal challenge.[237]

In short, the law enforcement privilege stands as a major obstacle to disclosure of novel law enforcement technologies and to adjudication of the legal rules that govern them. The scope of the privilege exceeds what a concern to prevent circumvention could justify. Even in the context of criminal cases, which fully engage the due process rights of individual defendants, courts have been reluctant to allow disclosure. The law thus erects barriers against external oversight even where police use novel technologies to obtain criminal convictions.

VI. REFORMING THE LAW OF SECRET LAW ENFORCEMENT TEHNOLOGIES

Any meaningful reform agenda must address two basic problems caused by anti-circumvention secrecy: (1) secrecy reallocates power away from legislatures and courts to the police, leaving the police free to use intrusive technologies without meaningful checks; and (2) it distorts the relationship between citizens and the government by expanding the investigatory and informational powers of government at the expense of an unwitting citizenry. This Article offers two strategies to achieve such reform. The first targets the legal doctrines that provide the government overbroad powers to resist disclosure in the face of requests from the public. The second requires affirmative disclosure and public comment so that legislatures, courts, and the public can engage in the process of regulating novel technologies before they

236. *See id.* at 999–1002. In a subsequent decision, the Court found that the warrant the government had obtained was valid, despite the fact that the warrant application gave no indication to the magistrate judge that the search was to be conducted using a Stingray device. *See* United States v. Rigmaiden, No. 08-cr-814, 2013 WL 1932800, *33–34 (D. Ariz. May 8, 2013).

237. Recognizing this problem, some non-profit organizations and legal services offices have begun to devote specialized staff to build challenges to novel surveillance technologies. *See, e.g.*, NAT'L ASS'N OF CRIM. DEF. LAW, *Nation's Criminal Defense Bar Launches Initiative to Educate, Litigate Privacy Challenges in a Digital Age* (2018), https://www.nacdl.org/Fourth-Amendment-Center-Launch/ [https://perma.cc/W5W9-738L].

come into routine use.

A. NARROWING THE SCOPE OF ANTI-CIRCUMVENTION SECRECY

As we have seen, existing doctrines protect far more information about novel technologies than a rigorous application of the anti-circumvention argument justifies. Courts endorse secrecy based on too little evidence about how disclosure would actually lead to circumvention.[238] The straightforward response to this problem would be to require courts to demand more from law enforcement. Why not amend the laws to impose a higher burden of justification on law enforcement agencies? Why not simply urge judges to exercise their existing powers more vigorously?

This straightforward solution is intuitively appealing, but it is likely doomed to fail. The history of FOIA is a history of judicial deference to agencies.[239] Despite Congress' textual mandate that courts must review secrecy claims "de novo" and that the "burden is on the agency to sustain its action,"[240] courts have been reluctant to vigorously guard the line between the public's business and proper secrets. As a general rule, courts defer to government claims and do not demand detailed or highly persuasive justifications.[241] Prior efforts to strengthen the judicial role by amending FOIA have failed. In 1974, Congress went so far as to override a veto by President Ford in order to empower judges to vigorously oversee government secrecy claims.[242] The effort failed; scholars and commentators agree that judges quickly reverted to a very deferential posture.[243] In light of this experience, textual amendments purporting to require courts to scrutinize the government's justifications more closely are not likely to make a difference, except perhaps at the margins.[244]

---

238. *See* Part V.

239. *See, e.g.*, Margaret B. Kwoka, *Deferring to Secrecy*, 54 B.C. L. REV. 185, 211–35 (2013); Margaret B. Kwoka, *Deference, Chenery, and FOIA*, 73 MD. L. REV. 1060, 1067–74 (2014).

240. 5 U.S.C. § 552(a)(4)(B) (2018).

241. *See, e.g.*, Larson v. Dep't of State, 565 F.3d 857, 865, 867–88 (D.C. Cir. 2009); ACLU v. U.S. Dep't of Def., 901 F.3d 125, 133–34, 136 (2d Cir. 2018)

242. *See* David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. PA. L. REV. 1097, 1118–19 (2017).

243. *See, e.g.*, *id.*; Kwoka, *Deferring to Secrecy*, *supra* note 239, at 199–200; Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 156–63 (2006); Nathan Slegers, Comment, *De Novo Review Under the Freedom of Information Act: The Case Against Judicial Deference to Agency Decisions to Withhold Information*, 43 SAN DIEGO L. REV. 209, 213–18 (2006); Paul R. Verkuil, *An Outcomes Analysis of Scope of Review Standards*, 44 WM. & MARY L. REV. 679, 687–93 (2002).

244. A recent amendment to FOIA which requires the government to show "reasonably foresee[able] . . . harm," in order to invoke exemptions may reign in the broadest applications of Exemption 7(E). 5 U.S.C. § 552(a)(8)(A)(i)(I) (2018); *see supra* note 190. But that amendment is unlikely to prompt courts to be more skeptical in general of government claims that disclosure will risk circumvention.

If increasing the justificatory burden on the government (or the stringency of judicial oversight) is unlikely to succeed, what will? Some authors have proposed that courts should be empowered to weigh the public interest in disclosure against the government's exemption claims.[245] This would empower judges to consider all of the arguments in favor of transparency canvassed in the previous Parts. No doubt, some courts would use this doctrinal tool to order disclosure. However, it seems more likely that courts will not wield this authority particularly aggressively, just as they have failed to vigorously exercise their (already very strong) textual authority to conduct de novo review.

The reason for this has to do with the prevailing judicial culture and self-conception about the proper role of judges—particularly federal judges. Many judges today resist the idea that it is *their* responsibility—rather than the agency's—to make value judgments about whether disclosure is warranted or predictive judgments about the likely harm of disclosure. This is especially true in matters of law enforcement and security, where deference is especially pronounced.[246] A public interest override cuts against the grain of this prevailing judicial culture. It asks the judge to make *her own* value judgment and prediction about the relative harms and benefits of disclosure. In a similar way, Congress's requirement of de novo review in FOIA cases imagined that the judge would make *her own* judgment about whether secrecy was warranted. But in practice, that provision has resulted in judges serving only as a mild check on the "plausibility" or "logic" of the agency's decision.[247] All such doctrinal constructs depend on the idea that the judge will take the ultimate secrecy determination out of the agency's hands—that the court will make its own determination, not merely sit in review of the agency's. But that role is not one that many contemporary judges seem willing to play. It simply does not appear to comport with the dominant views about the (circumscribed) role and (limited) competence of judges, especially in matters of law enforcement and security.

A different sort of reform, however, may be more effective. What we need are additional *categorical* limits on what falls within the FOIA exemption for law enforcement techniques and the corresponding privilege. Categorical rules do

245. *See* Katie Townsend & Adam A Marshall, *Striking the Right Balance: Weighing the Public Interest in Access to Agency Records Under the Freedom of Information Act*, *in* TROUBLING TRANSPARENCY: THE HISTORY AND FUTURE OF FREEDOM OF INFORMATION 226, 233–41 (David E Pozen & Michael Schudson, eds. 2018).

246. *See, e.g.*, *ACLU*, 901 F.3d at 134, 136; ACLU v. Dep't of Def., 628 F.3d 612, 624 (D.C. Cir. 2011); ACLU v. Dep't of Justice, 681 F.3d 61, 76 (2d Cir. 2012). *But see* N.Y. Times Co. v. U.S. Dep't of Justice, 765 F.3d 100, 116–17 (2d Cir. 2014) (finding that the government had waived various national security exemptions to disclosure because it had already released a version of the document it sought to withhold).

247. *See supra* notes 239–243 and accompanying text.

not ask the courts to weigh the relative strength of the government's case for secrecy against the public's interest in disclosure. Instead they require the courts simply to determine what the withheld material *is* and whether it falls inside or outside a particular description. This type of analysis casts judges in the more comfortable role of sorting facts into legal categories—exempt vs. non-exempt—rather than making predictive judgments or value judgments about the relative harms and benefits of disclosure. It is therefore more likely to be an effective way to rein in existing anti-circumvention doctrines.

This Article offers four potential categorical limits on the scope of secrecy. First, FOIA exemptions and the law enforcement privilege should not allow police to keep secret the very existence of a secret technology. It is one thing for police to keep the public in the dark about how the police use some technology, it is quite another for police to conceal from the public that the technology exists at all. In the latter case, the public (and criminal defendants) cannot even know that there is something to be worried about and so secrecy serves to utterly frustrate any external checks. These kinds of secrets—known as "deep secrets"—are widely regarded as problematic, perhaps even raising constitutional problems because they circumvent the basic democratic levers of our constitutional system.[248]

Second, anti-circumvention doctrines should not allow the government to keep secret the *rules* that govern how a technology may be used. In other words, the anti-circumvention argument cannot justify "secret law." This limit on secrecy reflects the idea that secret law is fundamentally at odds with the rule of law and basic notions of due process, particularly where rules in question regulate government powers that affect the public.[249]

A prohibition on secret rules also has at least some pedigree in existing case law. In one of its early FOIA decisions, the Supreme Court held that the government's power to withhold privileged "deliberative process" materials under FOIA could not justify withholding " 'opinions and interpretations' which embody the agency's effective law and policy."[250] This decision rested

248. *See* David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 288–92, 305–06 (2010); *see also* Manes, *supra* note 22, at 817–26.

249. *See generally* Manes, *supra* note 22 (examining the problems with secret law in depth); LON FULLER, THE MORALITY OF LAW (rev. ed. 1969) (arguing that one of the principles essential to the "internal morality of law" is that laws cannot be kept from the public); Jonathan Hafetz, *A Problem of Standards?: Another Perspective on Secret Law*, 57 WM. & MARY L. REV. 1 (2016); Dakota S. Rudesill, *Coming to Terms with Secret Law*, 7 HARV. NAT'L SEC. J. 241 (2015); Sudha Setty, *No More Secret Laws: How Transparency of Executive Branch Legal Policy Doesn't Let the Terrorists Win*, 57 KAN. L. REV. 597 (2009); ELIZABETH GOITEIN, BRENNAN CENTER FOR JUSTICE, THE NEW ERA OF SECRET LAW (2016).

250. NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 153 (1975) (internal quotation omitted).

explicitly on the idea that FOIA itself "represents a strong congressional aversion to 'secret [agency] law' . . . and represents an affirmative congressional purpose to require disclosure of documents which have 'the force and effect of law.' "[251] Lower courts subsequently extended this "secret law" doctrine to another FOIA exemption that—at the time, at least—permitted secrecy of documents that would "risk circumvention of agency regulations" in general.[252]

Unfortunately, however, the courts have thus far declined to extend this anti-secret law principle to the rules that govern investigative techniques, in particular. In one early case, the D.C. Circuit determined that a Bureau of Alcohol, Tobacco, and Firearms manual "designed to establish rules and practices for agency personnel, i.e., law enforcement investigatory techniques" and which "ha[d] some effect on the public-at-large" nevertheless did not constitute "secret law" because the "manual is used for predominantly internal purposes."[253] Recent cases continue this trend.[254] But these cases have come under intense criticism,[255] and their reasoning does not seriously grapple with the idea that the government can act according to secret rules—and therefore short-circuit democratic checks—simply in order to preserve an advantage in the small slice of criminal investigations where it might make a difference.

Third, the government should not be permitted to withhold facts about the capabilities of a technology—or the manner in which it is used—insofar as those facts are necessary to determine whether the Fourth Amendment has been violated. The basic idea is that the government should not be able to evade accountability for potential violations of the fundamental law of the country by keeping those violations secret. In order to operationalize this limit, the party seeking disclosure could be required to come forward with a colorable argument that the technology is being used in such a way that it

251. *Id.* (quoting K. Davis, *The Information Act: A Preliminary Analysis*, 34 U. CHI. L. REV. 761, 797 (1967), and H.R. REP. NO. 1497, at 7 (2019)) (alteration in original).

252. *See* Crooker v. Bureau of Alcohol, Tobacco & Firearms, 670 F.2d 1051, 1067–75 (D.C. Cir. 1981) (construing FOIA Exemption 2, 5 U.S.C. § 552(b)(2)); Jordan v. U.S. Dep't of Justice, 591 F.2d 753, 781–82 (D.C. Cir. 1978) (Bazelon, J., concurring) (same). The Supreme Court has since ruled that these cases rested on a mistaken interpretation of Exemption 2 under which there was a general exemption for disclosures of any records that could lead to circumvention of agency regulations. *See* Milner v. Dep't of the Navy, 562 U.S. 562, 573–76 (2011). The Court clarified that FOIA only includes one specific anti-circumvention exemption—the one for law enforcement techniques found in Exemption 7(E). *Id.* at 575.

253. *Crooker*, 670 F.2d at 1073.

254. *See, e.g.*, ACLU v. Dep't of Justice, No. 12 Civ. 7412(WHP), 2014 WL 956303, at *8 (S.D.N.Y. Mar. 11, 2014) (rejecting "secret law" carve-out to Exemption 7(E)).

255. *See, e.g.*, Jameel Jaffer & Brett Max Kaufman, *A Resurgence of Secret Law*, 126 YALE L.J. F. 242, 248 (2016) (discussing cases that have allowed agencies to keep their effective law and policies secret).

violates the Fourth Amendment; the government would then be required to disclose facts necessary to illuminate the claim. In the FOIA context, this change would probably require legislation; nothing in the current text suggests that constitutional considerations are relevant. With respect to the evidentiary privilege, courts could simply relax the showing of "need" that is required for a criminal defendant to overcome a claim of privilege. Instead of imposing a high bar, courts could simply rule that disclosure is required whenever there is a colorable claim the Fourth Amendment may have been violated.[256]

Finally, secrecy about the capabilities of novel technologies could expire once a technology comes into routine use—as opposed to merely experimental use. The idea here is that it makes sense for law enforcement to have some leeway to try out novel technologies and deliberate about their effectiveness without necessarily opening itself up to scrutiny. However, once the police put a technology into routine use, the public's interest in understanding the capabilities of law enforcement outweigh the police's interest in preventing circumvention.[257] To be sure, this could make law enforcement's task harder at the margin. To the extent that disclosure tips off sophisticated criminals to adopt countermeasures they were not otherwise taking, law enforcement's task will be more difficult. But, ultimately, that may be a price we must pay to live in a democratically accountable society, and it is a price that we already happily pay with respect to all of the humdrum investigative tools that police have been using for decades—from wiretaps to polygraphs to fingerprints. It is unclear why we should be willing to extend to *new* technologies a shroud of secrecy that we seem quite able to live without with respect to old, well-known technologies.

B. PUBLIC NOTICE AND COMMENT FOR NOVEL INVESTIGATIVE TECHNOLOGIES

The more ambitious solution to the problem of secret investigative techniques redistributes regulatory power from the police to legislatures and courts through mandatory, affirmative disclosure requirements. Under the status quo, the police can obtain and deploy new technologies without necessarily putting anyone else on notice. This is especially true with respect

256. Courts would also have to rebuff government efforts to evade disclosure by making strategic concessions, as the government did in the *Rigmaiden* case. *See supra* notes 232–236 and accompanying text.

257. As I use the term here, "routine" use does not mean frequent use, but instead that the technology is among the tools that the police have at their disposal should they choose to use it. Democratic accountability and public deliberation concerns do not dissipate just because a technology is used relatively infrequently. In fact, some of the most intrusive technologies may be used infrequently because they are costly, complex, or controversial. This may be the case with respect to x-ray vans; we don't know.

to surveillance tools because they are less visible to the public than other police technologies. If the police adopt tasers, for example, the public will be able to see them. However, if the police begins using facial recognition software to analyze footage from existing surveillance cameras, that can easily remain invisible to the public for years. Doctrinal solutions that merely tighten up FOIA exemptions and privileges, like those proposed above, will only produce greater transparency if potential litigants learn enough about a particular technology to be able to bring affirmative challenges in court seeking disclosure.

I propose instead to flip the status quo by requiring law enforcement to issue a public notice whenever it acquires a new technology, before the technology goes into regular use. The notice would, at a minimum, document the capabilities of the technology, describe its purpose, and disclose the proposed policies governing its use, including the circumstances in which it can be used (and the internal or external authorizations required) and the restrictions on retention, access, or use of information collected using the technology. The notice could also require the police to identify and assess potential effects on individual rights to privacy, non-discrimination, and other civil liberties, and to include an analysis of the proposed technology's compliance with applicable constitutional and statutory restrictions. The basic idea is that the notice would provide the information necessary to permit the legislature and the public to exercise meaningful control and oversight over the deployment of novel technologies.

In conjunction with the public notice, the public would have the opportunity to comment on the proposed policy and for the legislature to hold hearings or otherwise engage in oversight. The policy would not go into effect until and unless the police considered and addressed the comments and issued a final policy. In form and function, the process would be akin to the notice and comment process that is familiar from many areas of administrative law practice.[258]

This proposal has the virtue of requiring a democratic conversation about the proper place of a technology *at the outset*, before it has become entrenched. It eliminates secrecy at the outset by imposing an affirmative disclosure requirement on law enforcement. It also recalibrates how the anti-circumvention argument may be deployed to resist transparency. By enacting a general notice-and-comment regime governing novel surveillance technologies, the legislature effectively makes a judgment that legislative oversight and democratic accountability values should generally prevail over

258. *See* Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 137–49 (2016).

anti-circumvention concerns.

Moreover, the notice-and-comment process permits some flexibility as to the level of granularity at which the police disclose the policies governing a surveillance technology. The idea is that the police could disclose policies that are granular and detailed enough to permit the public to understand (and, potentially, criticize) how the novel technology will be used, but not so granular that a criminal could readily use the policy as a detailed roadmap to evade the new technology. I have argued elsewhere, in an article examining the phenomenon of secret law, that adjusting the level of granularity at which the government discloses its rules and legal interpretations can be a powerful way to modulate the tension between democratic interests in transparency and governmental interests in secrecy.[259] In the context of a notice-and-comment process, there is the possibility of modulating the degree of secrecy in just this way: if the police pitch public notice in terms that are not sufficiently specific or concrete, the legislature and public will be in a strong position to demand greater transparency before the technology comes into use.

The affirmative notice and comment process also shifts the terrain on which we adjudicate arguments about anti-circumvention secrecy. In the ordinary FOIA process, *courts* have to make a legal judgment, ex-post, about whether disclosure of a particular piece of information falls within the exempt category of "techniques and procedures." As we have seen, courts have been reluctant to consider countervailing policy considerations favoring transparency when making those judgments. Indeed, courts have been very deferential to law enforcement secrecy arguments.[260]

By contrast, the affirmative notice-and-comment process creates a new locus for decisions about secrecy outside of the courts and away from legal wrangling over the scope of the relevant FOIA exemptions or other doctrines. Instead, the notice-and-comment process requires *legislatures* (and, by extension, the public) to make a *policy* judgment about whether additional disclosure is necessary in order to permit meaningful and sufficient public accountability. The idea is that the give-and-take between the legislature, the public, and law enforcement is likely to shift the boundary between secrecy and transparency to a place that may provide more meaningful disclosure than courts have been willing to offer. The hope is that in this way the public's interest in transparency and accountability will have more weight in decisions

259. *See* Manes, *supra* note 22, at 837–38.

260. *See, e.g.*, Pozen, *supra* note 242, at 1099; Kwoka, *Deferring to Secrecy*, *supra* note 239, at 211–35; Mark Rumold, *The Freedom of Information Act and the Fight Against Secret (Surveillance) Law*, 55 SANTA CLARA L. REV. 161, 179 (2015); Robert P. Deyling, *Judicial Deference and De Novo Review in Litigation over National Security Information under the Freedom of Information Act*, 37 VILL. L. REV. 67, 93 (1992).

about where to draw the curtain around police capabilities or policies.

This reform proposal draws on the recent "administrative turn" in scholarship regarding police regulation and oversight. In particular, this proposal builds on the recent work of Professor Christopher Slobogin, who has proposed administrative law processes like notice-and-public-comment as a means to regulate "panvasive," suspicionless police practices like drug-testing programs or traffic checkpoints that affect large segments of the population.[261] This Article proposes, in effect, that this administrative law approach should govern all novel surveillance technology.

These types of reforms are having some success on the ground. Indeed, in offering this reform agenda this Article is not writing on a blank slate. Not only does Slobogin's recent work prefigure the idea of notice and comment, but the proposal here closely mirrors legislative proposals developed by a broad coalition of civil rights organizations that is pursuing reforms in state and local legislatures around the country.[262] Indeed, over the past two years, surveillance transparency laws that include some or all of essential elements described above have been enacted in several cities and counties,[263] and at least two states have taken up legislation that would have statewide effect.[264] While there do not yet appear to be efforts at the federal level to require this kind of surveillance transparency, it is possible at least to imagine Congress enacting public notice-and-comment requirements as a condition of federal funding to

261. Slobogin, *supra* note 258, at 93; *cf.* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 60 STAN. L. REV. 1039, 1047–49 (2016).

262. *See, e.g.*, ACLU, COMMUNITY CONTROL OVER POLICE SURVEILLANCE: TECHNOLOGY 101, *supra* note 8; *The Public Oversight of Surveillance Technology (POST) Act: A Resource Page*, BRENNAN CENTER FOR JUSTICE (June 12, 2017), https://www.brennancenter.org/analysis/public-oversight-police-technology-post-act-resource-page [https://perma.cc/AK8T-VHYH]; Michael Price & Alyssa Derosa, *New York City is Making its Citizens Safer by Overseeing Police Technology*, HUFFINGTON POST, Apr. 3, 2017, https://www.huffingtonpost.com/entry/new-york-city-is-making-its-citizens-safer-by-overseeing-police-technology_us_58e23f04e4b0ba359596583b [https://perma.cc/Y6SH-8SLC]. The ACLU has developed model legislation that it hopes to enact in local and state legislatures around the country. *See* ACLU, *An Act to Promote Transparency and Protect Civil Rights and Civil Liberties with Respect to Surveillance Technology* (2017), https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf [https://perma.cc/E3UL-GQHH].

263. *See, e.g.*, Acquisition and Use of Surveillance Technologies, SEATTLE MUN. CODE §§ 14.18.010–.070 (Aug. 2, 2017); Surveillance Technology Use and Community Safety Ordinance, BERKELEY MUN. CODE §§ 2.99.010–.110 (Mar. 13, 2018). *See generally* ACLU, *An Act to Promote Transparency and Protect Civil Rights and Civil Liberties with Respect to Surveillance Technology*, *supra* note 262.

264. *See* S.B. 21, 2017-2018 Leg. Sess. (Ca. 2016); S.B. 1186 (Ca. 2018); An Act to Promote Transparency with Respect to Surveillance Technology, Me. S. Paper 268, Legis. Doc. 823 (introduced Mar. 2, 2017).

states and local law enforcement agencies.[265] It is also of course possible for the federal government to enact a surveillance transparency law to govern its own law enforcement agencies. In any event, there is a building movement for reform. Through this Article, I throw my hat in the ring with the advocates pursuing surveillance transparency laws.

VII. CONCLUSION

Secret innovation in law enforcement surveillance technology poses a challenge to democratic accountability as well as legislative and judicial oversight of police. Law enforcement has justified this secrecy by arguing that it is necessary to prevent criminals from circumventing novel police techniques. The practice on the ground and the decisions of courts, however, have produced a degree of secrecy that outstrips this justification. They have also failed to properly consider powerful countervailing values favoring transparency. The result is that the public, legislatures, and courts are largely shut out of the conversation even while we are seeing explosive growth in police surveillance technologies that raise profound constitutional, statutory, and policy problems.

Put simply, a concern to prevent criminals from misusing information has led to its suppression, even though that information is essential to democratic governance. In order to maintain meaningful external checks and public accountability, it will be necessary to tame the anti-circumvention argument, narrow its scope, and flip presumptions of secrecy so that transparency prevails in the face of speculation that disclosure might somehow, somewhere create an opportunity for evasion.

265. The federal government has distributed billions of dollars to federal and state law enforcement to fund police equipment. *See generally* NATHAN JAMES, CONG. RES. SERV., EDWARD BYRNE MEMORIAL JUSTICE ASSISTANCE GRANT PROGRAM (2013); Alicia Parlapiano, *The Flow of Money and Equipment to Local Police*, N.Y. TIMES (Dec. 1, 2014), https://www.nytimes.com/interactive/2014/08/23/us/flow-of-money-and-equipment-to-local-police.html?_r=0 [https://perma.cc/QE8S-LGFA].