Brooklyn Law Review

Volume 79 | Issue 1 Article 1

2013

The Legislative Response to Mass Police Surveillance

Stephen Rushkin

ARTICLES

The Legislative Response to Mass Police Surveillance

Stephen Rushin†

INTRODUCTION

Over the last two decades, police departments have dramatically expanded the use of advanced surveillance technologies. In 1997, around 20% of American police departments reported using some type of technological surveillance.[1] By 2007, that number had risen to over 70%.[2] And no longer do police rely exclusively on basic surveillance technologies. The increasingly efficient and technologically advanced law enforcement of the twenty-first century utilizes a wide range of surveillance devices including automatic license plate readers (ALPR),[3] surveillance cameras,[4] red light cameras,[5] speed cameras,[6] and biometric technology like facial recognition.[7]

---

† Visiting Assistant Professor, University of Illinois College of Law. I owe a debt of gratitude to the participants in the "Privacy, Surveillance Technologies, and the Fourth Amendment" panel at the Law and Society Association Annual Meeting for their thoughtful feedback.

[1] U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, LAW ENFORCEMENT MANAGEMENT AND ADMINISTRATIVE STATISTICS (LEMAS): 1997 SAMPLE SURVEYS OF LAW ENFORCEMENT AGENCIES (1997) [hereinafter LEMAS 1997], *available at* http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/2700?q=1997+LEMAs (to access follow "Log In/Create Account" hyperlink; once registered, follow the "codebook.pdf" hyperlink on the LEMAS 1997 page) (defining surveillance as the percentage of total departments that report using some type of video cameras).

[2] U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, LAW ENFORCEMENT MANAGEMENT AND ADMINISTRATIVE STATISTICS (LEMAS): 2007 SAMPLE SURVEYS OF LAW ENFORCEMENT AGENCIES (2007) [hereinafter LEMAS 2007], *available at* http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/31161 (defining surveillance as the percentage of total departments that report using some type of video cameras).

[3] *See, e.g.*, Ryan Gallagher, *Police Across U.S. Quietly Turning to Cameras That Track All Vehicles' Movements: Survey*, SLATE (Jan. 14, 2013), http://www.slate.com/blogs/future_tense/2013/01/14/automatic_license_plate_readers_survey_shows_most_u_

I have previously called this radical shift in policing the beginning of the *digitally efficient investigative state*.[8] By this, I mean that police today utilize technological replacements for traditional investigations that dramatically improve the efficiency of surveillance. These digitally efficient technologies do not give police any unique extrasensory ability.[9] They merely improve the efficiency of public surveillance. Furthermore, these technologies only collect information on public movements and behaviors. They do not intrude on any constitutionally protected or private space.[10] However, these tools have developed into a form of widespread community surveillance, which presents privacy concerns for many members of the community.

In addressing public surveillance under the Fourth Amendment, the Supreme Court has previously operated under two important presumptions. I call these two general rules the *jurisprudential assumptions of police surveillance.* First, individuals have no reasonable expectation of privacy in any activities they make in public that may be visible to law enforcement. [11] So while officers need probable cause or a warrant to enter a home or automobile, they do not need any

---

s_police_agencies_plan.html (noting recent surveys indicating that ALPR is spreading throughout American police departments).

[4] *See, e.g.*, *City Looks at Outside Firm to Oversee Police Surveillance Cameras*, ROCHESTER DEMOCRAT & CHRON., Jan. 4, 2013, (explaining how in cities like Rochester, the installation of over 200 surveillance cameras in the City now requires the hiring of a private company to monitor the cameras).

[5] *See, e.g.*, Larry Barszewski, *Fort Lauderdale to Add More Red-Light Cameras*, SUN SENTINEL (Jan. 23, 2013), http://articles.sun-sentinel.com/2013-01-23/news/fl-brief-lauderdale-red-light-cameras-20130123_1_american-traffic-solutions-red-light-cameras-intersection-approaches (noting that that cities like Fort Lauderdale are moving to install more red light cameras).

[6] *See, e.g.*, Erin Cox, *State Highway Administration Defends Speed Camera Program*, BALT. SUN (Jan. 15, 2013), http://articles.baltimoresun.com/2013-01-15/news/bs-md-speed-camera-briefing-20130115_1_camera-tickets-camera-law-camera-program (discussing Maryland's significant investment in speed cameras across the state).

[7] *See, e.g.*, Eric Hartley, *LAPD's 16 San Fernando Valley Surveillance Cameras Go Live*, L.A. DAILY NEWS (Jan. 16, 2013, 9:00 PM), http://www.dailynews.com/general-news/20130117/lapds-16-san-fernando-valley-surveillance-cameras-go-live (mentioning that surveillance cameras used by the LAPD use facial recognition software technology that can identify a person from 600 feet away).

[8] *See* Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281 (2011).

[9] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[10] This distinction between public and private is important. *See* United States. v. Knotts, 460 U.S. 276, 281-82 (1983) (noting that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another").

[11] *See, e.g.*, *Knotts*, 460 U.S. at 281 (determining that a person has no reasonable expectation of privacy in their public movements on roads or highways); Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (holding that a person has no reasonable expectation of privacy in the phone numbers they dial); Katz v. United States, 389 U.S. 347, 360 (1967) (establishing standard for a reasonable expectation of privacy).

authorization to investigate or record a person's activities in public. Second, while technologies that give the state an extrasensory ability may violate an individual's reasonable expectation of privacy, technologies that merely improve the efficiency of otherwise permissible investigation techniques are presumptively permissible.[12] Thus, while officers must obtain a warrant before using some extrasensory technologies, the Court generally does not regulate efficiency-enhancing technologies. These jurisprudential assumptions of police surveillance have been workable in the past because of the limited use and capability of efficiency-enhancing technologies.

I have previously argued, however, that in the age of the digitally efficient investigative state, efficiency-enhancing technologies have become sufficiently intrusive as to demand a new doctrinal path.[13] In *United States v. Jones*, the Supreme Court considered one such efficiency-enhancing surveillance technology—global positioning systems (GPS).[14] There, law enforcement officers installed a GPS device on a suspect's car without a valid warrant.[15] The government argued that the police did not need a warrant to install the GPS device because it was merely an efficient replacement for an otherwise legal police investigation tactic—public surveillance.[16] But Antoine Jones claimed that he had a reasonable expectation that all of his movements over the course of a month would not be recorded in great detail by the state, even if they were executed in public.[17]

The *Jones* case presented the perfect opportunity for the Court to amend one or both of the jurisprudential assumptions of police surveillance, but the Court punted the issue. The majority merely found that the installation of a GPS device violated the Fourth Amendment because of the device's physical installation on the automobile.[18] Post-*Jones*, many academics criticized the Court for not addressing the privacy issues raised by police surveillance technologies.[19] I believe the Court will eventually regulate the digitally efficient investigative state in some manner. Indeed, dicta in the concurrences by Justices Sotomayor and Alito

---

[12] Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 433-39 (2007).

[13] Rushin, *supra* note 8, at 282.

[14] United States v. Jones, 132 S. Ct. 945 (2012).

[15] *Id.* at 948.

[16] *Id.* at 949-50.

[17] *See id.*

[18] *Id.* at 953.

[19] *See, e.g.*, Lauren Millcarek, Comment, *Eighteenth Century Law, Twenty-First Century Problems:* Jones*, GPS Tracking, and the Future of Privacy*, 64 FLA. L. REV. 1101 (2012).

suggest that the Court will be receptive to broader regulation of efficiency-enhancing surveillance technology in the near future.[20] Nevertheless, history dictates that any judicial regulation will be limited and likely rely on the often-ineffective exclusionary rule for enforcement.[21] As a result, Congress and state legislators must play a significant role in any future regulation of police surveillance. Given that law enforcement in the United States is highly decentralized,[22] much of this regulation will have to come from state legislatures.

In this article, I present a model statute that a state could enact to regulate the digitally efficient investigative state. This statute adheres to three major principles about the regulation of police surveillance. First, any regulation must provide clear standards that law enforcement can easily understand and apply.[23] Second, as communities differ substantially in their need for public surveillance, any legislation must provide local municipalities with some ability to vary standards to meet their legitimate law enforcement needs. Third, any regulation must articulate the narrow scope of technologies and devices that fall under its regulatory purview. Because technology changes rapidly, this ensures that the law will not be misapplied to future, emerging technologies.

The model statute I offer in this article honors these three important principles. The statute regulates the indiscriminate collection and retention of data by law enforcement surveillance technologies, while also permitting the use of technological surveillance for mere observational comparison. The statute

---

[20] *See, e.g.*, *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (noting that "physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance" (citations omitted)).

[21] *See* Rachel A. Harmon, *Promoting Civil Rights Through Proactive Policing Reform*, 62 STAN. L. REV. 1, 10 (2009) (noting that the exclusionary rule is "by far the most commonly used means of discouraging police misconduct," which is ineffective because of its numerous exceptions and narrow scope).

[22] *See* Samuel Walker & Morgan Macdonald, *An Alternative Remedy for Police Misconduct: A Model State "Pattern or Practice" Statute*, 19 GEO. MASON U. C.R. L.J. 479, 484 (2009) (noting that American law enforcement is "organizationally fragmented" meaning that "there is no single controlling authority that could presumably establish minimal standards for personnel, operations, and accountability procedures").

[23] Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 124 (2012) (noting the importance of clear and articulable rules for law enforcement); Charlie Savage, *Judges Divided over Rising GPS Surveillance*, N.Y. TIMES, Aug. 14, 2010, at A12 (Professor Orin Kerr arguing that police need clear rules).

establishes a maximum length of time for data retention. It also limits the sharing of personally identifiable information, and requires that law enforcement demonstrate a legitimate investigative purpose for identifying and accessing data. To enforce these broad regulations, the statute gives the state attorney general the authority to bring lawsuits against police departments that fail to abide by these regulations and excludes from criminal court any locational evidence obtained in violation of the statute.

This statute would not address all of the concerns of the digitally efficient investigative state. After all, no statute can fully predict and control the development of new and emerging technologies. Nevertheless, it would be a major step toward coherency. This legislation would give a police department discretion to craft unique data policies tailored to its community's specific needs, while also encouraging some level of statewide consistency. To date, only a small handful of law review articles have addressed the unique issues raised by digitally efficient community surveillance technology, such as automatic license plate readers (ALPR).[24] Furthermore, none of this work has offered a comprehensive legislative response that could guide future regulation. Thus, this article fills a void in the available legal scholarship.

I have divided this article into four parts. In Part I, I detail the growth and capabilities of the digitally efficient investigative state. I compile the most comprehensive set of data to date on the scope of digitally efficient investigative technologies in American police departments. I also present empirical evidence on the current state of internal departmental regulations. In Part II, I explore the law of police surveillance. In this Part, I further detail the jurisprudential assumptions about police surveillance that have guided the Court in the past. Post-*Jones*, it appears that these jurisprudential assumptions may no longer be valid, drastically increasing the incoherence of police surveillance law. Part III offers a comprehensive legislative response intended to curb the potentially dangerous effects of

---

[24] *See, e.g.*, Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 BERKELEY TECH. L.J. 755 (2008); Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. & TECH. L. REV. 589 (2012); Linda M. Merola & Cynthia Lum, *Emerging Surveillance Technologies: Privacy and the Case of License Plate Recognition (LPR) Technology*, 96 JUDICATURE 119 (2012); Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L. J. 27 (1995); Rushin, *supra* note 8; Tyson E. Hubbard, Note, *Automatic License Plate Recognition: An Exciting New Law Enforcement Tool with Potentially Scary Consequences*, 18 SYRACUSE SCI. & TECH. L. REP. 3 (2008).

mass police surveillance. I present and defend my proposed statutory regulation. Currently only a few states in the country regulate the use of any type of police surveillance technology.[25] I argue that this lack of regulation is increasingly indefensible. Both states and the judiciary must eventually take steps to comprehensively limit the use of digitally efficient community surveillance technologies.

I. THE DIGITALLY EFFICIENT INVESTIGATIVE STATE

Two years ago, I theorized on the emergence of a new type of policing that I called the digitally efficient investigative state.[26] This new type of policing relies on numerous technological surveillance methods that replace traditional policing tactics. Two classic examples of technologies used by the digitally efficient investigate state are video surveillance cameras with biometric recognition and automatic license plate readers (ALPR). I have argued that the advent of these new technologies demands a new type of regulatory response. In the first part of this section, I detail the characteristics of the digitally efficient investigative state.

In the second part of this section, I summarize the most up-to-date empirical data on the expansion of the digitally efficient investigative state. Since I theorized on this emerging institution of social control two years ago, surveys by social science researchers have uncovered important new information about the growth and scope of the use of digitally efficient investigative technologies in American police departments. In this subsection, I also explore the current state of internal departmental regulations of mass surveillance technologies. The available evidence paints a pessimistic picture. Departments rarely self-regulate their collection of data or reveal their data retention policies. This failure to effectively self-regulate presents a cogent argument for legislative action.

A. The Characteristics of the Digitally Efficient Investigative State

I define the digitally efficient investigative state as a technologically advanced form of policing, reliant upon efficiency-enhancing surveillance of an entire community. The digitally efficient investigative state seeks not just to monitor

---

[25] *See, e.g.*, ME. REV. STAT. 29-A, § 2117-A (2010); N.H. REV. STAT. ANN. § 236:130 (2011); VA. CODE ANN. § 2.2-3800 (2010).

[26] Rushin, *supra* note 8, at 284.

the activities of a single suspicious individual, but instead relies on widespread surveillance of the entire community. Two of the most common technologies used in the digitally efficient investigative state are ALPR and surveillance cameras with biometric recognition. Although most in the public are familiar with the capabilities of surveillance cameras, ALPR and biometric recognition are relatively new additions to the field of police surveillance. ALPR devices use "digital cameras mounted on a law enforcement vehicle or at stationary locations to snap images of passing license plates."[27] ALPR systems then convert these digital images of license plates into text files.[28] Once converted, ALPR systems can either "compare[] the plate numbers to available databases, often called hotlists," or they can store the data into searchable databases.[29] Video surveillance cameras have long served as a replacement for traditional, in-person police observation.[30] But today these surveillance cameras are increasingly armed with biometric recognition, like facial recognition software, which "permit law enforcement to identify the individuals captured by surveillance cameras" based on their facial features.[31]

Nine important characteristics define the digitally efficient investigative state. First, this policing technique only involves the collection of information on public behavior made visible to law enforcement. ALPR and surveillance cameras do not intrude into any private or protected space. This is different from other policing technologies like wiretaps or heat sensors. Wiretaps allow police to listen to conversations that were not publicly "broadcast to the world."[32] Heat sensors permit police to see "details of the home that would previously have been unknowable without physical intrusion."[33] Digitally efficient surveillance technologies, conversely, merely record information about observable behavior made visible to the devices. ALPR chronicles license plates as vehicles pass stationary or mobile ALPR cameras, and surveillance cameras record video, and occasionally audio, of public actions. The public nature of digitally efficient surveillance is a primary reason that the judiciary has historically avoided regulating these technologies.

---

[27] *Id.* at 285.
[28] *Id.*
[29] *See id.* at 285-86.
[30] *Id.*
[31] *Id.* at 288.
[32] Katz v. United States, 389 U.S. 347, 352 (1967).
[33] Kyllo v. United States, 533 U.S. 27, 40 (2001).

Second, the public information collected by these technologies is often personally identifiable. That is to say, once a digitally efficient surveillance device records an image of a license plate or a pedestrian, law enforcement can often identify the driver or pedestrian. Police using ALPR commonly cross-reference license plate numbers with state records of automobile owners to detect stolen cars or wanted criminals.[34] At least "[t]hirty-seven states currently load driver's license photographs into state databases, which are searchable using facial recognition software."[35] In both cases, police are able to take data collected via these efficiency-enhancing technologies and connect it to a specific individual.

The National Institute of Standards and Technology (NIST) defines personally identifiable information as "any information that can be used to distinguish or trace an individual's identity . . . and other information that is linked or linkable [to a specific person's identity]."[36] Classic examples of personally identifiable information would be a person's name, address, and telephone number.[37] The NIST also considers biometric data, including photographic images and videos, vehicle identifiers, and property records, to be personally identifiable.[38] Under this broad definition, data recovered by digitally efficient technologies is undeniably personally identifiable information. Police can easily link a car's license plate number to a specific owner. And police can often use biometric data from surveillance cameras—commonly facial recognition—to identify a pedestrian on the street. Thus, once digitally efficient surveillance technologies collect data, this data can be linked or connected with a specific person through cross-reference to other government databases.

Third, these technologies involve not just narrow observation of a single suspect, but the broad surveillance of an entire community over an extended period of time. This is different than less expansive surveillance technologies

---

[34] *See* CYNTHIA LUM ET AL., CTR. FOR EVIDENCE BASED CRIME POL'Y, GEORGE MASON UNIV., LICENSE PLATE RECOGNITION TECHNOLOGY: IMPACT EVALUATION AND COMMUNITY ASSESSMENT 21 (2010), *available at* http://gemini.gmu.edu/cebcp/lpr_final.pdf; Rushin, *supra* note 8, at 285-86.

[35] Rushin, *supra* note 8, at 288 (citing Joey Bunch, *Smiling Upon Grins: Colorado Allows Expressions That Other States Say Mess Up Driver's License Software*, DENVER POST, May 30, 2009, at B2, *available at* http://www.denverpost.com/news/ci_12481772).

[36] ERIKA MCCALLISTER ET AL., NAT'L INST. STANDARDS & TECH., U.S. DEP'T OF COMMERCE, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) 2-1 (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

[37] *Id.* at 2-2.

[38] *Id.*

previously considered by the Court, like GPS. A single GPS device affixed to an automobile can give police detailed information on the movements of a single automobile for an extended period of time.[39] A GPS device, however, is limited in scope. It only monitors and records the movements of a single criminal suspect at a time. This limits the broad community impact of GPS surveillance. Police have to identify an individual as a criminal suspect and then install the device to facilitate surveillance. By contrast, the technologies I describe as part of the digitally efficient investigative state broadly and indiscriminately monitor the public behavior of an entire community. Surveillance cameras record any and all behavior made public in front of their lenses. ALPR devices run the license plates of all automobiles that fall within the device's view. Thus, every person in a community becomes a target of the digitally efficient investigative state, not just pre-identified criminal suspects.

Fourth, because the digitally efficient investigative state monitors the entire community, it collects information on illegal activity as well as innocuous behavior. Some policing technologies, like red light and speed cameras, have been narrowly devised to only record images and collect data when a person violates a traffic law. The digitally efficient investigative state is different. Devices like ALPR and surveillance cameras are useful *because* they collect data on all passing cars and pedestrians. A single ALPR device or surveillance camera might replace the efforts of dozens, even hundreds, of individual law enforcement officers. ALPR, for example, is only useful because it is an unbelievably efficient replacement for a traditional policing technique—cross-referencing the license plates of passing cars with databases of active warrants and stolen automobiles. But when a device can cross-reference and record data on up to 1,800 license plates per minute,[40] it will invariably gather enormous amounts of data on innocent people.

Fifth, the technological tools used by the digitally efficient investigative state only improve the efficiency of otherwise permissible surveillance techniques. They do not offer officers any extrasensory ability. Many technological developments in policing have been met with suspicion because they give police a superhuman ability not typically associated

---

[39] United States v. Jones, 132 S. Ct. 945, 948 (2012) (noting that law enforcement gathered data on Antoine Jones's movements in his automobile for 28 days straight).

[40] Rushin, *supra* note 8, at 285.

with public policing. For example, in *Kyllo*, the Court barred the warrantless use of heat sensors that could allow police to see movements inside the walls of the home.[41] ALPR, surveillance cameras, and facial recognition arguably all complete tasks that an individual officer could complete without technological assistance. They just do so with astonishing efficiency.

Sixth, these technologies give officers two distinct capabilities: observational comparison and indiscriminate data collection. Observational comparison refers to the limited and temporary collection of data by a digitally efficient technology for comparison and cross-reference to relevant databases. For example, "[w]hen used for observation comparison, ALPR only retains data on license plates that match known or suspected criminal hotlists."[42] In the case of surveillance cameras armed with facial recognition, "the collection of data would be limited to individuals whose appearance so closely resembles a known criminal as to create reasonable, individualized suspicion."[43] By contrast, indiscriminate data collection refers to data retention practices whereby police indefinitely retain all information collected by digitally efficient technologies, regardless of whether the data is linked to any criminal investigation.

Seventh, advances in data storage capabilities have facilitated and incentivized the use of these technologies for indiscriminate data collection. Traditionally, one of the greatest limitations on long-term government surveillance was the limited data retention capabilities of the state.[44] But as the cost of data storage decreases, and the technological feasibility of such storage improves,[45] the government has no disincentive to collect as much data as possible on public behavior—so long as this information might be useful to a state.[46] In the case of law enforcement, information may seem irrelevant at the time of collection, but may end up being extremely valuable in solving future crimes.[47] Indeed, as I discuss in Part I.C, the only empirical evidence suggests that the overwhelming majority of

---

[41] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[42] Rushin, *supra* note 8, at 285.

[43] *Id.* at 288.

[44] *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 14 (2008).

[45] *See* Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 140-42 (2008).

[46] *See* Rushin, *supra* note 8, at 291.

[47] *Id.* at 286 (describing the hypothetical situation where a child is abducted, and police can immediately turn to surveillance data from the time and location of the suspected abduction).

departments with digitally efficient surveillance technology, like ALPR, use it for indiscriminate data collection.[48]

Eighth, indiscriminate data collection allows law enforcement to aggregate large amounts of information about a single individual, thereby revealing personal information about habits and behaviors. Five of the justices in *Jones* noted in two separate concurrences that the accumulation of large amounts of data on public movements transforms normal surveillance into a potentially unconstitutional invasion of individual privacy.[49] These extensive records on individual movements might reveal private interests, patterns of behavior, or habits. For example, aggregation of surveillance data of an individual might enable "the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[50] Police and the state can use this type of revealing personal information to target unpopular minorities or conduct fishing expeditions.[51]

Ninth, departments commonly share this personally identifiable information. Police have organized both nationally and regionally to share personally identifiable surveillance data.[52] As I explain further in Part I.C, the limited empirical data suggest that departments currently share data collected through digitally efficient surveillance technologies.[53] The sharing of this data is understandable and potentially useful. Criminals, like most individuals, often move in and out of different police jurisdictions. Information sharing allows police to efficiently identify not just criminals and stolen property from their jurisdiction, but also those from jurisdictions across the country. In a country like the United States with an extremely decentralized array of policing agencies, this type of data sharing can facilitate cooperation and dramatically increase the likelihood of apprehending criminals and recovering stolen property. For example, Cincinnati is currently building a regional data-sharing network for ALPR data for departments across Southwest Ohio, Southeast Indiana and Northern Kentucky, called SOSINK. The purpose of this regional network is to both apprehend wanted subjects traveling across this regional territory and collect intelligence relevant to

---

[48] *See infra* Part I.C.

[49] *See generally* United States v. Jones, 132 S. Ct. 945, 955-64 (2012) (Sotomayor, J., concurring & Alito, J., concurring).

[50] *Id.* at 956 (Sotomayor, J., concurring).

[51] *See* Rushin, *supra* note 8, at 299.

[52] *Id.* at 292.

[53] *See infra* Part I.C.

ongoing investigations in departments throughout the area.[54] Maryland law enforcement has developed a similar data-sharing network.[55] The state hopes to eventually have 32 agencies sharing information.[56]

This type of regional data sharing of surveillance data is relatively common; one study found that 43% of surveyed departments share data as part of a regional system.[57] But this type of sharing is also potentially problematic. Such sharing of personally identifiable data may increase the possibility of "secondary use."[58] As Daniel Solove explains, "[t]he potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability."[59]

The expansion of the digitally efficient investigative state is one of the most important developments in the history of policing. Digitally efficient surveillance technologies expand the reach of American police departments. Emerging evidence over the last two decades suggests that police presence may actually reduce crime by altering situational incentives.[60] One possible way to lower the overall crime rate of a community, then, is to increase the number of law enforcement officers.[61] But local communities must operate on finite budgets, limiting the number of police officers they can hire. Thus, criminologists and policing scholars have found that departments can most effectively reduce crime by allocating more of their staff to high

---

[54] *See* Russell A. Neville, *Cincinnati Regional Automatic License Plate Recognition Technology Project*, POLICE CHIEF MAG. (June 2009), *available at* http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1823&issue_id=62009.

[55] *See* Press Release, Office of Governor Martin O'Malley, Governor Martin O'Malley Announces Enhanced Fight Against Auto Theft (Aug. 4, 2010), *available at* http://www.governor.maryland.gov/pressreleases/100804.asp.

[56] DAVID J. ROBERTS & MEGHANN CASANOVA, INT'L ASS'N OF CHIEFS OF POLICE, AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS: POLICY AND OPERATIONAL GUIDANCE FOR LAW ENFORCEMENT 24 (2012).

[57] *Id.*

[58] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477, 521 (2006).

[59] *Id.* at 522.

[60] *See generally* Ronald V. G. Clarke, *'Situational' Crime Prevention: Theory and Practice*, 20 BRIT. J. CRIMINOLOGY 136 (1980) (describing situational crime prevention theory and how supervision of any variety, including police, can affect an individual's propensity for criminal behavior); Lawrence W. Sherman & David Weisburd, *General Deterrent Effects of Police Patrol in Crime "Hot Spots": A Randomized, Controlled Trial*, 12 JUST. Q. 625 (1995).

[61] *See generally* Steven D. Levitt, *Using Electoral Cycles in Police Hiring to Estimate the Effect of Police on Crime*, 87 AMER. ECON. REV. 270 (1997); AARON CHALFIN & JUSTIN MCCRARY, U. C. BERKELEY, THE EFFECT OF POLICE ON CRIME: NEW EVIDENCE FROM U.S. CITIES, 1960–2010 (2012).

crime neighborhoods, or hot spots.[62] A strong body of empirical case studies shows that such hot spot policing can reduce, and not merely displace, crime.[63]

All of these theories of crime reduction rely upon a principal assumption: police cannot be everywhere at once. Thus, scholars in this field try to find methods to improve the efficiency of police activity. The digitally efficient investigative state radically shifts this fundamental assumption of policing and crime control theory. Early quantitative studies on the effects of digitally efficient technologies have returned mixed results on its crime fighting abilities.[64] But if these technologies do become tools for deterrence, investigation, and criminal apprehension, their crime fighting ability will be virtually unmatched by any other technological development in recent history.

Legal scholars and policymakers should look at this trend in policing innovation as a potential tool for both crime control and a source of potential widespread privacy violations. A growing body of evidence confirms that law enforcement uses these surveillance technologies to target minority groups.[65] Psychological and historical evidence suggests that the availability of pervasive surveillance tools may facilitate law enforcement corruption.[66] With the unregulated ability to monitor an entire community, law enforcement may be incentivized to conduct fishing expeditions that "exacerbate racism, stereotyping, or profiling."[67] This elevates the risk of false positives and harms citizens' perceptions of procedural fairness.[68] Thus, while the digitally efficient investigative state may be an important development for crime prevention, it also raises numerous privacy concerns.

---

[62] *See generally* David Weisburd & Anthony A. Braga, *Hot Spots Policing as a Model for Police Innovation*, *in* POLICE INNOVATION 225 (2006).

[63] *See, e.g.*, Anthony A. Braga, *Hot Spots Policing and Crime Prevention: A Systematic Review of Randomized Controlled Trials*, 1 J. EXPERIMENTAL CRIMINOLOGY 317 (2005) (finding that the majority of empirical studies support the effectiveness of hot spot policing).

[64] *Compare* Jennifer King et al., *Fighting Crime with Publicly-Financed Surveillance Cameras: The San Francisco Experience*, CAL. POL'Y OPTIONS 2009 145, 158 (2009), *available at* http://www.spa.ucla.edu/webfiles/doc/116679final.pdf (explaining how the installation of 19 surveillance cameras in San Francisco correlated with a subsequent reduction in crime), *with* LUM ET AL., *supra* note 34, at 27-59 (finding that ALPR devices had no significant effect on crime in a single case study).

[65] *See* Rushin, *supra* note 8, at 299.

[66] *Id.* at 300-01.

[67] *Id.* at 300.

[68] *See id.* at 301-02.

B. Empirical Evidence on the Scope of Surveillance Technologies

Despite the importance of the digitally efficient investigative state, no comprehensive research has fully documented the extent to which police departments across the country have adopted these new surveillance technologies. To better illustrate the magnitude of the digitally efficient investigative state, I have gathered survey data from four sources: (1) the Law Enforcement Management and Administration Statistics (LEMAS), (2) the International Association of Chiefs of Police (IACP), (3) the Police Executive Research Forum (PERF), and (4) independent surveys conducted by academics researching police organizations.

The Bureau of Justice Statistics (BJS) publishes the LEMAS data every three to four years as part of a comprehensive survey of approximately 3,000 state and local law enforcement agencies.[69] Because the BJS conducts the LEMAS survey semi-regularly, this data set is useful for observing changes over time in police behavior. But the BJS survey data only gives information on the current use of various surveillance technologies. So far, the BJS has not collected data on departmental policies on surveillance data retention.

The data from the IACP and PERF comes from a handful of one-time surveys. Fewer departments respond to IACP and PERF surveys than BJS requests. Nonetheless, the IACP and PERF studies often include detailed questions on departments' data retention, usage, and access policies—something the LEMAS study lacks. The IACP and PERF surveys also have included information on future plans for the technology and law enforcement departments' participation in regional data sharing.

1. Surveillance Cameras and Biometric Recognition

Surveillance cameras are nearly ubiquitous in American police departments. According to the 1997 LEMAS survey, nearly 700—or approximately 20% of all departments responding to the question—reported using some type of surveillance cameras.[70] In the following decade, the percentage of departments increased

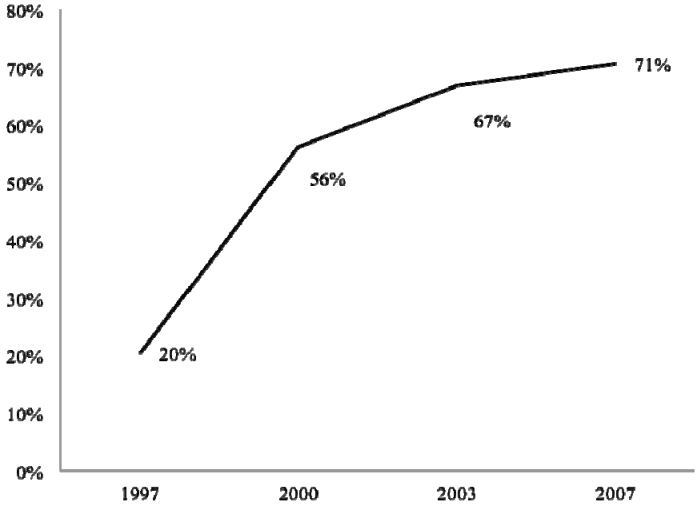
---

[69] U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, DATA COLLECTION: LAW ENFORCEMENT MANAGEMENT AND ADMINISTRATIVE STATISTICS, *available at* http://bjs.ojp.usdoj.gov/index.cfm?ty=dcdetail&iid=248 (last visited Aug. 28, 2013).

[70] LEMAS 1997, *supra* note 1.

dramatically to 56% in 2000, 67% in 2003, and 71% in 2007.[71] Between 1997 and 2007, the number of departments using surveillance cameras increased by 189%. The IACP study similarly found that departments regularly employed surveillance cameras. In a 2001 survey of 207 police agencies, around 80% claimed to use some type of surveillance camera.[72] Although the IACP survey found that a higher number of departments used surveillance cameras around the turn of the century than the LEMAS survey, this discrepancy can be traced to the demographic profiles of the departments responding to each survey instrument.[73] It is safe to say that, while surveillance cameras were relatively rare two decades ago, they are extremely common today. Figure 1 shows the historical trend in police use of surveillance cameras over time.

FIGURE 1, PERCENTAGE OF POLICE DEPARTMENTS USING ANY CAMERA SURVEILLANCE[74]



[71] U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, LAW ENFORCEMENT MANAGEMENT AND ADMINISTRATIVE STATISTICS (LEMAS): 2000 SAMPLE SURVEYS OF LAW ENFORCEMENT AGENCIES (2000) [hereinafter LEMAS 2000], *available at* http://www.icpsr.umich.edu/icpsrweb/NACJD/series/92/studies/3565; U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, LAW ENFORCEMENT MANAGEMENT AND ADMINISTRATIVE STATISTICS (LEMAS): 2003 SAMPLE SURVEYS OF LAW ENFORCEMENT AGENCIES (2003) [hereinafter LEMAS 2003], *available at* http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/04411; LEMAS 2007, *supra* note 2.

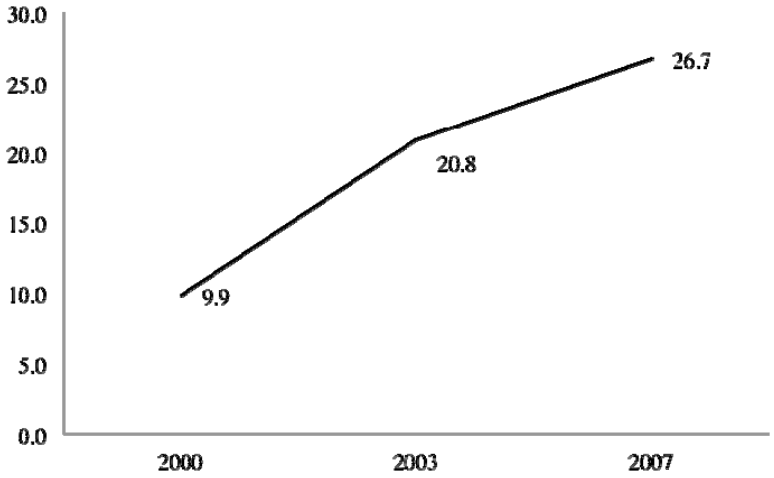
[72] LAURA J. NICHOLS, INT'L ASS'N OF CHIEFS OF POLICE, CUTTING EDGE OF TECHNOLOGY EXECUTIVE BRIEF: THE USE OF CCTV/VIDEO CAMERAS IN LAW ENFORCEMENT 4, 15 (2001).

[73] *See id.* at 14 (explaining the breakdown of the survey pool—including the relative amount of larger departments surveyed).

[74] LEMAS 2007, *supra* note 2; LEMAS 2003, *supra* note 71; LEMAS 2000, *supra* note 71; LEMAS 1997, *supra* note 1. In calculating the data for Figure 1, I group

The actual number of surveillance cameras used by individual departments also varies widely from one department to the next. But overall, the number of cameras employed by the average American police department has increased steadily over the last decade. The LEMAS survey first kept records on the number of surveillance cameras used by departments in 2000, when the average department reported employing around 10 surveillance cameras.[75] The police in the United States in 2000 operated just under 30,000 total cameras.[76] By 2007, the average department utilized nearly 27 cameras, or a total of nearly 77,000 nationwide.[77] This represents a 161% increase in total cameras and a 170% increase in cameras per department over a mere seven-year period. Figure 2 graphically illustrates the trend in the average number of surveillance cameras per department over a 10 year period.

FIGURE 2, AVERAGE NUMBER OF SURVEILLANCE CAMERAS PER DEPARTMENT[78]



The LEMAS data may also dramatically underestimate the actual number of surveillance cameras used by police in the United States. Many cities, like Chicago, give police access to an integrated network of surveillance cameras—public transit cameras, police cameras, and school cameras. Estimates range

together in this calculation three categories of surveillance cameras: fixed cameras, mobile cameras, and cameras mounted on squad cars.

[75] LEMAS 2000, *supra* note 71.

[76] *Id.*

[77] LEMAS 2007, *supra* note 2.

[78] *Id.*; LEMAS 2003, *supra* note 71; LEMAS 2000, *supra* note 71.

from 8,000[79] cameras to 15,000[80] cameras. When responding to the LEMAS survey, Chicago reported use of only 1,073 cameras in 2007.[81] In all likelihood, this number only represents the number of cameras installed and operated exclusively by police—not the number of cameras used by the city and monitored in some manner by law enforcement. Thus, the LEMAS conclusions almost certainly underestimate the actual number of cameras that police access regularly.

In other IACP surveys, police departments have also rated surveillance cameras as among the highest priority targets for continued technological investment. A 2005 study of 47 law enforcement departments asked administrators to rate the relative importance of future investments in different investigative technologies.[82] Video cameras were among the top five most important sources for future technological investment.[83]

Overall, biometric recognition systems, like facial recognition, seem to be rarely used by the average police department. In the LEMAS survey, only 191 departments claimed to use the technology in 2003 and 98 in 2007.[84] But according to the IACP study, departments indicated a significant interest in investing in facial recognition technology in the future.[85] In addition, the majority of law enforcement administrators believe facial recognition will be of high value to departments in the future.[86]

2. Automatic License Plate Readers (ALPR)

There is less historical data on the adoption of ALPR devices. The LEMAS surveys only recently started asking departments about their use of ALPR. The 2007 LEMAS survey was the first. Only 170 departments or about 19% of those agencies that responded to the survey question claimed

---

[79] NANCY G. LA VINGE ET AL., URBAN INST., EVALUATING THE USE OF PUBLIC SURVEILLANCE CAMERAS FOR CRIME CONTROL AND PREVENTION—A SUMMARY 2 (2011).

[80] Police Exec. Research Forum, *How Are Innovations in Technology Transforming Policing?*, *in* CRITICAL ISSUES IN POLICING SERIES 13 (2012) [hereinafter PERF].

[81] LEMAS 2007, *supra* note 2.

[82] INT'L ASS'N OF CHIEFS OF POLICE, LAW ENFORCEMENT PRIORITIES FOR PUBLIC SAFETY: IDENTIFYING CRITICAL TECHNOLOGY NEEDS 2-3 (2005) [hereinafter IACP CRITICAL TECH. NEEDS].

[83] *Id.* at 3.

[84] LEMAS 2003, *supra* note 71; LEMAS 2007, *supra* note 2. It is unclear why exactly the number of departments that use biometric technology has not increased like other technologies.

[85] IACP CRITICAL TECH. NEEDS, *supra* note 82, at 7 (noting that among the categories of video cameras and biometric technologies, respondents placed fixed surveillance cameras and facial recognition at the top of their relative priority lists).

[86] *See* NICHOLS, *supra* note 72, at 13.

to use ALPR in some capacity.[87] While this initially suggests that ALPR is relatively uncommon in the United States, the breakdown of ALPR by city reveals that large cities commonly employ ALPR. Approximately 48% of departments with over 1,000 sworn officers utilize ALPR, compared to 32% of departments with between 501 and 1,000 officers, and 19% of those with between 251 and 500 sworn employees.[88] California, New York, and Florida had the most agencies that claim to use ALPR, with Texas, Virginia, Colorado, and Georgia not far behind.[89]

Since the LEMAS data came out, three other surveys have attempted to document the use of ALPR in American police agencies. The IACP published the first of these post-LEMAS studies in 2009 after surveying 444 law enforcement departments in the United States. Of the 305 that responded, 23% reported using ALPR.[90] Like LEMAS, the IACP designed the survey to carefully consider the effect of police organization size on ALPR adoption. Table 1 breaks down ALPR usage by department size.

TABLE 1, 2007 LEMAS AND 2009 IACP REPORTED ALPR USAGE BY DEPARTMENT SIZE[91]

	Percentage Using ALPR	
Department Size	**LEMAS (2007)**	**IACP (2009)**
51+	18.8%	34.0%
101+	19.7%	41.3%
251+	29.1%	52.2%
501+	40.6%	66.0%
1001+	48.1%	80.0%

The sample size of those responding to the IACP survey was smaller than the LEMAS survey, which might partially explain the variation. Nonetheless, the IACP numbers build a compelling case that the usage of ALPR is increasing. In a more recent study, Cynthia Lum, Linda Merola, Julie Willis,

---

87 ROBERTS & CASANOVA, *supra* note 56, at 6; LEMAS 2007, *supra* note 2.
88 ROBERTS & CASANOVA, *supra* note 56, at 6.
89 *Id.*
90 *Id.* at 19.
91 ROBERTS & CASANOVA, *supra* note 56; LEMAS 2007, *supra* note 2.

and Breanne Cave surveyed a random but statistically representative sample of 200 police departments.[92] Of the 169 departments that responded, Lum et al. found that 21% used ALPR.[93] Among larger departments of 100 sworn officers or more, the number increased to 37%.[94] This generally comports with the IACP and LEMAS findings. Like the IACP report, Lum et al.'s study finds convincing evidence that ALPR usage has increased since the 2007 LEMAS report, and that ALPR usage depends in large part on department size.

The most recent research on the subject comes from a 2011 survey conducted by PERF. They found that 71% of responding agencies currently use ALPR and 85% of administrators plan to acquire more ALPR devices or increase use in the future.[95] Again, it is worth noting that the sample size in the PERF survey was only 70 agencies—not quite as large as the Lum et al. study and significantly smaller than LEMAS.[96] The distribution of the PERF sample also skews heavily toward large departments.[97] This possibly affects the overall findings, and results in a disproportionately large percentage of departments that report ALPR usage compared to the other surveys. But even when accounting for the somewhat skewed sample, the results are strong evidence that departments have increased ALPR adoption in recent years. Respondents to the PERF survey instrument also noted that they expected to equip 25% of all squad cars in their department with ALPR devices in the next five years.[98]

The LEMAS and PERF reports do not provide detailed information on the exact number of ALPR systems deployed per department, but media reports have uncovered detailed information about the heavy distribution of ALPR devices in some of America's largest cities. The District of Columbia and surrounding suburbs currently operate over 250 ALPR devices.[99]

---

[92] LUM ET AL., *supra* note 34, at 13-14.

[93] *Id.* at 19.

[94] *Id.* at 18-19.

[95] PERF, *supra* note 80, at 1-2.

[96] POLICE EXECUTIVE RESEARCH FORUM, USE OF TECHNOLOGY IN POLICING: THE CHIEF'S PERSPECTIVE 9 (2011) [hereinafter PERF CHIEF'S PERSPECTIVE], *available at* http://www.policeforum.org/library/critical-issues-in-policing-series/perfpresentation.pdf.

[97] *Id.* at 3. Further, the median size of the department using ALPR in the PERF study was 336 sworn officers. ROBERTS & CASANOVA, *supra* note 56, at 7. Thus, the PERF sample size appears to be skewed toward large departments.

[98] PERF CHIEF'S PERSPECTIVE, *supra* note 96, at 9.

[99] Allison Klein & Josh White, *License Plate Readers: A Useful Tool for Police Comes with Privacy Concerns*, WASH. POST (Nov. 19, 2011), *available at* http://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_story.html.

The state of Maryland has installed around 300 devices statewide.[100] New York City had installed 238 by 2011.[101] Dallas plans to use somewhere between 48 to 68 systems in the near future.[102] This rapid proliferation was predictable. As early as 2005, a survey of law enforcement conducted by the IACP found that police administrators rated ALPR as the highest priority locational and global position technology for future investment.[103] Overall, the body of evidence on ALPR suggests that the technology is becoming common in American law enforcement agencies.

In sum, the data from these various sources generally reveal two major trends about the adoption of digitally efficient surveillance technology. First, digitally efficient surveillance technologies are becoming ubiquitous among American police departments—particularly in large, urban departments. Second, this rapid transformation in policing technology has happened in a relatively short period of time. This should come as no surprise. Given the potential criminological and cost benefits of digitally efficient surveillance technologies, departments should be investing in these types of technologies. The next logical question is whether and how departments have internally regulated these technologies after adoption. The next section will summarize the limited empirical work on the state of internal departmental regulations.

C. The State of Internal Departmental Regulations

The empirical evidence on the scope of the digitally efficient investigative state paints a clear and persuasive picture—digitally efficient technologies are becoming increasingly common, particularly in large police departments. This means that departments are often collecting enormous amounts of data on a daily basis. Police agencies in Southern California, for instance, have amassed over 160 million data points from the use of ALPR alone.[104] Fundamental to the emergence of the digitally efficient investigative state is the ability to retain

---

[100] ROBERTS & CASANOVA, *supra* note 56, at 28.

[101] Al Baker, *Camera Scans of Car Plates Are Reshaping Police Inquiries*, N.Y. TIMES, Apr. 12, 2011, at A17, *available at* http://www.nytimes.com/2011/04/12/nyregion/12plates.html.

[102] CITY OF DALL., TEX., REQUEST FOR COMPETITIVE SEALED PROPOSAL: DPD MOBILE AND FIXED AUTOMATIC LICENSE PLATE RECOGNITION (ALPR) SYSTEM 2-4 (2012); ROBERTS & CASANOVA, *supra* note 56, at 28.

[103] IACP CRITICAL TECH. NEEDS, *supra* note 82, at 7.

[104] Jon Campbell, *License Plate Recognition Logs Our Lives Long Before We Sin*, L.A. WEEKLY (June 21, 2012), http://www.laweekly.com/2012-06-21/news/license-plate-recognition-tracks-los-angeles/.

large amounts of data due to improving technological feasibility and decreased cost.[105] This means that law enforcement agencies collect data on all recorded activity, not just suspicious or criminal behavior.

Departments have every incentive to keep as much data as possible, if that data could be useful in any way to a future criminal investigation. But the possibility of unregulated data retention on innocent people raises serious privacy concerns.[106] Without regulation, historical and psychological evidence indicates that unregulated surveillance data retention may allow the state to target unpopular minority groups for unjustified surveillance, increase the likelihood of corruption, and facilitate fishing expeditions that could eventually disrupt the lives of the innocent.[107]

New evidence suggests that departments have implemented vastly different internal regulations on the use, retention, and access to data acquired from digitally efficient technologies. The overwhelming majority of departments use these technologies not just for observational comparison, but also indiscriminate data collection. Some departments keep data for a matter of days, while others retain it indefinitely. The BJS does not ask departments about data retention policies in the LEMAS surveys. Thus, the best information on data retention by American law enforcement comes from the pair of studies done on ALPR and surveillance cameras by the IACP in 2001 and 2009 respectively. According to these reports, 96% of departments using surveillance cameras, and 95% of those using ALPR engage in some kind of indiscriminate data collection—not just observational comparison.[108]

Among departments that take part in the practice of indiscriminate data collection, the length of retention varies widely. Among departments using surveillance cameras, the vast majority retain video footage for over a month.[109] Of course, the IACP completed this survey on surveillance cameras over a decade ago, when long-term data storage was less feasible. We may expect that today, departments can affordably store video footage for even longer periods of time.

---

[105] *See supra* Part I.A.

[106] *See* Rushin, *supra* note 8, at 299-302.

[107] *Id.*

[108] NICHOLS, *supra* note 72, at 9 (defining observational comparison as the presence of a formalized policy permitting no storage of data, according to figure 10); ROBERTS & CASANOVA, *supra* note 56, at 29 (defining observational comparison as the presence of a formalized policing permitting no storage of data, according to table 18).

[109] NICHOLS, *supra* note 72, at 9.

Table 2 summarizes the IACP data on surveillance camera data retention.

TABLE 2, 2001 IACP DATA ON SURVEILLANCE CAMERA DATA RETENTION

Maximum Retention	Percentage
Observational Comparison	4%
1 day	2%
7 days	3%
30 days	20%
Over 30 days	71%

The IACP also found that a significant number of departments outsourced the operation of police surveillance cameras, as well as the storage and maintenance of data. Around 47% of all camera operators were found to be sworn police officers.[110] Furthermore, while surveillance camera data is generally stored at police facilities, the responsibility for maintenance, collection, and disposal of data falls to non-police officers in 43% of departments.[111]

As for ALPR locational data, the typical department retained data for between two and six months.[112] But a very substantial portion of police departments—around 28%—admit to having either no policy limiting data retention, or having a departmental policy that mandates indefinite retention.[113] Table 3 aggregates the IACP findings on ALPR data retention.

---

[110] *Id.* at 8 (noting in figure 7 that only 53% of operators are police officers).

[111] *Id.* (noting in figure 6 that only 57% of the departments have police manage data, but noting in figure 9 that in 90% of agencies the data is stored at police facilities).

[112] ROBERTS & CASANOVA, *supra* note 56, at 29. I define the typical department as the median department responding to the survey. Although the data is not broken down by case, we can surmise from table 18 that the median is somewhere between two and six months.

[113] *Id.*

TABLE 3, 2009 IACP DATA ON ALPR DATA RETENTION

Maximum Retention	Percentage
Only observational comparison	6%
0-30 days	22%
2-6 months	22%
1 year	6%
2 years	6%
3-5 years	9%
Potentially indefinite detention or no formalized policy	28%

Civil rights advocates have also attempted to gather more up-to-date information on data retention policies by filing Freedom of Information Act (FOIA) requests with departments all across the country. The ACLU has led this charge by filing 587 requests in 38 states.[114] So far, the ACLU has received responses from 293 departments.[115] Although the ACLU has not yet released the full extent of their data, they have observed that retention policies vary widely from one jurisdiction to the next.[116] Departments commonly keep data for several years, with many departments keeping retained data indefinitely when possible.[117]

While some departments have proactively established internal policies to regulate the use of these technologies, many have not. Further, internal policies on data access, retention, and sharing differ dramatically from one department to the next.

---

[114] Am. Civil Liberties Union, *You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements* (July 17, 2013), https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record.

[115] *Id.* at 3.

[116] *Id.* at 20.

[117] *Id.*

II. THE LAW OF POLICE SURVEILLANCE

Traditionally, courts have shied away from regulating police surveillance in public spaces. This is because the courts have operated under a set of jurisprudential assumptions of police surveillance. These jurisprudential assumptions were reasonable in the past because of the limited technological efficiency of previous surveillance technologies. In *Jones*, the Supreme Court had the opportunity to confront these jurisprudential assumptions in light of modern technology. A majority of the justices indicated that these jurisprudential assumptions were increasingly unsupportable in today's digitally efficient world of policing.[118] But the Court did not alter these doctrinal assumptions in any way, nor did they offer much indication on how they may alter these assumptions in the future. Thus, after the *Jones* decision, the law of police surveillance today is as incoherent as ever.

I have previously argued that the digitally efficient investigative state does not run afoul of the Fourth Amendment, based on the presence of these jurisprudential assumptions,[119] but dicta in the concurrences of the *Jones* case imply that these jurisprudential assumptions may not exist for much longer. Even so, there is no clear indication how the Court could establish a default rule that both narrowly limits some uses of digitally efficient technologies without adversely affecting other non-invasive, legitimate uses.

In this section, I evaluate the doctrinal basis for the traditional jurisprudential assumptions about police surveillance. I then spend considerable time analyzing the dicta in the *Jones* case to predict how the Court may respond to these technologies in the future. I conclude that, while the Court will likely make some effort to rein in the digitally efficient investigative state in the future, any regulation will be limited in capacity. The regulation will almost certainly rely upon an often-ineffective enforcement tool like the exclusionary rule. Thus, even if the judiciary is institutionally capable of controlling the digitally efficient investigative state, the legislature must also take a proactive role in any future regulation.

---

[118] *See* United States v. Jones, 132 S. Ct. 945, 955-64 (2012) (Sotomayor, J., concurring and Alito, J., concurring) (both concurrences finding support for a broad doctrinal shift in the treatment of technological surveillance).

[119] Rushin, *supra* note 8, at 309-13.

A. The Fourth Amendment and Privacy

Almost all legal challenges to surveillance, including the challenge levied in *Jones*, claim that government surveillance amounts to an unreasonable search or seizure in violation of the Fourth Amendment of the United States Constitution. The Fourth Amendment does not bar all searches; instead it merely protects against unreasonable searches and seizures by government agents.[120] In judging whether a tactic qualifies as an unreasonable search or seizure, the Court generally uses a test originally developed in Justice Harlan's concurrence in *Katz v. United States*.[121] This test asks whether the action violates a person's reasonable expectation of privacy.[122] An act violates a person's reasonable expectation of privacy if the person "exhibited an actual (subjective) expectation of privacy," and such an expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[123]

The Court grappled with the jurisprudence of police surveillance for many decades before adopting the *Katz* standard. In a 1928 case, *Olmstead v. United States*, federal prohibition officers used an early version of a wiretap to listen in on the conversation of a criminal suspect.[124] The officers did not obtain a warrant before using the device.[125] Using this technology, law enforcement listened to the suspect's conversations for many months.[126] They then used the conversations as evidence to justify an arrest and later conviction.[127] The Court upheld this wireless wiretapping as constitutional, arguing that the practice involved no physical intrusion into the person's home or seizure of tangible property.[128] The Court compared phone lines to public highways, noting that the phone lines "are not part of his house or office any more than are the highways along which they are stretched."[129] Thus, after *Olmstead*, the Fourth Amendment did not protect against technological surveillance unless the technology

---

[120] U.S. CONST. amend. IV.

[121] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[122] *Id.*

[123] *Id.*; *See also* California v. Ciraolo, 476 U.S. 207, 211 (1986) (applying Justice Harlan's two-prong test).

[124] Olmstead v. United States, 277 U.S. 438, 456-57 (1928), *overruled by* Katz v. United States, 389 U.S. 347, 352-53 (1967).

[125] *Id.* at 442-43.

[126] *Id.* at 457.

[127] *Id.*

[128] *Id.* at 466.

[129] *Id.* at 465.

somehow tangibly intruded in a protected place.[130] The Court honored this rigid view of the Fourth Amendment for nearly four decades, permitting law enforcement to use other surveillance technologies like detectaphones[131] and wiretaps without a warrant.

The Court finally reversed track in 1967 in *Katz v. United States*.[132] There, police surreptitiously attached a listening device to a public telephone booth and listened to the conversations of a suspected gambler.[133] Katz appealed his conviction by arguing that the use of a listening device inside a phone booth violated the Fourth Amendment.[134] The Court agreed with Katz, finding that the use of a warrantless wiretapping device on a public phone violated the Fourth Amendment because the "Fourth Amendment protects people, not places, from unreasonable searches and seizures."[135] Even though the police never physically invaded Katz's personal property, and even though Katz was using a public phone booth, the Court concluded that he had a reasonable expectation that his words would not be "broadcast to the world."[136] Justice Harlan's concurrence in *Katz* set out a two-prong test to determine whether the action of a state agent violates the bar on unreasonable searches and seizures. According to Harlan, courts should ask (1) whether a person exhibited a subjective expectation of privacy, and (2) whether society is ready to recognize that subjective expectation as reasonable.[137] In later cases, including *Jones*, the Court has relied on this test to determine whether a police surveillance technology requires a warrant before use.

B. The Jurisprudential Assumptions of Police Surveillance

In applying the *Katz* test to emerging surveillance technologies the Court has relied on two important jurisprudential assumptions: first, an individual has no reasonable expectation of privacy in anything they expose to the public or a third party, and second, policing technologies that

---

[130] Hutchins, *supra* note 12, at 424 (noting that *Olmstead* "recognized a new constitutional threshold for Fourth Amendment protection—tangible physical intrusion by the government").

[131] Goldman v. United States, 316 U.S. 129, 135-36 (1942) (holding that the use of a detectaphone to listen to a defendant's conversation through an adjoining wall did not require a warrant before use).

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

[133] *Id.* at 354-55 n.14.

[134] *Id.* at 348-49.

[135] Rushin, *supra* note 8, at 305.

[136] *Katz*, 389 U.S. at 352.

[137] *Id.* at 361 (Harland, J., concurring).

merely improve the efficiency of otherwise legal policing tactics do not violate a person's reasonable expectation of privacy. Each of these assumptions was once defensible, but decreasingly so in our technologically efficient state.

1. Assumption One: No Reasonable Expectation of Privacy in Actions Exposed to Others

The first major assumption of police surveillance law is that an individual has no reasonable expectation of privacy in anything they expose to the public or a third party. Historically, the Court has relied on this assumption as a fundamental building block for numerous jurisprudential doctrines, including the open fields doctrine, the third party doctrine, and the misplaced trust doctrine. Today, this assumption grounds the belief that police can observe and record all public behavior—whether that surveillance comes in the form of aerial observation,[138] surveillance of driving movements,[139] or through the use of some other digitally efficient technology.

One of the earliest judicial default rules premised on this presumption is the open fields doctrine.[140] Established in *Hester v. United States*[141] and later reaffirmed in *Oliver v. United States*,[142] this doctrine clarified that individuals have no reasonable or constitutionally protected expectation of privacy in open fields. For example, in *Hester*, two state agents trespassed onto a criminal suspect's land and observed him in possession of illegal alcohol.[143] The Court held that, even if the officers had unlawfully trespassed onto the suspect's land, the subsequent observation of liquor was not an unreasonable search in violation of the Fourth Amendment.[144] The agents made these observations from an open field, and the Court held that a person has no reasonable expectation of privacy in observations made from an open field.[145] The Court reaffirmed the open fields doctrine in 1984 in *Oliver*. There the justices found that the open field doctrine does not conflict with the two-prong test handed down in *Katz*.[146] Individuals do not have

---

[138] Florida v. Riley, 488 U.S. 445 (1989); Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

[139] United States v. Knotts, 460 U.S. 276 (1983).

[140] Hester v. United States, 265 U.S. 57, 58 (1924).

[141] *Id.* at 59.

[142] 466 U.S. 170, 179 (1984).

[143] *Hester*, 265 U.S. at 57-58.

[144] *Id.* at 58-59.

[145] *Id.*

[146] *Oliver*, 466 U.S. at 179.

a reasonable expectation of privacy in actions executed in open fields because they cannot reasonably expect that such actions will be free from "government interference or surveillance."[147]

Implicit in the open fields doctrine is a notion that individuals should not expect privacy in such environments because such locations are often visible to other people. Thus, the open fields doctrine is premised upon a conception of privacy that rigidly distinguishes between private and public. When people make any action public through committing it in a potentially public environment, such as an open field, they thereby expose that behavior to the world. In such scenarios, the Court has historically held that the person loses any reasonable expectation of privacy.

The third-party doctrine also relies on a belief that all information exposed to others deserves no protection under the Fourth Amendment. In *United States v. Miller*, the Bureau of Alcohol, Tobacco, and Firearms (ATF) acquired bank records related to Miller's alcohol distillery.[148] The Court held that the ATF did not need a warrant to obtain Miller's bank records because the records contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[149] Thus, *Miller* stands for the proposition that, even when a person turns over records to a third party for a limited purpose, he assumes the risk that the third party will reveal those records to law enforcement.[150] The Court has since reaffirmed this rule in various different scenarios, including in *Smith v. Maryland*. There, police installed a device known as a pen register on a criminal suspect's phone without a warrant.[151] The pen register gave law enforcement a record of every phone number the suspect dialed.[152] The Court found this kind of law enforcement tactic constitutional because it merely recorded the numbers dialed, not the content of the communications. While a person has a reasonable expectation of privacy in their communications over a telephone, they should realize that a phone company has a legitimate business need to record numbers dialed.[153] Thus, by using a telephone, users should reasonably expect that a third party is or could be compiling data on the numbers they dial.[154] In such situations,

---

147 *Id.*
148 United States v. Miller, 425 U.S. 435, 437-39 (1976).
149 *Id.* at 442.
150 *Id.* at 443.
151 Smith v. Maryland, 442 U.S. 735, 737, 745-46 (1979).
152 *Id.*
153 *Id.* at 743.
154 *Id.* at 745-46.

"a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[155]

The misplaced trust doctrine similarly rests on a presumption that individuals risk observation and investigation every time they reveal any words or behaviors to third parties. Soon after *Katz*, the Court held in *United States v. White* that police could legally record conversations between informants and criminal suspects without a warrant; even if a person has every reason to trust that the information shared will be private, he cannot reasonably be certain that such information will stay private.[156] Even if that suspect has a misplaced trust in the informant, the suspect assumes the risk by conveying personal information. This reaffirmed the Court's holding from an earlier case, *Hoffa v. United States*, that stated that "[t]he risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak."[157] Whether you turn over bank records to a financial assistant, [158] phone numbers to a phone company, [159] or confidential information to a supposed friend, [160] you lose virtually any reasonable expectation of privacy. Similarly, if your actions end up being visible to other people,[161] even on your own property, you cannot reasonably expect privacy.

The Court has continued to adhere to this jurisprudential assumption in cases involving advanced technological surveillance by law enforcement. Three of the most prominent pre-*Jones* cases involving technologically advanced police surveillance mechanisms, *Florida v. Riley*, [162] *Dow Chemical Company v. United States*,[163] and *United States v. Knotts*,[164] all appear to abide by this jurisprudential assumption.

The *Riley* case involved a police helicopter that flew approximately 400 feet above a suspect's greenhouse.[165] The owner had partially enclosed the greenhouse and covered the

---

[155] *Id.* at 743-44.

[156] United States v. White, 401 U.S. 745, 751-53 (1971).

[157] Hoffa v. United States, 385 U.S. 293, 303 (1966) (quoting . Lopez v. United States, 373 U.S. 427, 465 (1963) (Warren, J., dissenting)).

[158] United States v. Miller, 425 U.S. 435, 443 (1976).

[159] *Smith*, 442 U.S. at 743-44.

[160] *Hoffa*, 385 U.S. at 303.

[161] Oliver v. United States, 466 U.S. 170, 179 (1984).

[162] 488 U.S. 445 (1989).

[163] 476 U.S. 227 (1986).

[164] 460 U.S. 276 (1983).

[165] *Riley*, 488 U.S. at 448-49.

top of the greenhouse with corrugated roof panels.[166] Some of these panels were clear, some opaque.[167] The owner had only left about 10% of the roof uncovered by roofing panels.[168] By flying over this structure in a helicopter, a police officer could visually identify marijuana growing inside the greenhouse.[169] The Court ruled that, because the owner would reasonably expect there to be air traffic over this greenhouse, he had to reasonably expect that aircraft flying over the structure could see inside.[170] Adhering to the first assumption of police surveillance law, the Court rejected the suspect's privacy claim on the basis that he had implicitly made his marijuana farm public to those flying above.

The Court reached a very similar conclusion in *Dow Chemical*.[171] In that case, the Environmental Protection Agency (EPA) used an aerial camera to photograph a manufacturing facility in Midland, Michigan.[172] The aircraft never left navigable airspace and took photographs from between 1,200 and 12,000 feet.[173] The camera allowed the EPA to gain an extremely close-up look at details in the facility—"a great deal more than the human eye could ever see."[174] Even so, the resultant pictures were not significantly distinguishable from those used to make maps.[175] While Dow has a reasonable expectation of privacy inside its building facilities, the Court determined that the outside of the facility—particularly when viewed from above—is more akin to an open field.[176] This means that "observation of persons in aircraft lawfully in the public airspace immediately above or sufficiently near the area" does not offend the Fourth Amendment.[177]

Finally, in *Knotts*, the Court upheld the use of a warrantless radio transmitter tracking device installed inside a chemical drum purchased by a criminal suspect. Police believed that the suspect was using certain chemicals in the production of illegal substances.[178] With the permission of the chemical company, police installed the tracking device on a chloroform

---

166 *Id.* at 448.
167 *Id.*
168 *Id.*
169 *Id.*
170 *Id.* at 450-51.
171 Dow Chem. Co. v. United States, 476 U.S. 227 (1986).
172 *Id.* at 229.
173 *Id.*
174 *Id.* at 230.
175 *Id.* at 232.
176 *Id.* at 239.
177 *Id.*
178 United States v. Knotts, 460 U.S. 276, 278 (1983).

container before the chemical company handed it over to the suspect.[179] The officers then used a radio receiver to acquire occasional signals emitted by the tracker; these signals helped the officials generally follow the suspect, but did not reveal his precise location in the way GPS can today.[180] The officers used this device to establish probable cause for a warrant.[181] Upon executing the warrant, police discovered that the suspect was part of an extensive methamphetamine laboratory.[182] The suspect challenged his conviction by claiming that the tracking device violated his reasonable expectation of privacy.[183] The Court rejected his claim, arguing that the suspect had a diminished expectation of privacy in an automobile on a public thoroughfare.[184] The court reasoned that when a car travels in public, "both its occupants and its contents are in plain view";[185] the suspect's "direction[,] . . . stops . . . and . . . final destination" were all "voluntarily conveyed to anyone who wanted to look."[186] Consequently, the Court upheld the admission of evidence acquired via the tracking device.[187]

In sum, the Court has tightly honored the traditional assumption that anything exposed to the public is presumptively outside the bounds of Fourth Amendment protection. Such an assumption has traditionally been workable given the limited scope of investigative technologies. Surveillance technologies—be they aerial photography or radio transmitters—could only collect information on a limited number of suspects over a limited period of time. Police were forced to choose which suspects to surveil, thereby limiting the overall scope of public surveillance efforts. As the digitally efficient investigative state grows in strength, however, this assumption is becoming dangerously unsupportable.

2. Assumption Two: The Courts Should Not Limit Police Efficiency

The second major jurisprudential assumption of police surveillance is that policing technologies that merely improve the efficiency of otherwise legal policing tactics do not violate a

---

179 *Id.* at 278.
180 *Id.*
181 *Id.* at 279.
182 *Id.*
183 *Id.*
184 *Id.* at 281.
185 *Id.* (internal citations omitted).
186 *Id.*
187 *Id.* at 282.

person's reasonable expectation of privacy. These efficiency-enhancing technologies are typically contrasted with technologies that give police a pervasive, extrasensory ability. The Court has long displayed a reluctance to regulate police efficiency. As early as *Dow Chemical*, the Court was quick to note that, although an aerial camera can get a very precise view of images below, "[t]he photographs were not so revealing of intimate details as to raise constitutional concerns. The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."[188] Indeed, the Court has long distinguished between sense-enhancing technologies and extrasensory technologies.[189] While the Court has restricted the use of certain extrasensory technologies, it has been reluctant to restrict any technologies that merely improve the efficiency of otherwise legitimate police surveillance techniques.

The *United States v. Kyllo*[190] case typifies the Court's approach to extrasensory technology, while the *White*[191] and *Knotts*[192] cases are examples of the Court's deference toward efficiency-enhancing technologies. In *Kyllo*, law enforcement officials suspected the defendant of growing marijuana in his home by using high-intensity lamps.[193] Police knew that such high-intensity lamps would produce a significant amount of heat.[194] From the outside of the house, an officer used a heat-sensing device to scan the inside of the defendant's house.[195] The device was capable of showing differences in heat within the house.[196] The officer found that the home's garage was substantially warmer than the rest of the house, which was consistent with the growing of marijuana via indoor heat lamps.[197] Based on this information, police obtained a warrant to search the home and found marijuana inside the garage, which was used to secure a conviction.[198] The defendant

---

[188] Dow Chem. Co. v. United States, 476 U.S. 227, 228 (1986).

[189] *See generally* Hutchins, *supra* note 12, at 433-38 (describing the difference between sense-augmenting and extrasensory technologies); Nicholas J. Heydt, Comment, *The Fourth Amendment Heats Up: The Constitutionality of Thermal Imaging and Sense-Enhancing Technology*—Kyllo v. United States, 29 WM. MITCHELL L. REV. 981, 993-94 (2003) (discussing sense-enhancing technologies).

[190] 533 U.S. 27 (2001).

[191] 401 U.S. 745 (1971).

[192] 460 U.S. 276 (1983).

[193] *Kyllo*, 533 U.S. at 29.

[194] *Id.*

[195] *Id.* at 29-30.

[196] *Id.*

[197] *Id.* at 30.

[198] *Id.*

challenged the unwarranted use of the heat sensor by claiming that its use violated his reasonable expectation of privacy.[199] The Court agreed, holding that this type of warrantless, extrasensory surveillance violated the constitution because it was capable of "explor[ing] the details of the home that would previously have been unknowable without physical intrusion . . . ."[200] Justice Stevens, in attempting to justify the warrantless use of this technology in his dissent, tried to categorize heat sensors as an efficiency-enhancing technology: "the ordinary use of the senses might enable a neighbor or passerby to notice the heat emanating from a building . . . ."[201] But the majority of the Court ultimately disagreed, finding the use of a heat sensor without a warrant to be unconstitutionally extrasensory in nature.[202]

This contrasts with the *White* and *Knotts* cases. In each of those cases, the Court concluded that the police do not need to acquire a warrant before using a technological replacement for everyday police activity.[203] In *White*, the Court noted that an undercover officer does not violate a suspect's reasonable expectation of privacy by taking notes on the conversation.[204] Thus, it should come as no surprise that the Court has consistently held that police may engage in warrantless recording of conversations while undercover.[205] As Justice White persuasively argued:

> If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks.[206]

The Court made the same basic argument in the *Knotts* case. There, the Court concluded that the warrantless use of a tracking device was nothing more than a digital replacement for traditional observational surveillance.[207] If police had unlimited resources and officers, they could have conceivably tracked the criminal suspect with the same accuracy. The

---

[199] *Id.*

[200] *Id.* at 40.

[201] *Id.* at 43 (Stevens, J., dissenting).

[202] *Id.* at 40 (majority opinion).

[203] Hutchins, *supra* note 12, at 456 (discussing the difference between sense-augmenting technologies as replacements for police activity and extrasensory technologies).

[204] United States v. White, 401 U.S. 745, 751 (1971).

[205] *See* United States v. Caceres, 440 U.S. 741, 750-51 (1979).

[206] *White*, 401 U.S. at 751.

[207] United States v. Knotts, 460 U.S. 276, 281 (1983).

digital tracking device was nothing more than an efficiency-enhancing technology. As such, the justices upheld the warrantless use of the technology because the court "never equated police efficiency with unconstitutionality."[208]

The Court, though, does not always rely upon a complete dichotomy between efficiency-enhancing and extrasensory technologies. The Court does permit the unwarranted use of certain extrasensory technologies, depending on the quantity and type of information revealed by the technology.[209] The *Dow Chemical* case epitomizes this exception to the rule. Recall that when the state used aerial cameras to zoom into details on the Dow Chemical facility below, the Court acknowledged that no police officer could have seen images in such fine detail without the assistance of the camera.[210] This seems to suggest that the technology was more akin to a heat sensor (extrasensory) than an audio record recorder (efficiency-enhancer). But the Court nonetheless permitted the warrantless use of this technology because of the limited amount of private information it could potentially uncover by photographing a business facility from above.[211] Because the only possible information that the aerial photography could obtain was pictures of an open field, the technology could only minimally invade any person's reasonable expectation of privacy.

This raises an important question—if a technology could record, through extrasensory methods, evidence of illegal behavior only, would police *ever* need to obtain a warrant to use this technology? One emerging technology might raise this very question. [212] The United States intelligence community has made a substantial investment in laser-based molecular scanners.[213] The technology is up to ten million times faster and a million times more sensitive than any other technology

---

[208] *Id.* at 284.

[209] *See* Hutchins, *supra* note 12, at 438.

[210] Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986).

[211] *Id.* at 236-39 (noting the reduced expectation of privacy because the property was more akin to an open field than the property immediately surrounding a home).

[212] Maggie Fox, *New Laser Spectrometer Provides Instant Analysis*, REUTERS, Feb. 7, 2008, *available at* http://www.reuters.com/article/2008/02/07/us-laser-detector-idUSN0734345320080207 (explaining the possible future uses of laser spectrometers that can detect and identify microscopic amounts of material on many feet away on passing pedestrians).

[213] John Roach, *New Security Scanners to Reveal Everything About You, Instantly*, NBC NEWS (July 11, 2012, 1:39 PM), *available at* http://www.nbcnews.com/technology/futureoftech/new-security-scanners-reveal-everything-about-you-instantly-876156; *Hidden Government Scanners Will Instantly Know Everything About You From 164 Feet Away*, GIZMODO, (July 10, 2012), http://gizmodo.com/5923980/the-secret-government-laser-that-instantly-knows-everything-about-you.

currently available.[214] It can immediately ascertain everything about a passing person—from small drug residue to gun powder—from up to 50 meters away.[215] Police can operate this technology without passing pedestrians even knowing it is in operation.[216] Such a technology is undeniably extrasensory in nature. No human could possibly detect the presence of illegal substances on a molecular level. The technology could theoretically be calibrated to uncover only the presence of illegal substances. The Court has generally held that the use of an extrasensory aid, like a canine, that should only alert officers to the presence of an illegal drug does not require a warrant, or even reasonable suspicion before use.[217] But the widespread use of a technology like laser-based molecular scanners could someday force the Court to rethink this conclusion.[218]

To summarize, while the Court has generally upheld the assumption that police may freely use efficiency-enhancing technologies, police must obtain authorization before turning to extrasensory technology. They have tempered this dichotomy in cases where the extrasensory aid can only alert police to the likely presence of illegal behavior. But that assumption may become more and more unjustified in light of technological advancement.

C. Jones and the Emerging Doctrinal Incoherence

Before *Jones*, the Court had relied on these two jurisprudential assumptions of police surveillance. But *Jones* forced the Court to consider how these assumptions fit with the increasingly efficient, digital surveillance of the twenty-first century. It is worth mentioning at the outset that the technology at issue in *Jones* is distinguishable from the digitally efficient investigative technologies discussed in this article. The law enforcement agency used the GPS device in *Jones* to only monitor the movements of a single criminal suspect. While the device could efficiently monitor the movements of a single person, it was not part of a dragnet surveillance technique that collected

---

[214] *Hidden Government Scanners Will Instantly Know Everything About You From 164 Feet Away*, *supra* note 213.

[215] *Id.*

[216] *Id.*

[217] Florida v. Harris, 133 S. Ct. 1050 (2013); Illinois v. Caballes, 543 U.S. 405 (2005); *but see* Florida v. Jardines, 133 S. Ct. 1409 (2013) (holding that a canine sniff on a person's home or curtilage is a Fourth Amendment search).

[218] The ability of laser-based molecular scanners to detect any substance on a molecular level makes it many magnitudes more efficient than a traditional, extrasensory aid like a canine. Thus, this could raise the same legal and pragmatic concerns expressed *supra* Part I.A regarding unregulated efficiency.

surveillance data on the entire community.[219] Thus, it is hard to predict how the Court will eventually handle the digitally efficient investigative state based solely on their treatment of GPS devices. Even so, the *Jones* decision gave the Court a clear opportunity to directly confront the jurisprudential assumptions of police surveillance.

In the case, police suspected that nightclub owner and operator Antoine Jones was trafficking narcotics.[220] The Federal Bureau of Investigation and the D.C. Metropolitan Police Department used a variety of investigation techniques, including the installation of a surveillance camera, pen registers, and a wiretap of Jones's cell phone.[221] Based on potentially incriminating information obtained through these measures, law enforcement successfully acquired a warrant to install a GPS device on Jones's Jeep Cherokee.[222] The warrant only authorized law enforcement to install the device within a 10-day time period while the automobile was in Washington, D.C.[223] Rather than following the terms of the warrant, police installed the device "[o]n the 11th day, and not in the District of Columbia but in Maryland . . . ."[224] Thus, while the police had initially obtained a warrant for the GPS device, the warrant was no longer valid at the time of installation. Police installed the device by attaching it to the underside of the Jeep while it was parked in a public lot.[225]

Over the next 28 days, police tracked the movement of Jones's automobile.[226] The police even replaced the battery on the GPS device at one point while the car was again in a public parking lot in Maryland.[227] Because the GPS device was only affixed to Jones's car, the police could only monitor the movement of his car along public thoroughfares.[228] Still, the police acquired over 2,000 pages of data during this time period, some of which helped build the government's case against Jones and his co-conspirators for conspiracy to distribute and possession with the intent to distribute cocaine.[229] Jones challenged the admission of the GPS data in the District Court. But the court permitted

---

[219] *See* Rushin, *supra* note 8, at 317.

[220] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[221] *Id.*

[222] *Id.* It is worth noting that the car in question actually belonged to Jones's wife, although Jones used the vehicle.

[223] *Id.*

[224] *Id.*

[225] *Id.*

[226] *Id.*

[227] *Id.*

[228] *Id.*

[229] *Id.*

nearly all of this data into evidence, citing *Knotts* for the proposition that an individual has no reasonable expectation of privacy in public movements.[230] The district court jury found Jones guilty and sentenced him to life imprisonment.[231]

In a fascinating decision though, the United States Court of Appeals for the District of Columbia overturned the conviction, ruling that the installation and data collection violated the Fourth Amendment.[232] The D.C. Circuit reached this conclusion by centering their analysis on whether a person has a reasonable expectation that their movements will not be recorded in an extended, uninterrupted manner.[233] Because the marginal cost of every day GPS surveillance is "effectively zero," police could monitor a person's movement cheaply and incredibly efficiently.[234] In applying a so-called "mosaic theory," the court noted that "long-term surveillance of an individual reveals important and intimate details about their behaviors."[235] The court therefore concluded that police should obtain a valid warrant before using technology that can reveal such intimate and private details of one's life.[236]

This was a radical doctrinal shift that fundamentally undermined both of the jurisprudential assumptions of police surveillance. By finding that the recording of personal surveillance data on public movement at some point violates the Fourth Amendment, the D.C. Circuit indicated that it presumably believes that a person can have a reasonable expectation of privacy in public. This undermines the first assumption of police surveillance law, which says that people have *no* reasonable expectation of privacy in public. The second jurisprudential assumption of police surveillance, that the courts should not limit improvements on policing efficiency, is likewise upended if a technology like GPS can become unconstitutionally invasive based merely on its ability to enhance the efficiency of surveillance.

The Supreme Court unanimously agreed with the D.C. Circuit that the installation of a GPS device violated the Fourth Amendment. The Court, though, split on *why* this kind of surveillance violated the Fourth Amendment. Five of the justices—Justice Scalia writing the majority with Justices Thomas, Roberts, Sotomayor, and Kennedy joining—held that

---

230 *Id.*

231 *Id.* at 949.

232 United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd*, United States v. Jones, 132 S. Ct. 945, 954 (2012).

233 *Id.* at 563-64.

234 *Id.* at 565.

235 Rushin, *supra* note 8, at 317.

236 *Maynard*, 615 F.3d at 562-66.

the installation of a GPS device violated the Fourth Amendment because of the device's physical installation on the automobile.[237] These justices were not yet prepared to uphold the mosaic theory advanced by the D.C. Circuit. Instead, they emphasized that, because the attachment of the GPS device amounted to a technical trespass, it violated the original understanding of the Fourth Amendment.[238] The majority did not discount, though, that the Court might have to reconsider some of the basic jurisprudential assumptions of police surveillance law. Scalia cited *Knotts* in explaining that GPS is a mere technological replacement for traditional surveillance, which has always been upheld as constitutionally permissible without a warrant.[239] Scalia noted that, while "[i]t may be that achieving the same results through electronic means, without any accompanying trespass, is an unconstitutional invasion of privacy," the *Jones* case "[did] not require [the Court] to answer that question."[240] The Court has never recognized that long-term surveillance amounts to an unconstitutional search, and the majority argued that attempting to do so now would force the court to unnecessarily grapple with many "vexing problems."[241]

Justice Sotomayor wrote separately to note that long-term and efficient technological surveillance might impinge on a person's reasonable expectation of privacy.[242] Sotomayor concluded that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[243] Nevertheless, Sotomayor felt that this police action could be found unconstitutional based on the trespass of personal property alone.[244] By contrast, four of the justices—Justice Alito writing the concurring opinion with Justices Kagan, Breyer, and Ginsburg joining—concluded that the installation of a GPS device violated the suspect's reasonable expectation of privacy by aggregating copious amounts of data on his public actions.[245] These justices believed that the majority's focus on the physical trespass of the device was reminiscent of the *Olmstead* era decisions that emphasized physical trespass as a necessity to any claim of unreasonable

---

[237] United States v. Jones, 132 S. Ct. 945, 949 (2012).

[238] *Id.*

[239] *Id.* at 953.

[240] *Id.* at 954.

[241] *Id.*

[242] *Id.* at 955-56 (Sotomayor, J., concurring).

[243] *Id.* at 957.

[244] *Id.* at 955 (noting that the reaffirmation of the trespass principle was sufficient to decide this case).

[245] *Id.* at 963-64 (Alito, J., concurring).

search and seizure.[246] According to Justice Alito, the majority's reasoning generally ignores the important privacy interests at stake in the long-term use of GPS tracking, and instead "attaches great significance to something that most would view as relatively minor"—the attachment of a small device to the bottom of a car.[247] Such a viewpoint makes no distinction between the use of GPS tracking for a single day or many years.[248] In Alito's mind, there is clearly a distinction to be made between brief electronic surveillance and extended surveillance; long-term surveillance reveals detailed information about personal behavior and habits, while short-term does not. But above all, Alito's concurrence appears to express concern that the majority's rationale does nothing to address electronic surveillance that does not involve physical trespass.[249]

Alito believes that the Court should look at surveillance techniques on a case-by-case basis and judge whether the electronic surveillance used "involved a degree of intrusion that a reasonable person would not have anticipated."[250] Using this test, Alito would permit the short-term use of electronic surveillance on public streets, but bar the use of long-term surveillance for most criminal offenses.[251] "For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[252]

The Alito recommendation is similar to the proposal I made two years ago.[253] His solution would involve the judiciary limiting the length of data retention for surveillance technologies. He would permit longer retention in cases where police are investigating serious criminal offenses. And he emphasizes that the legislature may be the most appropriate branch to regulate these technologies long-term. Similarly, I argued that the judiciary should regulate the digitally efficient investigative state by limiting the length of data retention.[254] I

---

[246] *Id.* at 959.

[247] *Id.* at 961.

[248] *Id.* (noting that the "Court's approach leads to incongruous results" because it would make no distinction between use of the GPS device for "a brief time" or a "much longer period [of time]").

[249] *Id.* at 962.

[250] *Id.* at 964.

[251] *Id.*

[252] *Id.*

[253] Rushin, *supra* note 8, at 318.

[254] *Id.*

emphasized the need for the judiciary to not establish a firm limit on data retention and surveillance, thereby giving police latitude to adjust the use of these technologies to the relative seriousness of the crime being investigated and the relative threat posed by the suspected criminal offense.[255] I concluded that the "legislatures must play a critical role in developing more nuanced and specific enactments" that elaborate specific regulations for the use of surveillance technology.[256] Both my recommended solution and Alito's represent a limited acceptance of the so-called mosaic theory that recognizes that the aggregation of long-term electronic surveillance data can be so revealing of personal details as to become an unreasonable search or seizure.

After the *Jones* decision, it seems likely that the Court will someday break away from the two jurisprudential assumptions of mass police surveillance. At least five of the justices showed clear support for the adoption of some version of the mosaic theory. And even the justices that did not officially support the future adoption of such a doctrinal path acknowledged that it might be necessary in the future. But, this raises two important questions—how should we begin to regulate the use of these surveillance devices, and what branch of government should do the regulating?

Scholars are sharply divided on the appropriateness of judicially regulating emerging technologies. Orin Kerr has been perhaps the most outspoken and persuasive critic of judicial policymaking in such cases. Kerr has advanced three important arguments in support of this position: (1) the courts lack the physical and administrative resources to develop comprehensive policies, (2) judges are not technologically sophisticated enough to craft technology regulations, and (3) these judicial regulations rarely hold up in different factual situations.[257] After the *Jones* decision, Kerr also argued that if the Court were to adopt the mosaic theory, it would necessarily have to confront many

---

[255] *Id.* at 321 (suggesting that "we may prefer more liberal data retention policies for surveillance around national monuments and critical infrastructures in recognition of the threat posed by terrorism").

[256] *Id.* at 328.

[257] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 857-88 (2004).

extremely difficult choices.[258] Thus, Kerr believes that the Court should avoid such a path in the future.[259]

I disagree with Kerr's conclusions on the limited institutional capacity of the judiciary to regulate emerging surveillance technology. But even if the Court does eventually adopt some version of the mosaic theory—as I believe they will—this judicial response will be very limited. Thereafter, state legislatures will ultimately have to develop most nuanced regulations of these devices going forward.[260] In the next section, I develop a model state statute that could address some of the major problems implicated by the digitally efficient state.

III. THE LEGISLATIVE RESPONSE

Any future judicial response must be coupled with state legislation. Even if the judiciary eventually accepts some version of the mosaic theory in interpreting the Fourth Amendment, we should not expect the Court to hand down detailed regulations for the use of these technologies. Justice Alito's concurrence in *Jones* is telling. His proposal to regulate the efficiency of surveillance technologies would only control data retention.[261] And the amount of data that a police department could reasonably retain without a warrant would vary from one situation to the next based upon the relative seriousness of the possible crime at issue.[262] This barely scratches the surface of broader problems posed by the digitally efficient state. Under what conditions should we permit extensive data retention? When should we limit this kind of retention? Is data aggregation more acceptable as long as the data is not cross-referenced with other databases, thereby personally identifying individuals? Should we regulate law enforcement's access to this personal data? And where should this data be stored?

Even my original proposal for judicial regulation of mass police surveillance only addressed a handful of these questions. I recommended that courts require police to develop clear data retention policies that are tailored to only retain data as long as necessary to serve a legitimate law enforcement

---

[258] *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

[259] *Id.* at 315-16 (pushing instead for the Court to adopt a sequential analysis of search and seizure law, where the Court "take[s] a snapshot of the act and assess[es] it in isolation").

[260] *Id.* at 328.

[261] *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

[262] *Id.*

purpose.[263] Like Alito's proposal, such a standard would vary according to the seriousness of the crime under investigation and the individual circumstance. I also argued that in cases where police retain surveillance data without a warrant through electronic means, they should have a legitimate law enforcement purpose before cross-referencing that data with other databases for the purposes of identifying individuals.[264]

Both the *Jones* concurrence and my previous proposal would establish a broad judicial principle mandating that police regulate data retention according to the seriousness of the crime under investigation and the legitimate need for such retention. This type of judicial response is limited in nature. Legislative bodies would likely need to step in to provide more detailed standards.

The legislative branch has several advantages over the judiciary that make it appropriate for this type of detailed policy building. The legislature has a wider range of enforcement mechanisms than the judiciary. The legislature can mandate in-depth and regular oversight. And it has the resources and tools to develop extensive, complex regulations. As a result, the legislature is the best-positioned branch to address some of the critical issues raised by the digitally efficient investigative state, such as data storage, access, and sharing policies.

In this Part, I offer guidelines for a legislative response to mass police surveillance. I first detail some of the foundational principles that legislative bodies ought to recognize in regulating police use of technology. Next, I give a brief overview of how a handful of states have attempted to regulate these technologies. I conclude by offering and defending my statutory recommendations.

A. Foundational Principles for Regulating Police Surveillance Technology

In making this legislative recommendation, I rely on three foundational principles about legislative regulation of law enforcement technologies. First, any regulation must provide clear and articulable standards that law enforcement can and will easily enforce.[265] Courts and legislators have often agreed

---

[263] Rushin, *supra* note 8, at 318.

[264] *Id.*

[265] David Goetz, *Locating Location Privacy*, 26 BERKELEY TECH. L.J. 823, 856 (2011); Pell & Soghoian, *supra* note 23, at 124 (explaining the importance of clear rules for law enforcement); Savage, *supra* note 23, at A12 (quoting Professor Kerr advocating clear standards for law enforcement).

that police regulations should be easy to apply across many different factual circumstances.[266] If a regulation is unclear, there is a higher probability that law enforcement will, even in good faith, misapply the standard. For example, in *Atwater v. City of Lago Vista*, Texas state law permitted officers to arrest offenders who violated traffic laws for failure to wear a seatbelt, even though the final punishment for such a violation was a mere fine.[267] In upholding an officer's decision to arrest a woman for failure to buckle her seatbelt, the Court stressed that police need rules that emphasize "clarity and simplicity."[268]

Earlier regulations have encountered resistance from law enforcement because they were not easily administrable standards. For example, in *Arizona v. Gant*, the Court upended a longstanding doctrine that said police could search an automobile incident to an arrest of a person in that vehicle.[269] The new standard said that police "may search a vehicle incident to a recent occupant's arrest only if the arrestee is within reaching distance of the passenger compartment at the time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest."[270] Justice Alito found this new standard undesirable compared to the previous standard. In Alito's mind, the Court should strive for "a test that would be relatively easy for police officers and judges to apply."[271] While some commentators disagree about the relative importance of clear and simple rules,[272] most judges and policymakers agree that any policymaker should consider the administrability of a mandate.

Clear and simple rules also have another advantage over ambiguous mandates—these kinds of clear directives are less susceptible to organizational mediation.[273] If a state regulation of a policing organization is "vague or ambiguous," the police organization may "mediate the implementation and impact the law."[274] Lauren Edelman had demonstrated this

---

[266] *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 360 (2009) (Alito, J., dissenting) (noting that courts and policymakers should strive to develop "a test that would be relatively easy for police officers and judges to apply").

[267] Atwater v. City of Lago Vista, 532 U.S. 318, 323 (2001).

[268] *Id.* at 347.

[269] *Gant*, 556 U.S. at 351.

[270] *Id.*

[271] *Id.* at 360 (Alito, J., dissenting).

[272] *See* William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2182 (2002) (claiming that police may actually be better at applying vague rules, contrary to the majority of all comments by courts and commentators).

[273] Stephen Rushin, *The Regulation of Private Police*, 115 W. VA. L. REV. 159, 198-99 (2012).

[274] *Id.*

type of mediation in the case of equal employment and affirmative action laws that are intended to change the behavior of private organizations.[275] These initial laws only established broad regulatory goals without offering clear and explicit procedural limitations.[276] This type of ambiguous mandate gave private companies room to interpret the laws and construct the meaning of compliance, thereby mediating "the impact of the law on society."[277]

In the past, the police have been guilty of organizational mediation of a variety of legal mandates. The general police response to *Miranda* is particularly demonstrative of this phenomenon. Scholars like Richard Leo and Charles Weisselberg have carefully shown how police have navigated around the limitations of the original *Miranda* decision to nonetheless engage in seemingly coercive interrogation techniques aimed at acquiring information.[278] The original *Miranda* opinion provided some limitations on interrogations, but the decision and subsequent holdings may have been ambiguous, thereby allowing for departments to navigate around them without technically violating the law. Thus, in crafting rules for police, both the Court and legislatures should aim to create easily administrable law enforcement rules if at all possible, but also laws that are specific enough to avoid organizational mediation.

Second, communities differ in their need for public surveillance. For example, New York City and Washington, D.C. have previously been targets for international terrorism. Given their plethora of high value targets and landmarks, these two cities may have a legitimate need for more public surveillance than other communities.[279] In arguing for a malleable standard for local departments, the IACP has suggested that some locations—namely bridges, critical infrastructure, and other high value targets—demand more surveillance and data retention to ensure public safety.[280] As an example, the IACP cites the fact that locations targeted on September 11, 2001 were part of a terrorist attack that took many years to plan and execute.[281]

---

[275] *See generally* Lauren B. Edelman, *Legal Ambiguity and Symbolic Structures: Organizational Mediation of Civil Rights Law*, 97 AM. J. SOC. 1531 (1992).

[276] *Id.* at 1532-33.

[277] *Id.* at 1532.

[278] *See generally* Charles D. Weisselberg, *Mourning* Miranda, 96 CALIF. L. REV. 1519 (2008); Richard A. Leo, *Inside the Interrogation Room*, 86 J. CRIM. L. & CRIMINOLOGY 266 (1996).

[279] *See* Rushin, *supra* note 8, at 321.

[280] *Id.*

[281] INT'L ASS'N OF CHIEFS OF POLICE, PRIVACY IMPACT ASSESSMENT REPORT FOR THE UTILIZATION OF LICENSE PLATE READERS 40 n.70 (Sept. 2009) [hereinafter IACP

Thus, certain communities may legitimately need and prefer longer retention periods around certain important targets. Conversely, a medium-sized suburb with low crime that places a higher value on privacy might prefer a bar on the retention of surveillance data all together. While any state statute should establish minimally acceptable requirements on data retention, the law must be sufficiently broad to permit necessary variation at the local level. A one-size-fits-all approach may not be workable, given the unique law enforcement needs of each city.

Third, any regulation must clearly articulate the narrow scope of technologies and devices that fall under its regulatory purview. Because technology changes rapidly, this ensures that the law will not be misapplied to future, emerging technologies. Kerr has previously argued that regulations of technology ought to proceed cautiously until the technology has stabilized.[282] Technology may have unforeseen uses that will take time to develop and understand. For example, in 1988, Congress passed the Video Privacy Protection Act.[283] This law protected the privacy of videotape rental information.[284] Congress passed the law after Judge Robert Bork's video rental history became public during his Supreme Court nomination process.[285] But in crafting this limitation on video rentals, Congress defined the term "video tape service provider" expansively as "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual material."[286]

On one hand, this expansive definition of a videotape service provider is useful because it is broad enough to avoid antiquation. As videotape technology waned in popularity and DVDs became the chosen medium for most movie rental providers, the law maintained its statutory force. But the vague language used by the original drafters of the law left online streaming content providers like Netflix wondering whether the law actually applied to their services.[287] It was also unclear what kind of approval Netflix and other providers had

---

PRIVACY ASSESSMENT], *available at* http://www.theiacp.org/LinkClick.aspx?fileticket=N%2bE2wvY%2f1QU%3d&tabid=87.

[282] Kerr, *supra* note 258, at 805.

[283] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012), *amended by* Video Privacy Protection Act Amendment Act of 2012, Pub. L. No. 112-258 (2013).

[284] *Id.*

[285] Brendan Sasso, *Obama Signs Bill to Let Facebook Users Share Netflix Videos*, HILL (Jan. 10, 2013, 2:31 PM), http://thehill.com/blogs/hillicon-valley/technology/276557-obama-signs-bill-to-let-facebook-users-share-netflix-videos.

[286] 18 U.S.C. § 2710(a)(4).

[287] Julianne Pepitone, *New Video Law Lets You Share Your Netflix Viewing on Facebook*, CNN MONEY (Jan. 10, 2013 9:50 PM), http://money.cnn.com/2013/01/10/technology/social/netflix-vppa-facebook/.

to obtain to allow users to share their viewing history on social media platforms like Facebook.[288] After years of ambiguity, Congress recently amended the law to permit users to share content watching habits on streaming sites like Netflix after they have given one-time approval.[289]

Before the law change, Netflix complained that the law's language was confusing, making them hesitant to adopt social media integration.[290] Similarly, when regulating police technology use, legislative bodies should adopt language that is sufficiently broad to avoid immediate antiquation. They should also be careful not to select language that is so overly broad as to limit the use of new, potentially important technological tools.

The legislative recommendation I make in this Part attempts to follow these three guiding principles: it attempts to (1) clearly define the limited scope of the applicable technologies, (2) be clear and simple for law enforcement to administer, and (3) permit some level of local variation to meet the needs of unique municipalities. My starting point for crafting this model was to analyze the small number of statutes already passed by state legislators. The next section looks at these statutes to demonstrate common trends.

B. Current State Regulations

A handful of states have laid out regulations of the digitally efficient investigative state. These state laws operate by either regulating ALPR and surveillance cameras specifically, or by establishing broad standards for data retention. For example, states like Virginia have passed relatively broad laws that regulate the retention of data by the government in all forms.[291] In other states, like New Jersey, the state attorney general has used state constitutional authority to hand down directives regulating the use of ALPR and establishing limitations on data collection.[292] States like Maine, Arkansas, New Hampshire, Vermont, and Utah have regulated ALPR through legislative measures.[293] Some states, like New York, have also handed down suggested model guidelines to inform

---

[288] *Id.*

[289] *Id.*

[290] *Id.*

[291] VA. CODE ANN. § 2.2-3800 (West 2010).

[292] State of N.J., Office of the Attorney Gen., Directive No. 2010-5 (Dec. 3, 2010), *reprinted in* ROBERTS &CASANOVA, *supra* note 56, at 73.

[293] ARK. CODE ANN. § 12-12-1802 to 1808 (2013); ME. REV. STAT. 29-A, § 2117-A (2009); N.H. REV. STAT. ANN. § 236:130 (2011); UTAH CODE ANN. § 41-6a-2001 to 2006 (2013); VT. STAT. ANN. tit. 23, § 1607 (2013).

internal policymakers.[294] In this section, I demonstrate that most of these early efforts to regulate the digitally efficient surveillance technologies share a handful of common concerns. They limit the identification of personal data, the length of data retention, the sharing of information with other departments, and law enforcement access to stored data. These early models also rely on a bevy of enforcement mechanisms. Thus, any model legislation aimed at holistically managing the digitally efficient investigative state should consider the possible solutions offered by existing laws.

First, the laws generally limit the length of data retention in some way. Maine's law on ALPR limits retention to 21 days.[295] New Hampshire also puts a strict limit on the collection of law enforcement data, barring "retention of surveillance data except for a few, specific situations."[296] By stark contrast, the New Jersey Attorney General has ordered that data be retained for no more than five years.[297] Model guidelines like those offered by the State of New York do not establish a maximum length of data retention,[298] but the New York recommendations do encourage departments to establish a clear policy on the length of data retention.[299] Arkansas limits retention to 150 days,[300] Utah allows retention by government agents for nine months,[301] and Vermont permits retention for up to 18 months.[302] Each of these statutes reaches a different conclusion on the appropriate length of data retention. The disparity between the New Jersey data retention limit of five years and relatively strict retention limits in states like Maine and New Hampshire is striking. But the Maine law might not be as restrictive as it initially appears. Although it does limit retention in most cases to 21 days, it also makes an exception for cases where law enforcement is engaged in an ongoing investigation or intelligence operation.[303] Overall, state legislatures have reached dramatically different conclusions on the relative threat posed by long-term data retention.

---

294 N.Y. STATE DIV. OF CRIM. JUST. SERVS., SUGGESTED GUIDELINES: OPERATION OF LICENSE PLATE READER TECHNOLOGY (Jan. 2011), *reprinted in* ROBERTS & CASANOVA, *supra* note 56, at 94.

295 ME. REV. STAT. 29-A, § 2117-A(5).

296 Rushin, *supra* note 8, at 319 (citing N.H. REV. STAT. ANN. §236:130 (2011)).

297 State of N.J., *supra* note 292, at 9.

298 N.Y. STATE DIV. OF CRIM. JUST. SERVS., *supra* note 294, at 16-17.

299 *Id.*

300 ARK. CODE ANN. § 12-12-1805 (2013).

301 UTAH CODE ANN. § 41-6a-2004 (2013).

302 VT. STAT. ANN. tit. 23, § 1607(d)(2) (2013).

303 ME. REV. STAT. 29-A, § 2117-A(5) (2009).

Second, a few of the available laws demonstrate a concern for the identification of personal data collected by the state. The New Jersey Attorney General Directive intends in part to limit the "disclos[ure] [of] personal identifying information about an individual unless there is a legitimate and documented law enforcement reason for disclosing such personal information to a law enforcement officer or civilian crime analyst."[304] In New York, the model guidelines would also require that officers attempting to query stored data for identifying matches have a legitimate law enforcement purpose for doing so, and that they record their identification procedure. [305] Neither Maine nor New Hampshire has a substantial policy on the identification of data, likely due in large part to their strict limitations on retention.[306] The longer a state legislature permits data retention, the more legitimately concerned it may be about the possibility of this data becoming personally identified. After all, the combination of long-scale retention and data identification procedures may allow law enforcement to create "digital dossiers" on innocent people that reveal private information about their habits, preferences, and daily movements.[307]

Third, the available laws and recommended models tend to put restrictions on the sharing of information with other agencies. The New Jersey directive permits the sharing of ALPR data among police departments in the state, provided that the departments keep records of the data being shared and all departments involved abide by the New Jersey rules.[308] Nonetheless, New Jersey uses regulations on sharing as a way to encourage the development of a consistent and organized state database.[309] The Utah law permits sharing and disclosure only under narrow circumstances. [310] Arkansas, by contrast, strictly prohibits sharing of collected data.[311] Other states, like New York, have been relatively hands-off when it comes to data sharing. They simply urge departments to build procedures for sharing data that are consistent with their overall recommendations on data protection.[312] We may expect states

---

[304] State of N.J., *supra* note 292, at 1.

[305] N.Y. STATE DIV. OF CRIM. JUST. SERVS., *supra* note 294, at 16-17.

[306] ME. REV. STAT. 29-A, § 2117-A; N.H. REV. STAT. ANN. § 236:130 (2011).

[307] Rushin, *supra* note 8, at 318 (citing Daniel J. Solove, *Digital Dossier and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002)).

[308] State of N.J., *supra* note 292, at 13-14.

[309] *Id.*

[310] UTAH CODE ANN. § 41-6a-2004 (2013).

[311] ARK. CODE ANN, § 12-12-1804 (2013).

[312] N.Y. STATE DIV. OF CRIM. JUST. SERVS., *supra* note 294, at 17.

to want to encourage departments to share whatever data they can legally retain. By doing so, departments can have access to significantly more information on the potential whereabouts of criminal suspects who travel outside jurisdictional lines.[313]

Fourth, available and model rules document and limit access to stored data. New Jersey's regulation requires departments to record all user access to stored ALPR data, including the name of the user accessing the data, the time and date of the access, whether the person used automated software to analyze the data, and the name of the supervisor who authorized the access.[314] New York's model guidelines also suggest that departments document when officers search and analyze stored data.[315] Officers should also only analyze data if they have a legitimate law enforcement purpose for doing so.[316] Additionally, the Maine provision stresses the importance of confidentiality in stored data.[317] That law restricts access to law enforcement officers.[318] And in Vermont, the law explicitly states that access to stored data should be limited to specified or previously designated personnel.[319] Thus, the current array of statutes acknowledges the need for limited access to available data and confidentiality of stored information.

Fifth, some of the model regulations require departments to train employees in the proper procedures for handling data. They also discipline employees who fail to follow policy parameters. The New York suggested guidelines recommend that departments establish a list of designated personnel who are authorized to access ALPR data,[320] and encourage departments to establish a training program to teach officers about the proper use of ALPR technology.[321] The New Jersey directive also requires that departments "designate all authorized users, and that no officer or civilian employee will be authorized to operate an ALPR, or to access or use ALPR stored data, unless the officer or civilian employee has received training by the department on the proper operation of these devices."[322] Once more, the New Jersey directive mandates that "any sworn officer or civilian employee of the

---

313 Rushin, *supra* note 8, at 292-93.
314 State of N.J., *supra* note 292, at 6-7.
315 N.Y. STATE DIV. OF CRIM. JUST. SERVS., *supra* note 294, at 16-17.
316 *Id.* at 16.
317 ME. REV. STAT. 29-A, § 2117-A(4) (2009).
318 *Id.*
319 VT. STAT. ANN. tit. 23, § 1607(c)(1)(C)(ii) (2013).
320 N.Y. STATE DIV. OF CRIM. JUST. SERVS., *supra* note 294, at 15.
321 *Id.*
322 State of N.J., *supra* note 292, at 14-15.

agency who knowingly violates the agency's policy, or these Guidelines, shall be subject to discipline."[323] Conversely, neither the Maine nor New Hampshire laws touch on officers' training in data retention.[324] But this is likely because they do not permit significant data accumulation, thereby making training in data management less imperative. On the whole, those states and entities that do permit large-scale data collection also encourage officer training as a safeguard against abuse.

Sixth, the current array of regulations uses a wide range of enforcement mechanisms. In New Jersey, as a penalty for non-compliance, the Attorney General maintains the authority to temporarily or permanently revoke a department's right to use ALPR devices.[325] Arkansas provides for civil remedies for individuals when a violation of the law causes them actual harm.[326] Utah, by contrast, simply makes violation of the statute a criminal misdemeanor.[327] Both the New Hampshire and the Maine laws have made the violation of ALPR regulations a criminal act in the state.[328] Although New York's regulations are non-mandatory, they still recommend that departments begin creating records in case the state someday begins to audit data access and retention records.[329]

In sum, current state statutes and recommended guidelines address a number of concerns related to the digitally efficient state. It is worth noting again that these laws go far beyond anything the judiciary would likely implement. The Supreme Court is institutionally limited in its capacity to develop a response to the digitally efficient investigative state. The variation on the mosaic theory adopted by Alito in his *Jones* concurrence would only establish a broad principle that long-term data retention by efficient public surveillance technologies may eventually violate a person's reasonable expectation of privacy. Such a rule is ambiguous and does not touch on data storage, access, and identification. State legislation offers the possibility of establishing detailed and definitive standards.

---

[323] *Id.* at 15.
[324] ME. REV. STAT. 29-A, § 2117-A (2009); N.H. REV. STAT. ANN. § 236:130 (2011).
[325] State of New Jersey, *supra* note 292, at 16.
[326] ARK. CODE ANN. § 12-12-1807 (2013).
[327] UTAH CODE ANN. § 41-6a-2006 (2013).
[328] ME. REV. STAT. 29-A, § 2117-A(6); N.H. REV. STAT. ANN. § 236:130(V) (2009).
[329] N.Y. STATE DIV. OF CRIM. JUST. SERVS., *supra* note 294, at 16-17.

C. Model Statute to Regulate Police Surveillance

The presently available statutes and model guidelines suggest a key set of concerns that any future state legislative body must consider. They demonstrate five common regulatory needs: data retention, identification, access, sharing, and training. The model statutory language I offer includes a possible solution for each of these areas. In doing so, I also try to honor the foundational principles for the regulation of police surveillance identified above. The model statute provides a clear standard that law enforcement agencies can implement. It attempts to give departments some latitude to alter their own policies to meet local needs. But the law also includes specific and detailed regulations in hopes of preventing organizational mediation.

The proposed statute also includes multiple enforcement mechanisms to ensure compliance. The model excludes from criminal court any evidence obtained in violation of this statute, thus removing the incentive for police departments to violate the policy. Of course, evidentiary exclusion is "limited as a means for promoting institutional change" because it is filled with exceptions and is narrower than the scope of police misconduct.[330] Thus, I propose two additional enforcement mechanisms. First, the model statute gives the state attorney general authority to initiate litigation against departments that fail to comply with these mandates. Other statutes regulating police misconduct, like 42 U.S.C. § 14141, have used a similar mechanism.[331] Second, the model mandates periodic state audits of departmental policies and data records to ensure compliance. Overall, the proposed law broadly addresses many of the problems implicit in the digitally efficient state and establishes a number of enforcement mechanisms to ensure organizational compliance.

1. Applicability, Definitions, and Scope

The first part of the proposed statute defines the scope of the legislation, including the technologies regulated by the statute. In this section of the statute, I tried to reflect the foundational principle of regulating police surveillance technologies by creating a tightly defined scope of presently available technologies that fall under the statute's regulatory purview. This might make the statute under-inclusive at some point in

---

[330] Harmon, *supra* note 21, at 10-11.
[331] *Id.* at 1.

the future, but works to the benefit of avoiding over-inclusivity that can stifle the development of new technologies.[332]

> *§1 Applicability, Definitions, and Scope*
>
> *This statute applies to all community surveillance technologies used by law enforcement that collect personally identifiable, locational data.*
>
> *"Community surveillance technology" means any device intended to observe, compare, record, or ascertain information about individuals in public through the recording of personally identifiable information. This includes, but is not limited to, surveillance collected with automatic license plate readers, surveillance cameras, and surveillance cameras with biometric recognition.*

This scope provision specifically addresses community surveillance devices, such as ALPR and surveillance cameras, as distinguished from traditional surveillance tools like GPS devices and wiretaps. As I have previously argued, "networked community surveillance technologies like ALPR surveil an entire community as opposed to a specific individual."[333] While the use of a GPS device to monitor the movements of one criminal suspect over a long period of time might be constitutionally problematic, such a practice raises an entirely different set of public policy questions. At minimum, the kind of tracking at issue in *Jones* was narrowly tailored to only affect one criminal suspect. The digitally efficient investigative state uses community surveillance technologies like ALPR and surveillance cameras that can potentially track the movements of *all individuals* within an entire community regardless of whether there is any suspicion of criminal wrongdoing. Hence, this statute is carefully limited to a small subset of technologies that pose similar risks and thus require similar regulation.

2. Differential Treatment of Observational Comparison and Indiscriminate Data Collection

Next, I propose that state laws should differentiate between observational comparison and indiscriminate data collection.[334] The model law permits the use of community

---

[332] *See supra* Part III.A.

[333] Rushin, *supra* note 8, at 317.

[334] *See supra* Part I.A (defining and distinguishing between observational comparison and indiscriminate data collection).

surveillance technologies for observational comparison. When a department uses these technologies for observational comparison, the device is "an incredibly efficient law enforcement tool that is reasonably tailored to only flag the suspicious."[335]

> *§2 Observational Comparison and Indiscriminate Data Collection*
>
> *Police departments may use community surveillance technologies as needed for observational comparison. But police departments using community surveillance technologies for indiscriminate data retention must abide by data integrity, access, and privacy restrictions outlined in §3 through §6.*
>
> *"Observational comparison" is defined as the retention of locational or identifying data after an instantaneous cross-reference with a law enforcement database reveals reasonable suspicion of criminal wrongdoing.*
>
> *"Indiscriminate data collection" is defined as the retention of locational or identifying data without any suspicion of criminal wrongdoing.*

This distinction strikes a reasonable balance by facilitating law enforcement efficiency in identifying lawbreakers, but also avoiding the unlimited and unregulated collection of data. When applied to ALPR, this statute would mean that police could use that technology to flag passing license plates that match lists of stolen cars or active warrants. But they could not retain locational data on license plates that do not raise any concerns of criminal activity without abiding by the regulations that follow.

3. Data Integrity, Access, and Privacy

I recommend that the indiscriminate collection of data be subject to four separate requirements that limit the retention, identification, access, and sharing of data. The statutory language below was designed to give law enforcement some leeway to create workable internal policies that meet organizational and community needs. As a result, the policy simply serves as a minimum floor of regulation, above which departments could adopt their own regulations.

---

[335] Rushin, *supra* note 8, at 285.

§3 Data Retention

Police departments using community surveillance technologies for indiscriminate data collection must establish and publicly announce a formalized policy on data retention. Departments may not retain and store data for more than one calendar year unless the data is connected to a specific and ongoing criminal investigation.

The one-year retention period is the most significant regulation this statute would place on indiscriminate data collection. Even the IACP acknowledges that the "indefinite retention of law enforcement information makes a vast amount of data available for potential misuse or accidental disclosure."[336] Without limits on retention, police surveillance can develop into "a form of undesirable social control" that can actually "prevent people from engaging in activities that further their own self-development, and inhibit individuals from associating with others, which is sometimes critical for the promotion of free expression." [337] At the same time, law enforcement often claim that information that seems irrelevant today may someday have significance to a future investigation.[338] Without regulation, there is a cogent argument to be made that police would have every incentive to keep as much data as possible.[339] Thus, I recommend that data retention be capped at one year. This would prevent the potential harms of the digitally efficient investigative state that come from long-term data aggregation.

The one-year time window represents a reasonable compromise. The median law enforcement department today retains data for around six months or less. [340] But before accepting this retention limit, state legislatures should critically assess their own state needs to determine whether there is a legitimate and verifiable need for retention beyond this point. The next section of the statute addresses identification of stored data.

---

[336] IACP PRIVACY ASSESSMENT, *supra* note 281, at 36.
[337] *Id.*
[338] *Id.* at 37.
[339] Rushin, *supra* note 8, at 321.
[340] *See supra* Part I.C.

§4 Data Identification

Police employees must have a legitimate law enforcement purpose in identifying the person associated with any data retained by community surveillance technologies.

The limit on data identification is somewhat different than most current statutory arrangements. This measure would, potentially, limit the ability of law enforcement to use the stored data for secondary uses. A secondary use is the use of data collected for one purpose for an unrelated, additional purpose.[341] This kind of secondary use can "generate[] fear and uncertainty over how one's information will be used in the future."[342] By limiting the identification of the data, the statute attempts to prevent such secondary use. Another way to avoid secondary use is to limit access to data and external sharing, as I attempt to do in the next portions of the statute.

§5 Internal Access to Stored Data

Departments must establish a formal internal policy documenting each time a police employee accesses community surveillance databases. Departments shall not allow anyone except authorized and trained police employees to access and search these databases.

§6 External Data Sharing

Police departments may share information contained in community surveillance databases with other government agencies, as long as all participating departments honor the minimum requirements established in this statute.

I propose that police limit access to data even among police employees. And each time a police employee accesses data, I require that the department document this event. This achieves two results. First, it creates a record of previous access points that the attorney general or state criminal courts can, theoretically, use to hold police accountable for improper data access. Secondly, and relatedly, this formalized documentation process may prevent nefarious secondary uses of the information. Because some evidence suggests that police retain community surveillance data in databases accessible to

---

[341] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 521 (2006).
[342] IACP PRIVACY ASSESSMENT, *supra* note 281, at 15.

private companies and civilians,[343] this would place the impetus on police departments to take responsibility for internal data management. And while the model statute does not limit the sharing of digitally efficient data, it does require that all departments with access to data abide by the statutory limits. This would promote the sharing of data across jurisdictional lines to facilitate efficient investigations, while providing a consistent level of minimum privacy protection in the state.

4. Enforcement Mechanisms

To ensure that departments abide by these minimal regulations, I propose a combination of enforcement mechanisms. The judicial and legislative branches have previously used these three enforcement mechanisms in other contexts to regulate police misconduct. By permitting a wide range of enforcement mechanisms, the statute attempts to avoid the traditional problems associated with police and organizational regulation. The first enforcement mechanism involves evidentiary exclusion.

§7 Evidentiary Exclusion

All evidence acquired by law enforcement in violation of this statute shall be inadmissible in state criminal courts.

The judiciary generally excludes evidence obtained in violation of the constitution. This mechanism is "by far the most commonly used means of discouraging police misconduct and perhaps the most successful." [344] Empirical evidence suggests that evidentiary exclusion can change law enforcement behavior and incentivize compliance with the law. [345] But the exclusionary rule suffers from several limitations. As Rachel Harmon has explained, the exclusionary rule is "riddled with exceptions and limitations, many of which are inconsistent with using the exclusionary rule as an

[343] NICHOLS, *supra* note 72, at 8 (noting that only 53% of surveillance camera operators are sworn police officers).

[344] Harmon, *supra* note 21, at 10.

[345] *See, e.g.*, William C. Heffernan & Richard W. Lovely, *Evaluating the Fourth Amendment Exclusionary Rule: The Problem of Police Compliance with the Law*, 24 U. MICH. J.L. REFORM 311, 339-40 (1991) (arguing that while police often did not always comply with Fourth Amendment protections, they were more likely to do so if the rules were simplified); Myron W. Orfield, Jr., Comment, *The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers*, 54 U. CHI. L. REV. 1016, 1017 (1987) (arguing that the exclusionary rule did influence internal policies in the Chicago Police Department).

effective deterrent of police misconduct."[346] Thus, if the misconduct happens to fall into one of these many exceptions, the exclusionary rule may not be an effective deterrent. But perhaps more importantly, as Harmon explains, "the scope of the exclusionary rule is inevitably much narrower than the scope of illegal police misconduct."[347] After all, the exclusionary rule would only work as a mechanism for preventing police misuse of digitally efficient databases if the police intended to use the resulting evidence in a criminal trial. But much of the misconduct I discuss in this article and previous work involves police utilizing retained data for undetermined secondary purposes. The exclusionary rule may do little to prevent this type of misconduct. To remedy this problem, I propose two other enforcement mechanisms.

> *§8 Attorney General Right of Action*
>
> *The Attorney General of this state shall have a civil right of action against any police department that engages in a pattern or practice of violating this statute.*
>
> *§9 State Audit of Departmental Policy*
>
> *The Attorney General of this state shall have the authority to periodically audit departmental policies to ensure compliance with this statute. The Attorney General will publicly post the results of this audit to bring attention to noncompliant departments.*

Two of the statutes currently in operation only classify the violation of data retention and access policies as a minor criminal act.[348] In theory, these laws could result in the prosecution of a police officer who fails to abide by their parameters. But as Harmon concludes, "prosecutions against police officers are too rare to deter misconduct."[349] This is because juries tend to sympathize with defendant police officers, and the criminal prosecution of minor misconduct is rarely among the top priorities for over-worked prosecutors.[350] Consequently, I avoid establishing criminal liability for officers who violate this statute. Instead, I suggest that the state

---

[346] Harmon, *supra* note 21, at 10.

[347] *Id.* at 10-11.

[348] *See supra* Part III.B.

[349] Harmon, *supra* note 21, at 9.

[350] *Id.* (explaining how "juries frequently believe and sympathize with defendant officers" and how prosecution of police officers is both inconsistent and "too rare to deter misconduct").

attorney general office should take on a proactive role in ensuring compliance through suing noncompliant agencies and occasionally auditing departmental policies.

The first alternative enforcement mechanism gives the state attorney general statutory authority to bring suit against departments that engage in a pattern of practice of violating this statute. This is similar to the statutory mandate given to the Department of Justice (DOJ) by 42 U.S.C. §14141.[351] Police scholar Barbara Armacost has called §14141 "perhaps the most promising mechanism" for addressing organizational misconduct.[352] The late Bill Stuntz even believed that §14141 may be "more significant, in the long run, than *Mapp v. Ohio* . . . which mandated the exclusion of evidence obtained in violation of the Fourth Amendment." [353] Pattern and practice litigation, as authorized in §14141, is unique because it permits the DOJ to bring federal suit against police departments that engage in systematic misconduct; in practice, the DOJ successfully ensured the appointment of judicial monitors in targeted cities to oversee organizational and policy reform.[354] Although there is only a small amount of empirical research on the effectiveness of §14141 in reducing police misconduct, the available evidence suggests it is one of the most effective means of bringing about organizational change.[355] One of the only potential pitfalls of this form of regulation is that the state attorney general may have limited resources. [356] If resource constraints make lawsuits unlikely for noncompliant departments, a police agency might rationally calculate that the benefits of noncompliance outweigh the potential costs of litigation.[357]

To remedy the concern over resource limitations, I propose that the state attorney general have statutory

---

[351] 42 U.S.C. § 14141 (2011) (giving the Department of Justice the authority to bring suit against police departments that engage in a pattern or practice of unconstitutional misconduct).

[352] Barbara E. Armacost, *Organizational Culture and Police Misconduct*, 72 GEO. WASH. L. REV. 453, 457 (2004).

[353] William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 538-39 n.134 (2001).

[354] Harmon, *supra* note 21, at 20-21 (explaining that "§ 14141 achieves its intended purpose: it authorizes structural reform litigation").

[355] *See* SAMUEL WALKER, THE NEW WORLD OF POLICE ACCOUNTABILITY 192 (2005) (stating that "[f]ederal pattern or practice litigation has been instrumental in bringing together disparate reform programs into [a] coherent package").

[356] Harmon, *supra* note 21, at 3 (noting the "limited resources" that "hampered" the implementation and effectiveness of § 14141).

[357] *Id.* (explaining that "according to deterrence theory, a rational actor will engage in conduct when doing so provides a positive expected return in light of the actor's utility function . . . [meaning that] a police department will adopt remedial measures to prevent misconduct when doing so is a cost-effective means of reducing the net costs of police misconduct or increasing the net benefits of protecting civil rights").

authority to audit police departments. This would expand the regulatory reach of the statute while also harnessing the power of public opinion to force police compliance. This would also guarantee regular interaction between the attorney general and local departments, allowing the attorney general to check up on data practices. Rather than facing only the remote possibility of a pattern or practice lawsuit, departments would be faced with regular, random audits of their data policies. Because the results of this regular audit system would be posted online, the departments would also be publicly accountable if they fail to abide by the statute. This could incentivize administrators to follow state law for fear of public embarrassment that could threaten their job security. Rachel Harmon has suggested the DOJ utilize a similar policy to overcome resource limits and expand the potential impact of §14141.[358]

In sum, these regulations attempt to holistically regulate the digitally efficient investigative state by limiting data retention and ensuring stored data are handled in a way that protects individual privacy, while still leaving ample room for legitimate law enforcement purposes. The enforcement mechanisms are sufficiently varied to ensure widespread compliance. And the statute as a whole follows the foundational principles of police surveillance regulations. The regulations are clear enough to avoid organizational mediation. They allow for individual variation. And they define the scope narrowly to only include a small subset of technologies like ALPR and surveillance cameras that pose a similar social risk.

CONCLUSION

The digitally efficient investigative state is here to stay. The empirical evidence clearly demonstrates that extremely efficient community surveillance technologies are an increasingly important part of American law enforcement. The language in *Jones* suggests that the judiciary may somehow limit public surveillance technologies in the future. To do so, the Court will have to confront the jurisprudential assumptions of police surveillance. That is no easy task. Much of the Court's previous treatment of police surveillance has rested on the belief that individuals have no expectation of privacy in public places, and

---

[358] Harmon describes how the Department of Justice could publish longer lists of departments that are suspected of a pattern or practice litigation and notify these departments that the worst offending departments will be prosecuted first. This "worst first" method would motivate a long list of departments that may be in violation of the statute to implement reforms for fear of lawsuit. *Id.* at 26-28.

that surveillance technologies that merely improve the efficiency of police investigations comport with the Fourth Amendment.

At present, it remains unclear how and when the Court will begin to alter these important assumptions. The language in *Jones* offers little guidance. But even when the Court does eventually broach this subject, the judiciary's institutional limitations will prevent it from crafting the type of expansive solution necessary to protect against the harms of the digitally efficient investigative state. In the absence of regulation, police departments across the country have developed dramatically different policies on the use of public surveillance technologies. Legislative bodies must take the lead and proactively limit the retention, identification, access, and sharing of personal data acquired by digitally efficient public surveillance technologies. The model state statute proposed in this Article would be a substantial step in reigning in the "unregulated efficiency of emerging investigative and surveillance technologies."[359]

[359] Rushin, *supra* note 8, at 328.